

Feasibility of a Cross-Border Electronic Funds Transfer Reporting System under the Bank Secrecy Act



FEASIBILITY OF A
CROSS-BORDER ELECTRONIC FUNDS
TRANSFER REPORTING SYSTEM
UNDER THE
BANK SECRECY ACT



*Prepared by the U.S. Department of the Treasury,
Financial Crimes Enforcement Network*

October 2006

TABLE OF CONTENTS

1.0 Executive Summary	v
2.0 Acknowledgments	ix
3.0 Overview.....	1
3.1 Goals and Design of the Feasibility Study	1
3.2 Background	2
4.0 Data Reasonably Necessary to Identify Illicit Finance	7
4.1 Individual targeting/research of known subjects.....	9
4.2 Data Matching against Other Data Sources.....	9
4.3 Link Analysis	10
5.0 Form, Manner, and Content of Reporting	11
5.1 Collecting from the “First In/Last Out” Institution in the U.S. 12	
5.2 Money Services Businesses as Collection Points	14
5.3 Form	15
5.4 Manner	17
5.5 Content.....	17
6.0 Technology Needed	19
6.1 Concept of Operations	19
6.2 Rough Order of Magnitude Cost Estimates	21
7.0 Information Security Protections.....	23
8.0 Conclusions and Recommendations.....	31
8.1 Project Risks	31
8.2 Pre-Acquisition Planning	34
8.2.1 User Requirements Analysis	35
8.2.2 Institutional Cost Analysis.....	35
8.2.3 Value Analysis.....	35
8.3 System Development and Deployment.....	36

Appendix A – Financial Crimes Enforcement Network Programs	37
Appendix B – Section 6302	45
Appendix C – Funds Transfer Rule	47
Appendix D – Fundamentals of the Funds Transfer Process.....	55
Appendix E – Cross-Border Funds Transfer Reporting in Canada and Australia.....	71
Appendix F – Potential Analytical Value of Cross-Border Funds Transfer Reports.....	83
Appendix G – FinCEN Industry Survey and Responses	111
Appendix H – Technical Alternatives Analysis.....	139
Appendix I – BSA E-Filing Fact Sheet	155
Appendix J – Preliminary Work Breakdown Schedule	157
Appendix K – Rough Order of Magnitude Cost Estimates.....	159
Appendix L – Project Management and Information Technology Processes.....	165
Appendix M – Acronyms.....	171

1.0 EXECUTIVE SUMMARY

Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004¹ amended the Bank Secrecy Act (BSA) to require the Secretary of the Treasury to prescribe regulations “requiring such financial institutions as the Secretary determines to be appropriate to report certain cross-border electronic transmittals of funds, if the Secretary determines that reporting of such transmittals is reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing.” Section 6302 requires further that, prior to prescribing the regulations contemplated by the Intelligence Reform and Terrorism Prevention Act, the Secretary shall submit a report to Congress that:

- i) identifies the information in cross-border electronic transmittals of funds that may be found in particular cases to be reasonably necessary to conduct the efforts of the Secretary to identify money laundering and terrorist financing, and outlines the criteria to be used by the Secretary to select the situations in which reporting under this subsection may be required;
- ii) outlines the appropriate form, manner, content, and frequency of filing of the reports that may be required under such regulations;
- iii) identifies the technology necessary for the Financial Crimes Enforcement Network to receive, keep, exploit, protect the security of, and disseminate information from reports of cross-border electronic transmittals of funds to law enforcement and other entities engaged in efforts against money laundering and terrorist financing; and
- iv) discusses the information security protections required by the exercise of the Secretary's authority under this subsection.²

The Secretary of the Treasury submits this Feasibility Report in accordance with the above requirements. Based on extensive fieldwork and analysis of information and data, and as discussed in substantial detail in this Report, we have determined that:

- i) The basic information already obtained and maintained by U.S. financial institutions pursuant to the Funds Transfer Rule, including the \$3,000 recordkeeping threshold, provides sufficient basis for meaningful data analysis.³

1 Pub. L. No.108-458 (Dec. 17, 2004), codified at 31 U.S.C. § 5318(n).

2 Section 6302 also provides that no regulations shall be prescribed until the Secretary certifies to Congress that FinCEN has the technical systems in place to effectively and efficiently receive, keep, exploit, protect the security of, and disseminate the reported information.

3 Section 6302 provides that information required to be reported under that section shall not exceed the information already required to be retained by financial institutions pursuant to section 21 of the

- Any reporting requirement should apply only to those U.S. institutions that exchange payment instructions directly with foreign institutions.
 - The \$3,000 threshold should apply only to discrete transactions and not to the aggregated total value of multiple transactions conducted very closely to one another in time.
- ii) Any reporting requirement should permit institutions to report either through a format prescribed by FinCEN, through the submission of certain pre-existing payment messages that contain the required data, or through an interactive online form for institutions that submit a low volume of such reports. The filing system should accommodate automated daily filing, periodic filing via manual upload, and discrete single report filing on an as-needed basis.
- iii) FinCEN would implement a federated data warehouse architecture to receive, keep, exploit, protect the security of, and disseminate information submitted under any reporting requirement. FinCEN would implement a separate path for the processing, enhancement, and storage of report information and would provide a single point of entry for users to submit queries to all BSA data systems, including cross-border funds transfer information, in a way that is invisible to the user.
- iv) FinCEN would apply existing policies and procedures that comply with all applicable legal requirements, industry and government best practices, and the Department of the Treasury's Information Technology Security Program Directive to every phase of the design and implementation of any system built to accommodate reporting of cross-border funds transfer data. Such compliance would be subject to certification.
- FinCEN also would impose strict limits on the use and re-dissemination of the data it provides to its law enforcement, regulatory, and foreign counterparts and strictly monitor those persons and organizations to which it grants access to the data.
 - Cross-border funds transfer data would be technologically protected and secure and would only be available to FinCEN and the law enforcement and regulatory agencies authorized by law to access it.

Federal Deposit Insurance Act (12 U.S.C. § 1829b and regulations promulgated thereunder (31 C.F.R. § 103.33(e) and (f) (the Funds Transfer Rule) and 31 C.F.R. § 103.33(g) (the Travel Rule)), unless:

- i) the Board of Governors of the Federal Reserve System (Board) and the Secretary jointly determine that particular items of information are not currently required to be retained under those law and regulations; and
- ii) The Secretary determines, after consultation with the Board, that the reporting of such additional information is reasonably necessary to conduct the efforts of the Secretary to identify cross-border money laundering and terrorist financing.

We conclude that, although construction of such a system is feasible, completion of such a system by December 2007 is not feasible. We estimate that the work would require approximately three and one-half years of effort. Further, we estimate that development and implementation of the proposed system would cost approximately \$32.6 million.

Other Considerations

In the course of conducting this study, FinCEN has identified a number of questions not posed by Congress that will affect *how* to implement the statutory requirements. These issues are discussed more completely elsewhere in this Report.

A significant concern is the cost, both to U.S. financial institutions and to the government, of implementing the reporting requirement and building the technological systems to manage and support the reporting. Related to these concerns are questions about the government's ability to use such data effectively. These concerns must be weighed carefully as we proceed.

Another concern is the potential effect that any reporting requirement could have on dollar-based payment systems such as: (1) a shift away from the U.S. dollar toward other currencies (i.e., the Euro) as the basis for international financial transactions; (2) the creation of mechanisms and facilities for clearing dollar-based transactions outside the United States; and (3) interference with the operation of the central payments systems. The U.S. has economic and national security interests in the continued viability and vitality of dollar-based payments and these possible outcomes must inform and guide the rulemaking process.

Next Steps

We propose an incremental development and implementation process. If the concerns noted above or any as-yet unidentified issues would impede the project or cause it to be infeasible, this incremental approach provides the opportunity to alter or halt the effort before FinCEN or the U.S. financial services industry incurs significant costs. As discussed in greater detail in this Report, the first phase in this project will comprise:

- Engaging with partners in the law enforcement, regulatory and intelligence communities to develop detailed user requirements to meet the most central needs of those who access BSA data.
- Engaging in a detailed discussion with representatives of the U.S. financial services industry, along with representatives of the major payment systems and members of the Canadian and Australian financial services industries. These discussions would focus on quantifying the cost the proposed requirement would impose on reporting institutions and the potential impact on the day-to-day operation of the payment systems.

- Engaging outside support to obtain and analyze a sizable sample of cross-border funds transfer data and exploring means of extracting value from the data, and identifying means to effectively and intelligently use the data to advance efforts to combat money laundering and illicit finance.

Based on these efforts, FinCEN will create a development plan that incorporates a series of milestones and would permit pilot testing of different aspects of the reporting system. This incremental development approach will enable FinCEN to build the system in manageable stages and to test the system's functionality at each stage before moving on to the next.

2.0 ACKNOWLEDGMENTS

The authors wish to thank all of those who contributed to this report. We would particularly like to thank our colleagues at the Board of Governors of the Federal Reserve System for their advice, feedback, and assistance. We would also like to thank the many representatives of the U.S. financial services industry and particularly, the members of the Bank Secrecy Act Advisory Group and its Cross-Border Funds Transfer Reporting Subcommittee for their input and guidance in the conduct of this study and the development of this report. We owe an enormous debt to Horst Intscher, Director of the Financial Transactions Reports and Analysis Centre (FINTRAC) in Canada, and to Neil Jensen, Director of the Australian Transaction Reports and Analysis Centre (AUSTRAC) in Australia, and all of our colleagues at both agencies who were so generous with their time and expertise and whose support and guidance were invaluable. We appreciate those members of the private sector who took the time and effort to respond to our Request for Information and thereby lent their technical expertise to the analysis of what such a system might look like. This study reflects the conclusions of FinCEN and does not purport to represent the positions of any of the persons, agencies, or other organizations that assisted us in our work. Nonetheless, we could not have completed this study without their very generous contributions.

We wish to thank specifically the following persons who offered their time and guidance in the conduct of this study.

Special Agent Steve Adelstein Office of the Arizona Attorney General	Chris Clubb Board of Governors of the Federal Reserve System
Khaled Bitar Financial Crimes Enforcement Network	Bill Conger BB&T
Kevin Bleckley Financial Crimes Enforcement Network	Alan Cox Financial Crimes Enforcement Network
Allison Brown Federal Trade Commission	Jennifer Craig Florida Department of Law Enforcement
Derek Bush Cleary Gottlieb Steen & Hamilton LLP	Lisa Dawson Financial Crimes Enforcement Network
John Byrne Bank of America	Donna Dohrman Internal Revenue Service
Joe Cachey Western Union	Small Business/Self-Employed

William Doyle
New York State Attorney General's Office

Linda Evans
Bureau of Alcohol, Tobacco, Firearms and
Explosives

Brian Ferrell
Financial Crimes Enforcement Network

Sean Forbush
Federal Deposit Insurance Corporation

Joe Frank
Bank of America

Doug Freedman
Barclays Capital

Special Agent Samuel Garcia
Bureau of Immigration and Customs
Enforcement

Teresa Gatlin
Florida Department of Law Enforcement

Yvonne Gilbert
New York State Police

Richard Gottlieb
J.P. Morgan Chase & Co.

Tonita Harrington
Conference of State Bank Supervisors

Special Agent Robert Heng
Drug Enforcement Administration

Special Agent Shannon Hodges
Internal Revenue Service – Criminal
Investigations

Assistant Attorney General Cameron
Holmes
Office of the Arizona Attorney General

Koko Ives
Financial Crimes Enforcement Network

Christina Klinger
Financial Crimes Enforcement Network

Charles Klingman
U.S. Department of the Treasury

Eric Kringel
Financial Crimes Enforcement Network

Ezra Levine
Howrey, LLP

Robert Long
Financial Crimes Enforcement Network

Jeremy Mandell
Board of Governors of the Federal
Reserve System

Debbie Matties
Federal Trade Commission

Kylin McCardle
Financial Crimes Enforcement Network

Special Agent Wallace Merriman
U.S. Department of Housing and Urban
Development
Office of Inspector General

Tim Moran
Financial Crimes Enforcement Network

Bridget Neill
Board of Governors of the Federal
Reserve System

James Kent Owens
Board of Governors of the Federal
Reserve System

Cherrie Pesce
Financial Crimes Enforcement Network

James Price
Bank of America

Richard Reise
American Bankers Association

Special Agent Ramon Rendon
U.S. Secret Service

Michael Rosenberg
Financial Crimes Enforcement Network

Jeff Ross
U.S. Department of the Treasury

Rob Rowe
Independent Community Bankers of America

Sergeant Pat Ryder
Nassau County (NY) Police Department

Racquel Self
Financial Crimes Enforcement Network

Andrew Shankman
Financial Crimes Enforcement Network

Michael Shore
Federal Trade Commission

Deb Silberman
Financial Crimes Enforcement Network

Richard Small
Citigroup

Christine Smith
Empire Corporate Credit Union

Dan Stipano
Office of the Comptroller of the Currency

Gary Sutton
U.S. Department of the Treasury

Lilly Thomas
Credit Union National Association

Emily Tzang
Financial Crimes Enforcement Network

Nancy A. Viano
U.S. Department of Agriculture
Office of Inspector General

Claude Walker
U.S. Department of the Treasury

David Ward
Financial Crimes Enforcement Network

Special Agent Laura Williams
Federal Bureau of Investigation

Suzanne Williams
Board of Governors of the Federal Reserve
System

Paul Wong
Board of Governors of the Federal Reserve
System

Catherine Woody
Conference of State Bank Supervisors

Al Zarate
Financial Crimes Enforcement Network

3.0 OVERVIEW

The Secretary of the Treasury has delegated his authority to administer the Bank Secrecy Act to the Financial Crimes Enforcement Network (FinCEN). Accordingly, FinCEN has responsibility to safeguard the U.S. financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activities. In order to fulfill its mission, FinCEN relies heavily on the use of BSA data, which is its primary and most important information asset. More than 200,000 financial institutions and money services businesses file over 15 million BSA forms or “reports” each year. Among other requirements, the BSA requires U.S. financial institutions to maintain certain records of funds transfers.

Section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004 directs the Secretary of the Treasury to prescribe regulations to require the reporting to FinCEN of information about certain cross-border electronic transmittals of funds where the Secretary finds such reports are reasonably necessary to help detect and prevent the proceeds of financial crimes and terrorist financing from flowing across America’s borders.⁴ The Act requires the Secretary to issue these regulations by December of 2007. The Act further requires that, prior to any such regulations taking effect, the Secretary certify that the technical capability to receive, store, analyze, and disseminate the information is in place. The Act also requires that, in preparation for implementing the regulation and data collection system, the Treasury study and report to Congress the feasibility of implementing such regulations.

3.1 Goals and Design of the Feasibility Study

This report assesses:

- What information in a funds transfer it is reasonably necessary to collect to conduct our efforts to identify money laundering and terrorist financing, and the situations in which reporting may be required;
- The value of such information in fulfilling our counter-terrorist financing and anti-money laundering missions;
- The form that any such reporting would take and the potential costs any such reporting requirement would impose on financial institutions;
- The feasibility of FinCEN receiving the reports and warehousing the data, and the resources (technical and human) that would be needed to implement the reporting requirement; and,

⁴ Pub. L. No.108-458, Dec. 17, 2004; codified at 31 U.S.C. § 5318(n)

- The concerns relating to information security and privacy issues surrounding the reports collected.⁵

This report also identifies a number of issues that policy makers must consider, such as whether the potential value of requiring financial institutions to report information about cross-border funds transfers outweighs the potential costs of building the technology, the costs to financial institutions of implementing compliance processes, and the social costs related to privacy and security of the information.

Our development of this feasibility study included multiple approaches. An internal working group of employees drawn from all operational divisions of FinCEN coordinated efforts within the organization, managed contact with external stakeholders, hosted small workshops with law enforcement representatives, visited relevant U.S. and foreign government and private sector organizations, surveyed industry and governmental organizations, solicited input from private sector technology experts, and researched extensively. In addition, FinCEN formed a subcommittee of the Bank Secrecy Act Advisory Group⁶ including representatives from across the spectrum of U.S. financial services industry members, and governmental agencies. The subcommittee did not author or review this study, but provided expert assistance in the identification and analysis of relevant issues, recommendations about the focus of the study, and important contacts within the U.S. financial services industry. We also drew upon the experience of the Australian Transaction Reports and Analysis Centre (AUSTRAC) and the Financial Transactions Reports and Analysis Centre (FINTRAC), our counterpart financial intelligence units in Australia and Canada, both of which already collect cross border funds transfer information.

3.2 Background

The Financial Crimes Enforcement Network (FinCEN), a bureau within the Department of Treasury, is the United States' financial intelligence unit (FIU). Our mission is to safeguard the U.S. financial system from the abuses of financial crime, including terrorist financing, money laundering, and other illicit activity. As administrator of the BSA, FinCEN is responsible for managing, analyzing, safeguarding, and appropriately sharing financial transaction

5 See, Section 6302(n)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (S.2845 P.L. 108-458)

6 Congress established the Bank Secrecy Act Advisory Group (the "BSAAG") in 1992 to enable the financial services industry and law enforcement to advise the Secretary of the Treasury on ways to enhance the usefulness of Bank Secrecy Act reports. Since 1994, the Advisory Group has served as a forum for industry, regulators, and law enforcement to communicate about how law enforcement uses Suspicious Activity Reports, Currency Transaction Reports, and other Bank Secrecy Act reports and how FinCEN can improve the reporting requirements to enhance their utility while minimizing the costs to financial institutions.

information collected under the BSA and other authorities. FinCEN currently collects more than 15 million reports per year related to financial transactions conducted through or by U.S. financial institutions. FinCEN's information technology systems integrate the collection, storage, analysis, and dissemination of the data to our Federal, State, and local partners as well as FinCEN's international counterparts.

Although the U.S. financial system remains susceptible to abuse by terrorist and criminal organizations to launder the proceeds of criminal activity and to facilitate illicit activity, U.S. Government efforts to increase transparency in the system make illicit financial activity more apparent to those agencies engaged in the effort to detect, prevent, and respond to financial crimes. As a result, it becomes significantly more difficult for those engaged in financial crimes to conduct business. As those illicit actors adapt to the increasingly transparent system, they must make additional and more complicated efforts to conceal their behavior and resort to slower, riskier, more expensive, and more cumbersome methods of raising and moving money.

As a result of the BSA regime, most money launderers, drug dealers, and high-level fraudsters understand that trying to pump massive amounts of cash through a U.S. bank is fraught with peril. As a result, they generally prefer instead to use other, less risky, methods to move money—sending it in bulk across our porous borders, for example, or through a less-regulated industry like money-transmitting services. If they do use banks, they take care to structure smaller transactions among dozens of different accounts—less risky, to be sure, but considerably slower and more costly.⁷

Every additional step or layer of complexity illicit actors must add to their schemes provides new opportunities for detection, and an increased risk to those who would abuse the financial system. Criminals who fear using the banking system do not have a ready and reliable alternative for moving large sums of money. To the extent that criminal transactions touch the formal financial system, there is the likelihood that those transactions will leave a trail that law enforcement officials can use to “follow the money” to link criminals to each other and to wider support networks.

The reports filed by financial institutions pursuant to the BSA focus largely on cash transactions and on transactions that are suspicious on their face. This approach has been very successful in creating a transparent financial system that is hostile to abuse by criminal actors. The value of transparency is twofold – it deters those who would use the financial system for illicit activity and promotes the detection of those who do so.

7 Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States, p. 56

As the financial system has evolved, criminals and terrorists have taken full advantage of new and technologically advanced means of moving and hiding their money. While the traditional Bank Secrecy Act reports still have significant utility in combating illicit finance, there is currently no Bank Secrecy Act report that provides the government insights into the complex network of relationships and financial activity that occurs once money is in the system. If a non-cash transaction does not raise the suspicions of a bank teller, the government may never become aware of it. As governments throughout the world strive to promote transparency in the financial system, the shortage of tools for detecting schemes that rely on these modern technological payment systems creates a potential blind spot in our efforts to protect the homeland and to combat financial crime.

Presumably, if the records of currency transactions are supposed to be useful in detecting criminal offenses, it is not immediately clear why records of at least some non-currency transactions should not also be subject to analysis (i.e., if they are linked in some way to suspicious cash activity, or for some other reason). Yet, while most non-currency transactions are auditable in principle, they are rarely subject to some kind of audit--either because the government lacks access to the information without individualized suspicion or lacks the technical capacity to analyze the information it does collect.⁸

Electronic funds transfers are attractive to legitimate businesses because they generally provide a secure and trusted means of sending large amounts of money quickly. For those reasons, electronic funds transfers are also attractive to legitimate users as a means of sending small amounts of money quickly. These same features make electronic funds transfers equally attractive to illicit actors because electronic funds transfers allow them to spirit their money beyond the grasp and sometimes out of the sight of law enforcement. In addition, because electronic funds transfers need not involve the actual physical movement of currency, they are a relatively rapid, reliable, and secure method for transferring funds without the risks associated with large cash deposits or physical transportation of illicit monies. (Appendix D describes the fundamentals of the electronic funds transfer process).

Traditionally, experts describe three stages of money laundering:

- Placement – introducing cash into the financial system or into legitimate commerce;
- Layering – separating the money from its criminal origins by passing it through several financial transactions;
- Integration – aggregating the funds with legitimately obtained money or providing a plausible explanation for its ownership.

⁸ Cuellar, Mariano-Florentino, Criminal Law: The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance, *The Journal of Criminal Law and Criminology* 93:311, 426 (2003).

The BSA reporting regime deals well with the placement stage. Some financial institutions file Currency Transaction Reports (CTRs) when a person conducts certain types of large currency transactions, others file Forms 8300 for large amounts of cash or monetary instruments received in a trade or business, and travelers entering the U.S. with more than \$10,000 in currency must complete Currency and Monetary Instrument Reports (CMIRs).⁹ However, while these three reports address placement, due to their focus on currency-based transactions, they do not provide insights into the rapidly developing electronic aspects of financial transactions. These reports identify the physical movement of currency within the U.S. financial system. Electronic funds transfers, by contrast, represent an entirely different mode for the movement of money.

The Suspicious Activity Report (SAR) provides some insight into the layering and integration stages by casting a light on transactions of any amount and type that financial institutions suspect are related to illicit activity or that are suspicious in that they do not appear to fit a known pattern of legitimate business activity.

We have found that electronic funds transfers feature prominently in the layering stage of money laundering activity, which is not addressed in any of the reports currently filed if the transactions do not raise suspicions within the financial institution.

The annual typologies reports of the FATF and a report published in 2000 by the Egmont Group of Financial Intelligence Units describe recent cases that illustrate methods of laundering and investigation. Given that these are simply reported cases, they do not necessarily reflect the relative importance of different techniques. With that qualification, the FATF and Egmont Group reports can be used to develop a matrix matching 11 predicate crimes with 20 money-laundering methods. There were 223 cases available for classification, and each case involved one or more offenses and methods of laundering, thus producing a total of 580 entries.

Three offense categories accounted for over 70 percent of entries: drugs (185), fraud (125), and other kinds of smuggling (92). The types of laundering methods were more evenly distributed – wire transfers were involved in 131 cases (22 percent), but no other single method was involved in more than 75 cases. For the three major offense categories, the observations were broadly distributed across methods.¹⁰

Complex electronic funds transfer schemes can deliberately obscure the audit trail and disguise the source and the destination of funds involved in money laundering and illicit finance. For example, a money launderer or illicit financier

9 See http://www.fincen.gov/reg_bsaforms.html

10 Reuter and Truman, Chasing Dirty Money, The Fight Against Money Laundering, (Institute for International Economics) p. 32

may simply transfer illicit funds through several different banks by means of multiple, structured transactions (i.e., in amounts below the applicable reporting thresholds) in order to blur the trail to the funds' source. Alternatively, the perpetrator may make multiple transfers from myriad bank accounts, into which he or his accomplices have made structured deposits to avoid detection, to a single collecting account located abroad. In even these simple examples, the perpetrators have made the government's task more daunting. First, detection of such schemes is exceedingly difficult. In these cases, unless a transaction exceeds the dollar thresholds for obtaining and maintaining customer and transaction information or filing Currency Transaction Reports (CTRs), or unless an institution otherwise identifies any part of the transaction as suspicious, the BSA recordkeeping and reporting regime would not necessarily capture the activity. Moreover, even assuming the government had a lead from an alternate source, obtaining the relevant information through subpoenas, warrants, letters rogatory, or other legal process is cumbersome and entails delays of weeks, months, or even years.¹¹

11 A "letter rogatory" is a means of obtaining assistance from foreign governments in absence of a treaty or executive agreement. In essence, a letter rogatory is a formal request from the courts of one country to the courts of another seeking assistance through the judicial processes in obtaining testimony or other evidence through the receiving nation's judicial process.

4.0 DATA REASONABLY NECESSARY TO IDENTIFY ILLICIT FINANCE

FinCEN, acting jointly with the Board of Governors of the Federal Reserve System, has taken some steps to address the particular vulnerabilities to money laundering and other illicit uses of electronic funds transfers. The existing Bank Secrecy Act funds transfer regulation consists of two rules: the “Funds Transfer Rule” (issued jointly by the Board of Governors of the Federal Reserve System and FinCEN as required by Section 1829(b) of the Federal Deposit Insurance Act) and the “Travel Rule.”¹² The recordkeeping rule generally requires institutions to collect and retain records of certain specified data regarding funds transfers of \$3,000 or more that the institution processes.¹³ The travel rule requires financial institutions to include, to the extent feasible, information collected under the recordkeeping rule that will travel throughout the payment chain. Any record that a financial institution is required to maintain pursuant to the Funds Transfer rule “shall be submitted or made available to the Secretary [through his delegate, FinCEN] or the Board [of Governors of the Federal Reserve] upon request.”¹⁴

12 See 31 C.F.R. § 103.33 generally and 31 C.F.R. § 103.33(g) (travel rule). The Annunzio-Wylie Anti-Money Laundering Act of 1992 (Pub. L. No. 102-550, § 1515) required the Secretary and the Board to jointly issue regulations requiring insured depository institutions to maintain records of funds transfers. The Treasury – and not the Board – is authorized to issue regulations requiring nonbank financial institutions to maintain records of transmittals of funds. Accordingly, although the recordkeeping rule and travel rule are derived from separate rulemakings, they are promulgated in one regulation found at 31 C.F.R. § 103.33. The government has found certain categories of entities involved in the payment chain of wire transactions to pose a low threat of money laundering or terrorist financing and thus has excepted certain parties of the transaction from requirements of the current rules. Compliance with both the recordkeeping and travel rules is waived if both parties to the transaction are any of the following: (1) banks or brokers or dealers in securities or futures commission merchants or introducing brokers or their subsidiaries; (2) government entities; or (3) the transmitter and recipient are the same person and the transaction involves a single bank or broker-dealer. See 31 C.F.R. § 103.33(e)(6) and (f)(6). In addition, “funds transfer” is defined under 31 C.F.R. § 103.11 to exclude all funds transfers governed by the Electronic Fund Transfer Act of 1978, as well as any other funds transfers that are made through an automated clearing house, an automated teller machine, or a point-of-sale system. Therefore, since such transfers are excluded from the “funds transfer” definition, they are exempt from the requirements of 103.33.

13 Earlier this year the Department of the Treasury and the Federal Reserve jointly issued an Advance Notice of Proposed Rulemaking announcing that they are reviewing and considering a reduction in the \$3,000 threshold, particularly in light of international standards, and seeking comment on the potential benefits and burdens of any such reduction. 71 Fed. Reg. 35,564 (June 21, 2006) See Interpretive Note to FATF Special Recommendation VII (requiring countries to mandate that cross-border wire transfers contain accurate and meaningful originator information). Countries may adopt a de minimus threshold of no more than \$1,000 or 1,000 Euros. Countries are expected to be in compliance with the Special Recommendation by December 2006.

14 See 12 U.S.C. § 1829b(b)(3)(C). Any information reported to Treasury or the Board in accordance with section 1829b(b)(3)(C) falls within an exception to the Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. See 12 U.S.C. § 3413(d) (excepting disclosures pursuant to Federal law or rule). Moreover, the Right to Financial Privacy Act does not apply to money transmitters. See 12 U.S.C. § 3401(1) (defining a “financial institution” for purposes of the Act’s coverage to include banks and other depository institutions).

In combination, these rules require U.S. financial institutions to obtain and maintain information about certain funds transfers that identifies, at a minimum:

- the name and address of the originator;
- the amount of the transfer;
- the execution date of the transfer;
- any payment instructions received;
- the name and address of the beneficiary (if available);
- the account number of the beneficiary (if available);
- any other specific identifiers of the beneficiary (if available); and
- the beneficiary's financial institution.¹⁵

Existing regulations make no distinction between domestic and international funds transfers; financial institutions must obtain and maintain the required information about all funds transfer transactions above the \$3,000 threshold. Therefore, institutions reporting cross-border electronic funds transfers would need to segregate cross-border funds transfers from information about domestic funds transfers. Reporting institutions also would need to segregate cross-border funds transfers above the \$3,000 threshold.

While the BSA does not require U.S. financial institutions to report to FinCEN the information they maintain about funds transfers, the data is available to FinCEN and to regulators to whom FinCEN has delegated BSA compliance examination authority through the examination process. Information about cross-border funds transfers also is available to law enforcement through normal administrative processes, information requests, subpoenas, or the 314(a) process (See appendix A). These processes can involve delays to access of information for days, weeks, months, or years. Because the Travel Rule is a recordkeeping requirement rather than a reporting requirement, information is not available to regulators and law enforcement on a real time basis. Therefore, as a practical matter, regulators, and law enforcement currently tend to seek access to this information only in connection with an existing investigation or in the course of a compliance examination.

¹⁵ Strictly speaking, the applicable rules use parallel but not identical language to describe the relevant transactions and the persons sending and receiving funds through different types of institutions (i.e., originator, transmitter, beneficiary, recipient, bank, and non-bank financial institutions). For purposes of simplicity, we describe the transaction as a funds transfer, the person initiating a funds transfer as an originator, the person receiving the funds as a beneficiary, and the parties' bank or financial institution as a financial institution throughout.

A reporting requirement would create a centralized database of this very basic cross-border electronic funds transfer information in a single format and link it with other highly relevant financial intelligence. Furthermore, this very basic information about such transfers provides both a source of information that can provide new leads standing alone and can potentially enhance the use and utility of current BSA data collected by FinCEN when combined with those other data sources. Among the ways in which FinCEN and its partners can exploit this data are individual searches for known subjects, data matching with other sources of lead information, and link analysis with other financial, law enforcement, and intelligence reporting. (Appendix F describes these and other potential avenues of exploiting this data).

4.1 Individual targeting/research of known subjects

Analysts and investigators researching specific identified subjects are likely to rely primarily on the capacity to search electronic funds transfer data for specific names or account numbers and receive results within seconds. This kind of query and reporting function allows analysts to construct a customized query in response to a specific need. Many commercial software tools provide the query and reporting capabilities for retrieving structured data.

4.2 Data Matching against Other Data Sources

FinCEN currently uses a large number of databases to identify and analyze financial crimes. FinCEN information comes from four primary sources:

- the Bank Secrecy Act Database that contains SARs, CTRs, Currency and Monetary Instruments Reports, Foreign Bank Account Reports, and other reports;
- several databases of criminal reports sourced from, among others, the Immigration and Customs Enforcement's TECS II system, the FBI's National Criminal Information Center, the Drug Enforcement Administration's Narcotics and Dangerous Drugs Information and NDIC Systems, the United States Secret Service database, and the United States Postal Inspection Service;
- FinCEN's own database of investigations and queries conducted through FinCEN's systems; and
- Commercial database services from organizations such as Dun & Bradstreet, LEXIS/NEXIS, and credit bureaus,¹⁶ as well as commercially available lists of "Politically Exposed Persons."¹⁷

16 FinCEN only has access to credit bureau header information, not full credit reports. Header information typically consists of identifying information such as name, address, SSN, etc.

17 See <https://www.world-check.com> and <http://www.worldcompliance.com>. Many government agencies and financial institutions employ such lists for intelligence and risk management purposes respectively.

In addition, FinCEN analysts have access to other lists and databases maintained by federal government agencies that they may use to cross-reference BSA data, or as the basis of a search of the data. These sources include the Office of Foreign Assets Control's list of Specially Designated Nationals, the Social Security Administration's Death Master File, and the State Department's list of Designated Foreign Terrorist Organizations.

4.3 Link Analysis

Link analysis is a technique used to explore associations within a large collection of data of different types. Link analysis requires a variety of readily available data, some of which provide indicators of money laundering activity (i.e., SARs, law enforcement data, case files, etc.). In the case of financial data, the connections might include names, addresses, phone numbers, bank accounts, businesses, funds transfers, and cash deposits. Combining and linking these pieces of data from multiple sources adds layers of understanding to the behavior that the data represents.

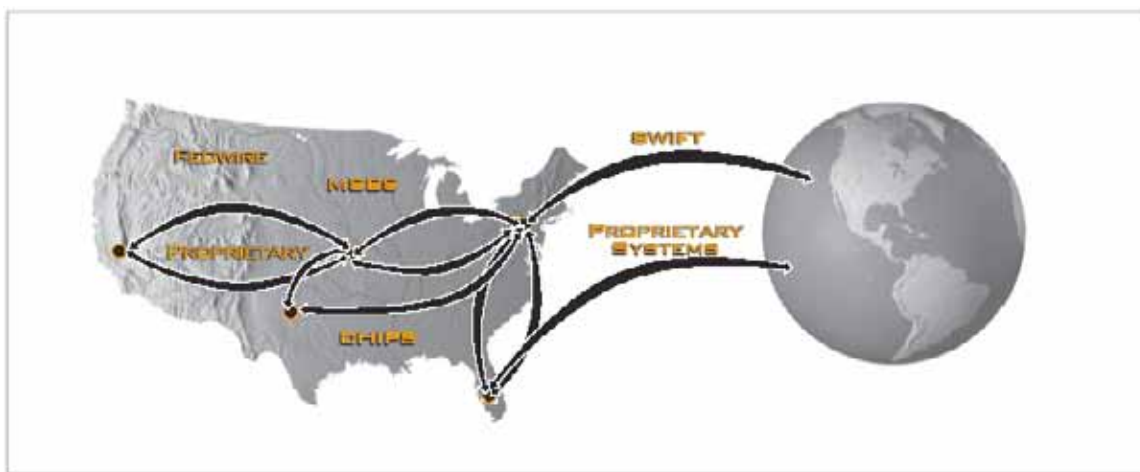
Link analysis depends on the integration of one or more sets of data records. Within each data set, each record has several data fields containing information. These might be records of an individual (with fields of name, address, and phone number), bank account (account number, owner, bank), or business (name, owners' names, board members, address). As noted, FinCEN already collects multiple Bank Secrecy Act reports, each containing specific data fields. While there are many differences between them, there are also many fields common to the various reports. Likewise, even the limited pieces of data necessary to a funds transfer message overlap some of the information collected in these reports. Link analysis looks for matching fields in each of these records. For example, two reports identifying two separate individuals but each associating its subject with the same phone number as the other, could indicate that two persons know each other well, or even live at the same address.

Link analysis is useful in financial investigations because it can integrate many disparate sources of information. As noted, with the exception of SARs, the individual reports that FinCEN currently receives, and even the records that might be available through cross-border funds transfer reporting, provide few indicators of suspicion. However, link analysis provides a way of combining these different records so that analysts can detect the patterns and relationships between the different sets of data. FinCEN employs link analysis to identify relationships between the various BSA reports it currently collects.

5.0 FORM, MANNER, AND CONTENT OF REPORTING

Financial institutions may use standardized or proprietary or internal systems to handle all or part of an electronic funds transfer (i.e., between branches of the same institution). Proprietary systems pose a special challenge to designing a reporting system because of the wide range of potential message formats, communications protocols, and data structures involved. The primary challenge that arises in this context is that a reporting requirement would require that the U.S.-based institution implement processes for identifying and extracting cross-border funds transfer information from its proprietary communications systems. The implementing regulation must take into account this kind of permutation in order to ensure that FinCEN collects cross-border transfers that follow this pattern.

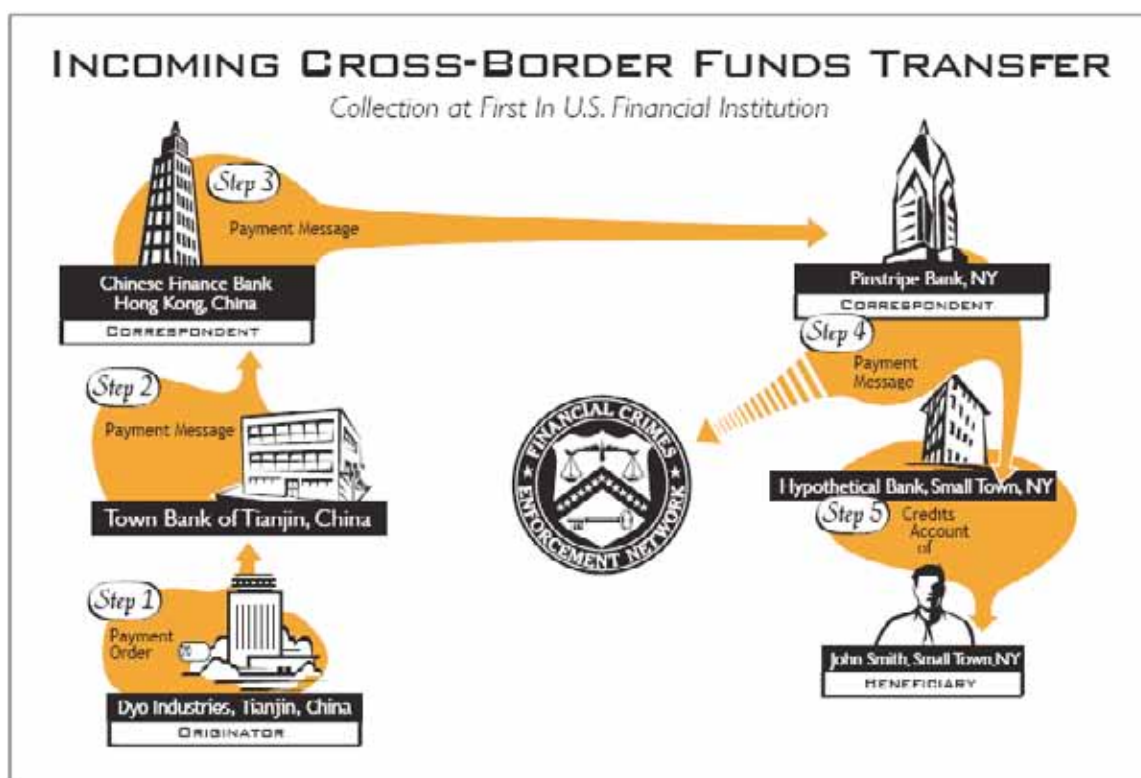
Although myriad systems are available to U.S. financial institutions to process electronic funds transfers, cross-border funds transfers tend to flow through a small number of channels as they enter and leave the United States (i.e., Fedwire, CHIPS and SWIFT; see Appendix D).¹⁸ As institutions pass payment orders along through correspondents en route to their destination, those institutions' systems convert the orders from the many available formats to one of only a few. At some point in the cross-border payment chain a single U.S. financial institution must communicate directly with a foreign financial institution.



¹⁸ Many in industry and government have raised the question of what changes, if any, the proposed collection system would require to the established funds transfer messaging systems (i.e., CHIPS, SWIFT, Fedwire). In its response to FinCEN's industry survey issued in March 2006, the American Bankers Association stated that "Imposing a new requirement to include this type of information for all wire transfers would require substantial changes to US payment systems." Such changes were not necessary to the implementation of the corresponding requirements in either Canada or Australia. It is the conclusion of this study that not only would no such change be required, but that if such a change were necessary in order to make such a system work, the system would not be feasible.

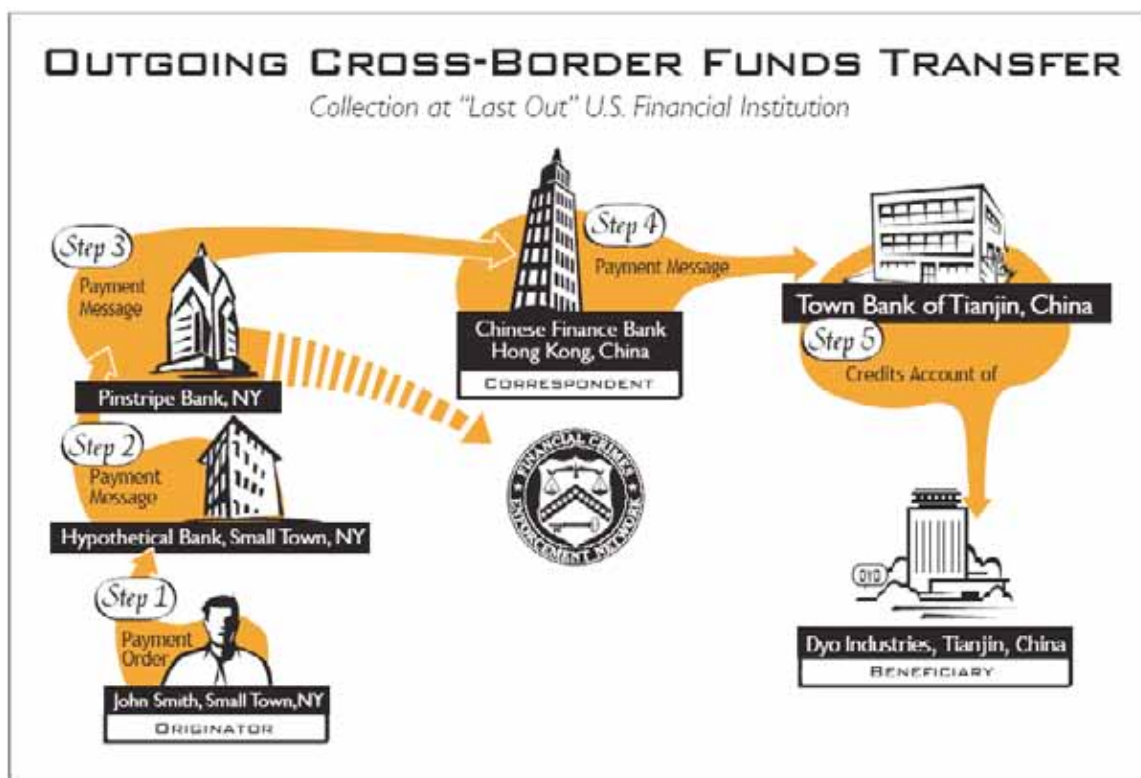
5.1 Collecting from the “First In/Last Out” Institution in the U.S.

The following graphic illustrates an incoming cross-border funds transfer transaction and identifies the “first in” U.S. bank (Pinstripe Bank) as the institution that must report the transfer. In this scenario, the originator, DYO Industries in China, is requesting their bank, Town Bank of Tianjin, to send a funds transfer to the beneficiary, John Smith in New York. The funds transfer flows through several intermediary correspondent banks along the way.



The “first in” bank in the U.S. may serve as a correspondent in the overall transaction chain or it may be the beneficiary’s bank. Because the details contained in a funds transfer message’s optional fields may change or disappear along the chain, the “first in” bank may have the most complete information related to the transaction of any U.S. financial institution.

The following graphic illustrates an outgoing cross-border funds transfer transaction, and identifies the “last out” U.S. institution (Pinstripe Bank) as the institution required to report the transfer to FinCEN.



A “last out” bank’s record should identify the originator, the originator’s bank, and other information about the transaction (e.g., beneficiary, beneficiary’s bank, information exchange, additional banks involved and their roles, date, amount, etc.). Similarly, the “last out” bank’s record may provide a more complete picture of the entities involved in the overall chain of the transaction. Investigators and analysts could then determine where to turn for further information on the transaction and customer. In addition, the customer identification (to the extent it is included in the original message) and other transaction detail information should remain intact and available throughout this correspondent stage and therefore remain available in the instructions handled by the last out banks.

Whether a “first in” or “last out” institution, because of the size and nature of institutions that serve in correspondent roles for cross-border funds transfers, these banks are more likely to be connected with and use centralized message systems (SWIFT, Fedwire, CHIPS) and their standardized message formats. These standardized formats increase the ability of these institutions to handle the transactions with little manual intervention. In addition, these larger banks may often automatically “map over” messages from one system’s format to another (e.g., from SWIFT to Fedwire; from SWIFT to CHIPS). Accordingly, many would have systems in place to perform much of the data extraction necessary to create the reports required.

We conclude that it would be most effective to collect funds transfer reports from the “First In/Last Out” institutions. In other words, the obligation to report should fall upon those U.S. institutions that transmit an electronic funds transfer instruction directly to a non-U.S. financial institution or conversely, those that receive such instructions directly from a non-U.S. financial institution. This approach aims to capture a funds transfer instruction at the point at which it crosses the U.S. border. The advantages of the approach are that it focuses the reporting requirement upon larger institutions that are most familiar with international funds transfers, have the technological systems in place to facilitate such transfers, and are in the best economic position to implement compliance systems and processes.¹⁹ Based on our research, we also believe that this will effectively capture the majority of funds transfers entering and leaving the United States without creating needless duplication among the reports submitted to FinCEN. In addition, such a requirement would have the effect of reducing the variation in the types of messages captured and the number of institutions submitting reports.

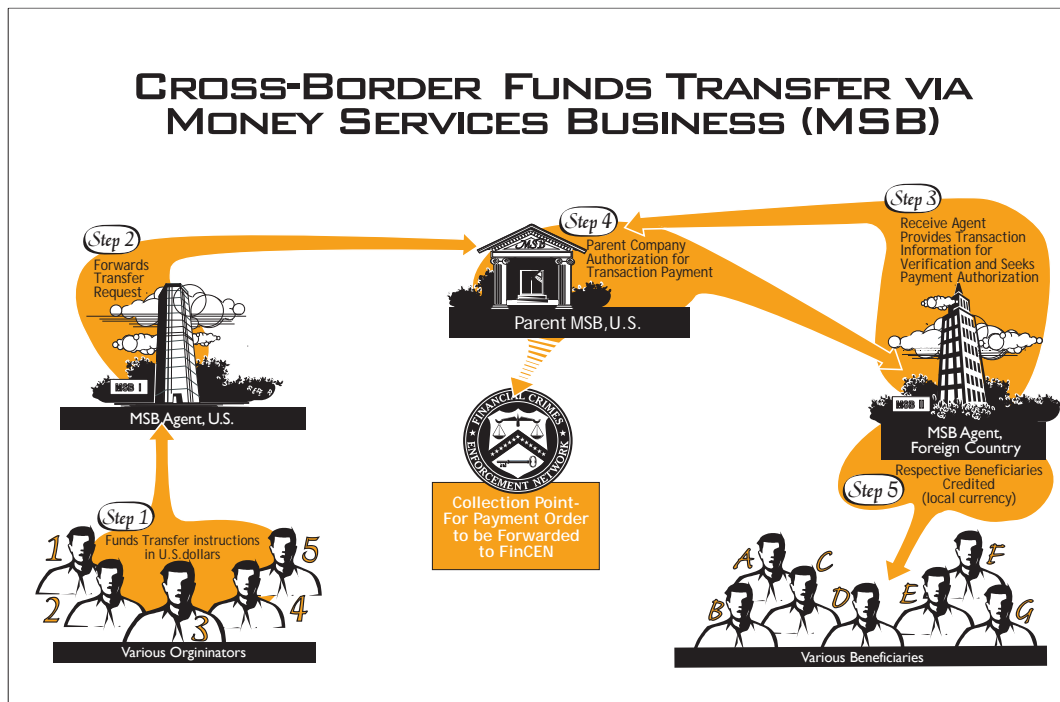
5.2 Money Services Businesses as Collection Points

In addition to the banking industry, certain money services businesses (MSBs) operate as retail money transmitters. Money transmitters provide many of the same attractions as the major bank-based electronic funds transfer systems. Money transmitters often maintain agent relationships with businesses around the globe, permitting rapid, secure transfer of funds. The largest MSBs generally maintain centralized communications systems and database records of customer transactions that provide an obvious source for the funds transfer information collection. (Appendix D describes funds transfer operations by MSBs.)

This kind of centralized data repository provides a much more efficient collection point than do the agent businesses. In addition, under current Bank Secrecy Act regulations, all money transmitters that meet the definition of an MSB are required to register with FinCEN, except if it serves solely as an agent of another MSB. Therefore, it is easier to identify and monitor this smaller collection universe of MSBs than to collect information directly from MSB agents.

19 In its response to FinCEN’s March 2006 industry survey, the American Bankers Association offered that “An unscientific poll of bankers visiting ABA’s compliance web page revealed that only 1 in 4 respondents identified themselves as conducting “last out, first in” cross-border transfers.” The ABA also noted “for some [banks] it required less IT logic to be built into the reporting system.” Significantly, the ABA opined “. . . a “last out, first in” reporting obligation would suffice to capture the cross border transfer of funds and whatever information is attached to that transmittal. Although this method shifts much of the reporting cost to a smaller number of generally larger banks, many of the[m] possess sufficient capacity to perform the reporting with greater efficiency than would be the case if the obligation rested with all originating or beneficiary’s institutions.”

The diagram below further illustrates a money transfer process occurring through one of the large, centralized money transmitters.



Money transmitters generally effect funds transfers through a bank.²⁰ However, there are other models, and it is beyond the scope of this study to enumerate the possible permutations. We conclude that a combination of realistic expectations, carefully tailored reporting requirements, and phased implementation of reporting can overcome this challenge.

5.3 Form

Electronic funds transfer messages generally are consistent in terms of the types of information that they contain regardless of the underlying message system on which they travel. Typically, funds transfers include information such as the account number of the bank customer, the originator of the transfer, the beneficiary of the transfer, the originating and beneficiary bank, the dollar

²⁰ Note, however, that this is not true of all money transmitters. As the 9/11 Commission noted, “A hawala, at least in its ‘pure’ form, does not use a negotiable instrument or other commonly recognized method for the exchange of money. Hawaladars instead employ a variety of means, often in combination, to settle with each other: they can settle preexisting debt, pay to or receive from the accounts of third parties within the same country, import or export goods (both legal goods, with false invoicing, or illegal commerce, such as drug trafficking) to satisfy the accounts, or physically move currency or precious metal or stones.” Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States p. 68.

amount (sometimes denominated in foreign currency), instructions for the disposition of the funds, and other information. In addition, some payment system messages contain a variety of codes that identify the country of origin and destination, the bank of origin and destination, and other information. However, depending on the funds transfer system, the actual format of the data can vary substantially.

To accommodate these variations, FinCEN must adopt a limited number of standard forms for funds transfer reporting. These standards must accommodate automated filing of large collections of funds transfer reports, manual uploading of mid-sized collections of funds transfer reports, and discrete filing by small volume funds transfer service providers. In addition, the standards must assimilate the variations between the different funds transfer message systems from which the reporting institutions will extract the data. Finally, the standards must be such that reporting institutions can convert the source data from their systems into the required format with a minimum of manual intervention or system modifications.²¹

Any implementing regulation should permit institutions to comply with this requirement through the submission of customized reports that comply with a format prescribed by FinCEN or through the submission of certain pre-existing formats (i.e., CHIPS or SWIFT messages) that contain the required data elements. The pre-existing forms deemed acceptable by FinCEN would serve as proxies for formally prepared reports. In addition, FinCEN must prescribe an acceptable standardized format that specifies the specific data elements required. Institutions that must report but that lack the ability to deliver data in one of the approved pre-existing formats would need to convert their own data into this prescribed format and deliver it to FinCEN.

Developing the minimum data requirements and standard formats will require close consultation with members of the U.S. financial services industry through the rulemaking process or otherwise. Collaboration is essential to ensuring that institutions can reasonably implement the technology to extract SWIFT messages from their systems or convert other data into the prescribed format with a minimum of investment in time and labor.

21 The ABA suggests, “regardless of the nature of any imagined reporting requirement, the financial services industry’s responsibility should extend only to the simple transmittal of raw data, with FinCEN assuming full responsibility for the refinement and distillation of the data into a format useful to law enforcement agencies.” While we believe that accommodation of every possible format is unreasonable, the approach proposed in the text recognizes the potential cost and strikes a balance aimed at accommodating the widest possible variation in reporting formats.

5.4 Manner

Reporting institutions would be responsible for extracting the cross-border funds transfer data from their operation systems and generating appropriate reports for submission to FinCEN through a secure web protocol. The BSA E-Filing program has successfully implemented this kind of solution to allow large filers to use Connect:Direct, a commercial product, to transfer the BSA data from their own systems to FinCEN. Since many of the reporting institutions have already established the connections with FinCEN, it will be easier to continue using the same method for funds transfer data submission.

As a practical matter, due to the volume of anticipated reporting, it will be necessary for FinCEN to mandate electronic filing of all cross-border funds transfer data. However, the specific means of delivering these electronic reports must be flexible enough to accommodate the various business processes of the reporting institutions and the volume of reports submitted by the various institutions. For institutions that process high volumes of cross-border funds transfers, FinCEN proposes to rely upon its existing BSA E-filing infrastructure. We propose that the modified BSA E-Filing system provide three separate means of submitting reports.

For those institutions with sufficient infrastructure and volume, FinCEN should provide a means to submit reports in large batch files through an automated communication between the institutions' systems and BSA E-Filing. For those institutions that lack the infrastructure or choose not to automate the report submission, FinCEN must also provide an interface through which employees of the institution can manually upload prepared electronic report files through a secure internet portal. Last, FinCEN must provide a secure internet portal through which institutions that process only a very small number of cross-border transfers may complete an online form containing the required information.

5.5 Content

As noted earlier, we conclude that the information or data elements about a funds transfer that U.S. financial institutions must maintain under 31 C.F.R. § 103.33 provide sufficient information for meaningful analysis. Thus, we recommend that any implementing regulation define the required elements of a cross-border funds transfer report in terms identical to those in the funds transfer rule, 31 C.F.R. § 103.33. The funds transfer rule currently applies to transactions of \$3,000 or more and we do not propose any different threshold for cross-border funds transfer reporting.²² We believe that any proposed rule

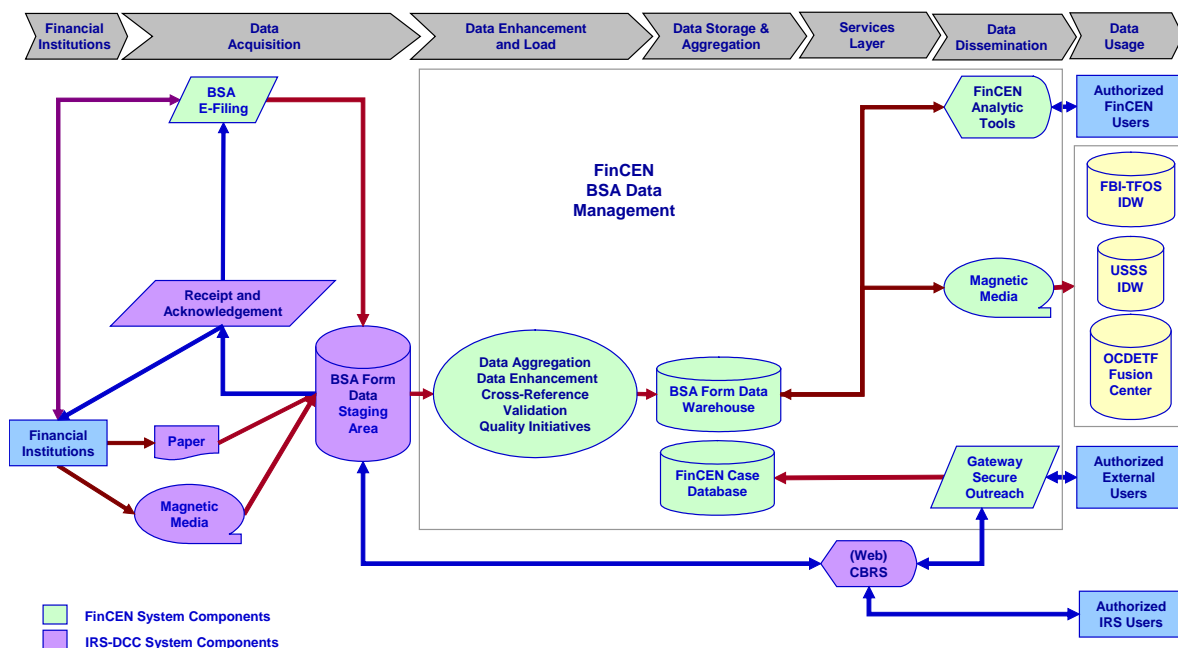
²² According to the American Bankers Association, "Thresholds – as long as there is no aggregation requirement – are not particularly complicating system wise – but distinctions can involve compliance monitoring challenges especially if the notion of structuring is applied to wire activity."

should incorporate by reference the data elements and threshold requirements of the Funds Transfer Rule in order to accommodate any changes that might occur in the future. We recommend further that any proposed regulation apply the applicable threshold only for discrete transactions rather than requiring financial institutions to attempt to identify multiple transactions aggregating to an amount above the threshold. We believe that the added costs to industry that an aggregation requirement would entail are unwarranted because the affected financial institutions already are required to monitor transactions for suspicious activity, including “structured” transactions, and to report any transaction or series of transactions in currency of more than \$10,000.

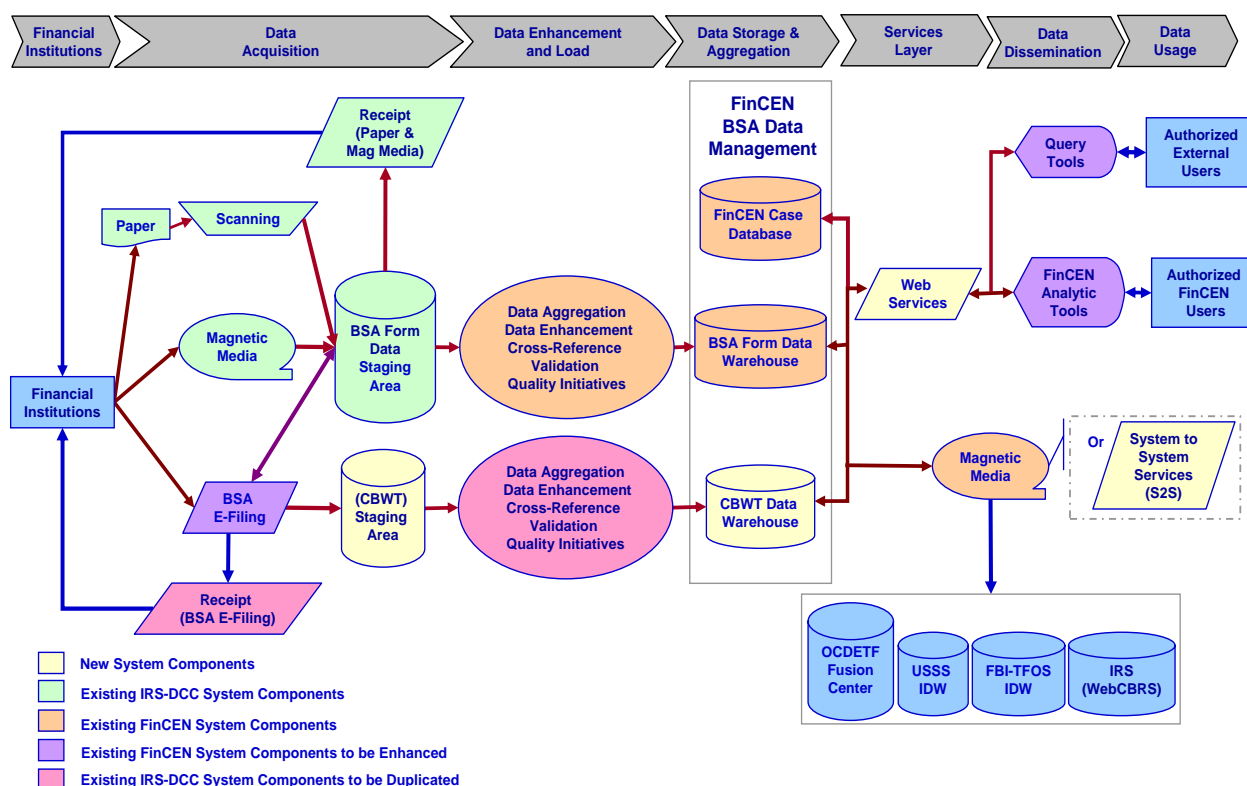
6.0 TECHNOLOGY NEEDED

6.1 Concept of Operations

A federated data warehouse architecture would provide FinCEN with the most flexible approach to integrating cross-border funds transfer data with existing, planned, and unanticipated data sources. (Appendix H contains additional discussion of the alternatives analysis conducted in support of this study). The figure below illustrates, at a very high level, the systems architecture of FinCEN's current data systems.



FinCEN recommends building a separate but integrated channel of data acquisition, processing, and storage of cross-border funds transfer data that would co-exist and integrate with the current BSA reporting. From a user's perspective, a single interface would provide access to the multiple data warehouses. The figure below illustrates, at a very high level, the system architecture we recommend for constructing such a system.



We propose to deploy a new funds transfer data warehouse and operating system in an environment separate from but integrated with existing BSA data. When fully implemented, FinCEN would have two data warehouses. FinCEN would receive the funds transfer data through the BSA E-Filing system but manage it in a separate funds transfer data warehouse environment. The funds transfer data warehouse would be separate from but tightly integrated with the existing BSA data warehouse. Thus, a dedicated system would handle management of the funds transfer reports and provide access to users through an interface that integrates the data with other BSA reports. This approach mirrors and extends the current BSA data collection process. We anticipate that the direct impact on the existing BSA data systems and BSA E-Filing will be minimal.

A federated architecture gives FinCEN the responsibility and power to plan and build smaller customized portals that satisfy the unique needs and requirements of separate user communities over time. This approach permits developers to deploy a generic portal that serves the most common user needs, and then extend the system through development of more advanced or tailored portals. In the end, this approach provides an incremental investment of money and labor, faster initial deployment, and a greater return on investment over the long term. A federated architecture reduces the time and consensus building required in the initial planning stages. In the subsequent deployment of specialized portals, user requirements analysis becomes easier because the user community consists of smaller groups with common needs, project management issues are more

manageable, the users' expectations of the systems' features are more realistic, and the users can more readily recognize clear, tangible benefits of the system.

BSA E-Filing currently is capable of handling large batch filing of BSA reports. FinCEN must enhance the hardware used for the BSA E-Filing system and then increase the dedicated telecommunications bandwidth of the system to accommodate the batch sizes required to submit funds transfer data. The submission of funds transfer data also requires very strict security arrangements. The current digital certificate process built into BSA E-Filing most likely will provide much of the security infrastructure required for transmitting batches of funds transfer data. FinCEN must also carefully reevaluate the current process for obtaining digital certificates to ensure that it does not hinder the increased usage of BSA E-Filing.

The modifications to the BSA E-Filing system necessary in order to accommodate the batch submission of funds transfer include:

- **Separate Submissions for Funds Transfer Reports:** Forms and other functionality to accommodate the separate work stream of funds transfer submissions.
- **Administrative Database Tracking:** FinCEN must modify the Oracle database used by BSA E-Filing for administrative tracking to track the submission of funds transfer batches. Similarly, administrative tracking functions must be adapted so that financial institutions could view a history of the funds transfer batches submitted to FinCEN.
- **Acceptance and Validation of Funds Transfer Batches:** The BSA E-Filing system must incorporate new business rules and procedures to accept batches of funds transfers in an entirely different format.

FinCEN must implement data transformation processes capable of mapping the elements of any such acceptable report formats into a single unified format for storage in its data warehouse. Providing multiple options to institutions with regard to the form of their reports would afford the maximum flexibility to institutions in implementing their own compliance processes. Institutions would be free to make whatever business decisions were appropriate within the limits established in the regulation.

6.2 Rough Order of Magnitude Cost Estimates

Significantly, we conclude that it is not feasible to implement such a system by the December 2007 deadline set out in Section 6302 of the Intelligence Reform Act. Based on a preliminary work breakdown schedule outlining the necessary steps in development, we conclude that deployment of the system described above would require approximately three and one-half years of labor and an

investment of approximately \$32.6 million over that time.²³ (Appendix K contains a more detailed breakdown of the cost estimates).

	Acquisition	Phase One	Phase Two	Sub-Totals
Hardware		\$1,630,392	\$1,324,397	\$2,954,789
Software		\$3,175,015	\$1,227,898	\$4,402,913
Maintenance Cost		\$690,369	\$767,905	\$1,458,274
Contract Service & Support	\$770,000	\$6,274,797	\$14,712,392	\$21,757,189
Other	\$347,710	\$754,110	\$933,660	\$2,035,480
Total	\$1,117,710	\$12,524,683	\$18,966,252	\$32,608,645

23 Note that this figure represents a rough order of magnitude cost estimate and could be revised significantly based upon the results of the proposed pre-acquisition phase and user requirements analysis.

7.0 INFORMATION SECURITY PROTECTIONS

The aggregation and analysis of large collections of data and the development of interconnected information systems designed to facilitate information sharing is revolutionizing the way in which the federal government attacks financial crime. While the benefits have been substantial, these developments pose significant risks to the critical operations of the government and the security of the data contained in these systems. Bank Secrecy Act data is highly sensitive data containing details about the financial activity of private persons. Without proper safeguards, this data could be at risk of inadvertent or deliberate disclosure or misuse and FinCEN's mission could be undermined. These risks generally fall into two closely related categories, the privacy of the personal information contained in government systems, and the risk of system compromise or misuse. A number of federal laws directly control the collection and use of data by government agencies with the aim of protecting the privacy of individual persons – namely, the Right to Financial Privacy Act, the Privacy Act, the Federal Information Security Management Act, and the Bank Secrecy Act itself.

U.S. law has long recognized that a person has no Fourth Amendment privacy interest in the records of his or her transactions maintained at a financial institution. See United States v. Miller, 425 U.S. 435, 442 (1976) (holding that a person has no “expectation of privacy” in his records held by a bank). In response to the holding in Miller, and two other Supreme Court cases issued in the early 1970s – California Bankers Ass’n v. Schultz, 416 U.S. 21 (1974) and Fisher v. United States, 425 U.S. 391 (1974) – which further limited a customer’s ability to challenge government access to records maintained by third parties, Congress enacted the Right to Financial Privacy Act of 1978 (RFPA).²⁴ RFPA is the primary federal statute that protects individual privacy interests in financial records. RFPA generally prohibits a federal government agency from obtaining customer records from a bank unless the customer first receives notice and an opportunity to challenge any such disclosure. The information collected by the proposed cross border funds transfer system, as with any other information required under the Bank Secrecy Act, would fall under the exception to RFPA concerning reports required under federal law. Although RFPA provisions would not apply to this data, other federal laws would.

The Privacy Act of 1974 places limitations on federal government agencies’ collection, disclosure, and use of personal information maintained in those agencies’ systems of records.²⁵ The Privacy Act defines a “record” as any item, collection, or grouping of information about individuals that contains those

²⁴ 12 U.S.C. § 3401 et seq.

²⁵ 5 U.S.C. § 552a

persons' names or other personal identifiers.²⁶ The Privacy Act requires that when agencies establish or make changes to a system of records, they must notify the public by a notice published in the Federal Register identifying the type of information collected, the types of persons about whom the data is collected, and the intended use of the information. Generally, a federal government agency may not disclose a record contained in a system of records without the prior consent of the individual to whom the record pertains, unless the disclosure would fall within a published routine use.²⁷ Cross border funds transfer data reported to FinCEN under the authority of the Bank Secrecy Act would fall within this system of records. Examples of routine uses of Bank Secrecy Act data include disclosures to agencies responsible for investigating and prosecuting civil or criminal violations of law, and to intelligence agencies in the conduct of intelligence to protect against international terrorism.

The Federal Information Security Management Act of 2002 (FISMA)²⁸ requires each federal government agency (including those operating national security systems) to develop, document and implement an agency wide information security program that includes:

- Periodic assessments of the risk and harm that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of data or information systems;
- Risk-based policies and procedures to reduce those risks to acceptable levels and ensure that information security is addressed throughout the life cycle of the agency's information systems;
- Plans for implementation of adequate information security for networks, facilities and systems;
- Security awareness training for agency personnel, including contractors and external users of the information systems;
- Periodic testing (at least annually) and evaluation of the information security policies, procedures, and practices in place within the agency;
- Procedures for detecting, reporting, and responding to security incidents; and
- An annual independent evaluation of its information security program and practices.

²⁶ 5 U.S.C. § 552a(a)(5)

²⁷ The routine uses for Bank Secrecy Act data are set forth at 70 Fed. Reg. 45756, 45760 (August 8, 2005) (Bank Secrecy Act Reports System—Treasury/FinCEN .003).

²⁸ Federal Information Security Management Act of 2002, Title III, E-Government Act of 2002, Pub.L.No. 107-347, Dec. 17, 2002.

FISMA also requires the National Institute of Standards and Technology (NIST) to develop standards and guidelines for all federal government agencies' non-national security systems related to: (1) categorization of their data and information systems based on risk level and security requirements; (2) the types of data and information systems that fit within each category; and, (3) minimum information security requirements for data and information systems in each category.

In turn, the Office of Management and Budget has established performance measures in each of the following areas:

- Certification and accreditation;
- Testing of security controls;
- Agency systems and contractor operations or facility reviews;
- Annual security awareness training for employees;
- Minimum security configuration requirements; and
- Incident reporting

Lastly, the E-Government Act of 2002 provides a further protection for personal information in government data systems, by requiring that agencies conduct “privacy impact assessments” prior to procuring or developing such systems.²⁹ A privacy impact assessment is:

An analysis of how information is handled: (i) to ensure handling conforms to applicable legal regulatory, and policy requirements regarding privacy; (ii) to determine the risks and effects of collecting, maintaining, and disseminating information in identifiable form in an electronic information system; and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.³⁰

FinCEN has developed policies and procedures for compliance with these requirements in accordance with the Department of the Treasury's Information Technology Security Program Directive. Compliance with these government-wide and department-wide standards ensures that FinCEN designs and operates its information systems in accordance with government best practices for the maintenance and dissemination of sensitive data. In developing a system for the collection, storage, analysis, and sharing of cross-border electronic funds transfer reports, FinCEN will incorporate compliance with these standards into every phase of the design and implementation of the system.

²⁹ E-Government Act of 2002, Pub.L.No. 107-347, section 208, (Dec. 17, 2002).

³⁰ Office of Management and Budget, Memorandum M-03-22, Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Washington, D.C., Sept. 26, 2003).

FinCEN is particularly well suited to protect and steward the data, given the strict limits the Bank Secrecy Act imposes on the use and dissemination of data collected under its authority. Pursuant to 31 U.S.C. § 5319, FinCEN must make Bank Secrecy Act data available to other agencies for uses consistent with the stated purposes set forth in 31 U.S.C. § 5311 (i.e., to require reports or records that “have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities to protect against international terrorism”). The Bank Secrecy Act protects the privacy of individuals by making a wrongful disclosure or unauthorized use of a suspicious activity report subject to a criminal penalty of up to five years imprisonment.

FinCEN has more than fifteen years’ experience in handling sensitive financial information about persons through the reporting it currently receives from financial institutions in the United States. FinCEN imposes strict limits on the use and re-dissemination of the data it provides to its law enforcement, regulatory, and foreign counterparts and strictly monitors those persons and organizations to which it grants access to the data. For example, all FinCEN employees and contractors that have access to BSA data are subject to rigorous background investigations. Likewise, external users have access to BSA data only under the terms of Memoranda of Understanding (MOU) between FinCEN and the users’ agency. Those MOUs require that the agencies conduct similar background investigations of all users within the agency, implement specific physical and technological security measures to protect the computers they use to access BSA data, and permit FinCEN to conduct electronic and on-site audits of their use of the data and the safeguards and procedures in place within the agency. Finally, all users of BSA data must agree to the terms of FinCEN’s “BSA Re-Dissemination Guidelines,” which spell out in detail the terms under which a user may share the BSA data they obtain with others. If collected, cross-border funds transfer data would be technologically protected and secure and would be available only to law enforcement and regulatory agencies authorized by law to access it. Finally, FinCEN has created a position within its Office of Information and Technology to advise the Chief Information Officer regarding privacy issues implicated by the collection of BSA information. This official will advise the CIO on the development and implementation of information technology to help ensure that Bank Secrecy Act and related data and records are collected, transmitted, maintained and utilized only for authorized purposes and that the privacy interests of those persons subject to BSA reporting are considered. In addition, the official will recommend policies, technology, and processes for preventing the purposeful or unintended disclosure or other misuse of information about individuals or organizations.

A further consideration stemming from the cross border nature of the funds transfers at issue is the potential relevance of privacy laws of foreign jurisdictions or other provisions regarding the uses of electronically stored data

and its flow between countries. For example, initiatives within the European Union recommend limits on the collection of data, limitations on the use of data based on relevance and the purpose for which the data was initially collected, reasonable security safeguards, and prohibitions on disclosure without the subject's consent or authorization. Some of these initiatives provide that member countries should permit the transmission of data to other countries only if the receiving country has implemented controls on the use of the data that are consistent with the principles of those EU initiatives. The EU initiatives apparently apply only to "personal data," defined as any information relating to an identified or identifiable *natural* person. To date, legislation in member countries implementing these initiatives generally has not extended the term "personal data" to include corporate data or business records such as funds transfer instructions. In addition, a substantial proportion of electronic funds transfer messages relate to the activity of corporations and other artificial entities rather than individuals. Should the Treasury Department implement a cross-border funds transfer reporting requirement, other countries' privacy restrictions could affect the usefulness of the data for money laundering analysis to the extent they served to limit the receipt of information other than as necessary to carry out the funds transfer.

The problem is not limited, however, to purely legal issues. A high level of confidentiality of banking services can be very lucrative for both financial institutions and their host countries. Whereas the U.S. government can and has taken steps to require that certain information be included in electronic payment messages, foreign institutions may hesitate to provide detailed information in funds transfer instructions and are beyond the reach of U.S. law. To require that U.S. banks reject any funds transfer instruction that does not include the elements required under U.S. law could significantly disadvantage U.S. institutions in the international financial system.

Foreign institutions that provide such confidentiality would present two problems for an electronic funds transfer reporting initiative. First, they would undermine the value of electronic funds transfers reporting in the United States by limiting the available information related to funds transfers entering the U.S. Second, the institutions that provide such confidentiality compete in the marketplace with U.S.-based banks. This increases the cost of compliance to U.S. institutions in a way, by making these other institutions more attractive to certain customers who seek anonymity.

The U.S. and other members of the Financial Action Task Force (FATF)³¹ have attempted to address these issues in a global context by adopting international

31 FATF is an inter-governmental policy-making body created in 1989 whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FATF works to generate the necessary political will to bring about legislative and regulatory reforms in these areas. The FATF has published the Forty Plus Nine Recommendations in order to meet this objective. See <http://www.fatf-gafi.org>.

“best practice” standards. For instance, FATF Special Recommendation VII, and the interpretive note thereto, requires countries to mandate that cross-border funds transfers of more than the specified threshold contain accurate and meaningful originator information, and that such information is immediately available to appropriate law enforcement, FIUs, and the beneficiary’s financial institution.

The originator information required to be included in cross-border funds transfers by the Interpretive Note to SR VII includes:

- Name of the Originator
- Location of the Account
- Account number, if one exists, or a unique reference number; and
- Address of the Originator, or national identity number, customer identification number, or date or place of birth if the country permits.

The interpretive note to Special Recommendation VII also states that there is value in nations requiring all incoming cross-border funds transfers to contain full and accurate originator information regardless of the value of the transfer.

Special Recommendation VII further requires that countries take measures to ensure that financial institutions conduct enhanced scrutiny of and monitor for suspicious activity funds transfers that do not contain complete originator information. The provisions of Special Recommendation VII and the BSA travel rule are illustrative of a global movement to promote transparency in the international financial system. As this movement matures, the value of electronic funds transfer data will likewise increase.

Of course, there are general concerns about government agencies having access to large collections of data related to the activity of individual persons. A discussion of these issues should begin with the nature of the data itself, the context in which it is collected, and the standards for its use and dissemination. In this case, any reporting requirement would collect only information already obtained and maintained by financial institutions and already available to the government -- albeit through cumbersome and sometimes inefficient processes -- and would be used largely for the same purposes to which it is currently put on a very limited scale. Such information is far more limited in scope than that collected in other BSA reports. In the context of the Bank Secrecy Act regime, such data adds an additional layer of transparency to the U.S. financial system, holding the promise to enhance both deterrence and detection of illicit financial activity. Dissemination of the data, as with all other BSA data, is subject to strict controls based on the data’s value to legitimate efforts to combat illicit financing undertaken by those with appropriate legal authority. Federal law

and court precedent establish that such information is appropriate to these tasks and provides the authority to obtain and use it. Thus, the primary question becomes whether this move toward more efficient and intelligent use of the information significantly alters the balance between government efforts to protect the nation and its financial system and individual privacy.

8.0 CONCLUSIONS AND RECOMMENDATIONS

8.1 Project Risks

There are a number of significant challenges facing the development and implementation of cross-border electronic funds transfer reporting in the United States. On a technical level, development of information technology systems capable of receiving, storing, analyzing, and disseminating an estimated 350-500 million records a year is a daunting task. In the regulatory context, developing a clear definition of what actually constitutes a cross-border electronic funds transfer is also difficult. Certain kinds of cross-border funds transfers traverse the United States without involving any U.S.-based sender or recipient, and the collection of such information implicates serious policy issues related to the privacy of data regarding both U.S. persons and non-U.S. persons, as well as the role of the U.S. dollar in the international economy. In addition, imposing yet another compliance cost on the U.S. financial services industry requires careful consideration of financial institutions' ability to implement compliance processes and the impact that might have on industry operations and the costs to customers. Last, but not least, any data collection and analysis effort such as the one contemplated by the Intelligence Reform Act also implicates personal privacy concerns. Properly maintaining and securing the data from unauthorized access, as well as managing the appropriate and intelligent use of the data, are paramount.

Technical Issues

The technical alternatives for the receipt, storage, analysis, and dissemination of the data described in this study presume an electronic reporting system that could receive data in standardized formats, normalize the data, and load it into a data warehouse. The technology for implementing this type of communication between the financial institutions and FinCEN already exists, and FinCEN has already implemented it in the BSA E-Filing system.

Section 361 of the USA PATRIOT Act specifies that FinCEN must establish and “maintain a government-wide data access service, with access to . . . information collected by the Department of the Treasury, including report information . . . (such as reports on cash transactions, foreign financial agency transactions and relationships, foreign currency transactions, exporting and importing monetary instruments, and suspicious activities). . . .” To fulfill its mandate under the USA PATRIOT Act, FinCEN must provide a powerful data warehouse and communication infrastructure that permits external users to access and analyze the BSA data in meaningful ways. The anticipated volume of cross-border electronic funds transfer reporting makes this a difficult task.

Any reporting system should leverage existing technology and integrate the various collections of data maintained by FinCEN. The proposed system would require:

- Integration with and enhancement of the BSA E-Filing system currently utilized or in development by FinCEN for the receipt of Bank Secrecy Act data.
- Processing, integrating and enhancement of data submitted by filers, which will share many common data elements, but may be in multiple formats and data structures, to create a uniform data structure.
- Storage of 2-3 years (going forward, not retroactive) worth of cross-border funds transfer data for online access with up to 7-8 additional years' data archived and accessible through other means.
- Integration with other databases including BSA data accessible to external users through a secure web-based interface.
- High-performance and high-availability system with 24/7/365 support, including maintenance, support and help desk services.
- Audit trail capability to track connections to and submissions to the databases, and to provide receipt acknowledgements for data submissions by users.
- Compliance with applicable industry and government standards and security measures appropriate to the handling of Sensitive but Unclassified (SBU) data for the use of Law Enforcement and Regulatory organizations.

These issues highlight the need to conduct a detailed requirements analysis and system design process prior to development. Below we propose an incremental approach to conducting such an analysis and planning for future development.

Regulatory Approach

The definition of “cross-border electronic transmittal of funds” lies at the heart of a successful implementation of the reporting requirement. The nature of the electronic funds transfer process as it has evolved in the United States poses specific difficulties in creating a definition that at once captures all of the nuances of the payment systems and avoids needless complexity.

Further, the regulation must also provide a clear definition of what types of electronic funds transfers an institution must report, and what particular information it should report about each transfer. For the purposes of our study, we have focused on electronic “funds transfers” as defined in 31 C.F.R. § 103.11 in which a U.S. institution sends or receives a payment instruction directing the

transfer of funds to or from an account domiciled outside the U.S.³² Refining an appropriate regulatory definition of what transactions fall within the new reporting requirement will implicate a number of concerns that we identify below.

Institutional Costs

U.S. financial institutions already comply with a wide array of reporting and record-keeping obligations under the Bank Secrecy Act. In the event that the Treasury Department imposes such a reporting requirement, relatively few and mostly large institutions would need to modify the information technology they currently employ and assign staff to manage the implementation process. Institutions would need to train staff in the use and maintenance of the system and the details of the reporting procedures. Some institutions may need or choose to rely on third-party vendors to provide the necessary tools or modifications to their systems. Many vendors currently provide financial institutions with technology to assist them in complying with Bank Secrecy Act regulations. It is possible, if not likely, that the vendors would expand their services to offer the service of extracting the appropriate funds transfer data and reporting that data to FinCEN on behalf of customer institutions. Whether done internally or through outsourcing, reporting institutions will incur some additional costs.

It is very difficult to estimate the costs of compliance with precision, and we have been unable to quantify the costs to U.S. financial institutions. Coordination of the flow of information presents a number of challenges in implementing the proposed system. U.S. financial institutions process and record funds transfers in myriad ways. The development of business processes within U.S. financial institutions to extract the required data from whatever systems they use and transform it into properly formatted reports may be necessary. Any new reporting requirement must necessarily include a reasonable amount of time in which institutions can develop and implement their compliance processes.

Privacy and Confidentiality

Throughout the conduct of this study, many have raised concerns about privacy and the security of personally identifiable and sensitive data about persons' financial transactions. FinCEN has always taken seriously the importance of safeguarding the financial data it collects. Nonetheless, as previously discussed, a system such as the one contemplated in this report raises important questions about the collection of a very large set of private information about persons within and outside the United States without any indicia of suspicious

32 Section 6302 contemplates a reporting requirement that is coextensive with the scope of the BSA funds transfer rule (31 C.F.R. § 103.33). Accordingly, this study does not address any debit card type of transmittals, point-of-sale (POS) systems, transaction conducted through an Automated Clearing House (ACH) process, or Automated Teller Machine (ATM).

activity. Policymakers must weigh the potential value of the data in supporting government efforts to safeguard the financial system from abuse and to deter, detect, and prevent illicit financing carefully against these concerns.

The privacy issues raised by the proposed system should turn primarily on the specific content of the reports proposed and the integration of those reports with other data sets and not on the volume of the reporting. The amount of information in a funds transfer message is limited, far more so than the data already collected by FinCEN through its Suspicious Activity Reports, Currency Transaction Reports, and Currency and Monetary Instrument Reports. In addition, the proposed reporting requirement would not establish a new source of information. Funds transfer data, whether domestic or cross-border is already available to the government but can be difficult to obtain and analyze (see appendix F). Rather, the proposed requirement is an administrative change that would permit investigators and analysts to access and employ data already available in a more effective way.

In addition to the concerns about personal privacy, there are practical, technical concerns regarding the prevention of unauthorized access to data by network intruders, particularly in light of the types of personal and business information contained in funds transfer data. FinCEN is sensitive to these concerns, and practiced in minimizing such risk. FinCEN stands between financial institutions and law enforcement, balancing regulatory costs and privacy concerns against the important value gained by law enforcement access to financial information. As with the current Bank Secrecy Act reports, FinCEN plays an important role as an intermediary between the sensitive information and unfettered or inappropriate access by law enforcement.

8.2 Pre-Acquisition Planning

In its response to FinCEN's March 2006 survey, the American Bankers Association "proposes for discussion whether piloting a single channel specific reporting requirement and then evaluating what has been achieved from a law enforcement perspective for what cost from an economic and privacy basis, isn't a preferred alternative to attempting to implement a comprehensive definition-and-exception driven cross-border, cross-system regime." We believe that there is some value to a phased implementation of a cross-border funds transfer reporting system.

Building on the ABA's suggestion, we propose a multi-phase development process. The pre-acquisition phase of the process would involve three parallel efforts.

8.2.1 User Requirements Analysis

First, FinCEN would engage with its partners in the law enforcement, regulatory and intelligence communities to develop detailed user requirements. This effort would focus on determining the functionality required to meet the most central needs of those who access BSA data.

8.2.2 Institutional Cost Analysis

Second, FinCEN proposes to engage in a detailed discussion with representatives of the U.S. financial services industry that would be subject to the proposed requirement, along with representatives of the major payment systems and members of the Canadian and Australian financial services industries.

There is no quantitative data on the labor or cost involved in implementing processes to comply with the proposed requirement. We propose that the reporting requirement should fall upon a relatively small segment of the financial services industry, and primarily upon large institutions with correspondingly more substantial resources. We recommend that, as part of the planning and requirements analysis phase of development, FinCEN engage in detailed discussions with representatives of industry, particularly with officials familiar with and responsible for the operation of funds transfer systems within U.S. financial institutions, to determine the specific needs of industry members. This exchange also should involve, to the extent possible, representatives from the major payment systems and institutions doing business in Australia and Canada.

These discussions would focus on quantifying the cost the proposed requirement would impose on reporting institutions and the potential impact on the day-to-day operation of the payment systems. In turn, the outcome of these discussions would lead to exploration of means to minimize or avert these impacts.

8.2.3 Value Analysis

Third, FinCEN would engage outside support in obtaining and analyzing a large collection of funds transfer data and exploring means of extracting value from the data. This effort would require correlating funds transfer data with BSA data to validate conclusions contained in this report and to identify means of effectively and intelligently using the funds transfer data to advance efforts to combat money laundering and illicit finance. Based on its own experience and that of other users of BSA data, FinCEN is convinced of the analytical value of funds transfer data (see Appendix F). Once FinCEN identifies and tests potential analytical techniques for employing the funds transfer data, however, it can select those techniques that best combine acceptable costs, reasonable analytical value, and realistic resource requirements. That process will drive the system design process.

All three of these efforts would provide vital information required to develop detailed requirements for the proposed regulation and technological system. If any of these efforts were to reveal insurmountable obstacles to the project, this multi-faceted pre-acquisition effort provides the opportunity to halt the effort before FinCEN or the U.S. financial services industry incur significant development and implementation costs. In fact, this approach would provide such answers prior to the issuance of a contract for development of the technological systems. In other words, this approach provides a clear decision point at which FinCEN or policy makers may terminate the effort if appropriate.

8.3 System Development and Deployment

Based on the above-described pre-acquisition efforts, FinCEN will create a development plan that incorporates a series of milestones that would permit pilot testing of different aspects of the reporting system. Key components of the system development that would benefit from such pilot testing are the data acquisition component (modification of BSA E-Filing), the ETL process, and the data analysis component. FinCEN would divide the development of the data acquisition component into phases that address batch delivery of SWIFT messages, batch delivery of non-SWIFT messages, manual upload of prepared reports, and online completion of reporting forms. The development of the Enhancement, Transformation, and Load (ETL) process would parallel these same phases, addressing the processing of the various reporting forms. This type of collaborative, incremental development approach would enable FinCEN to build the system in manageable stages and to test the system's functionality at each stage before moving on to the next. The results of these different stages of development would provide vital experience and lessons that would assist in the creation of appropriate final regulations, including clear definitions of which transfers U.S. financial institutions would need to report and the creation of appropriate and practical exclusions from the reporting requirement, if any.

APPENDIX A – FINANCIAL CRIMES ENFORCEMENT NETWORK PROGRAMS

The Department of the Treasury established the Financial Crimes Enforcement Network in April 1990.³³ FinCEN's original mission was to establish a government-wide multi-source financial intelligence and analysis network to support the detection, investigation, and prosecution of domestic and international money laundering and other financial crimes. In 1994, FinCEN's mission expanded to include regulatory responsibilities. The USA PATRIOT Act of 2001 established FinCEN as a Bureau within the Treasury Department to support law enforcement efforts and foster interagency and global cooperation against domestic and international financial crimes, and to provide U.S. policy makers with strategic analyses of domestic and worldwide trends and patterns.³⁴ FinCEN works toward those ends through information collection, analysis, and sharing, as well as technological assistance and innovative, cost-effective implementation of the Bank Secrecy Act. On March 8, 2004, FinCEN became a part of the Department of the Treasury's Office of Terrorism and Financial Intelligence, the lead office in the Treasury Department for fighting the financial war on terror, combating financial crime, and enforcing economic sanctions against rogue nations.

The Bank Secrecy Act is the nation's first and most comprehensive federal anti-money laundering statute. Since its enactment in 1970, Congress has amended the Act several times to improve and enhance information collection. The Bank Secrecy Act authorizes the Secretary of the Treasury to issue regulations requiring banks and other financial institutions to keep records and file reports on certain financial transactions determined to have a high degree of usefulness in criminal, tax, regulatory investigations and proceedings, and certain intelligence and counterterrorism matters. The authority of the Secretary to administer Title II of the Bank Secrecy Act (codified at 31 U.S.C. 5311-5330 with implementing regulations at 31 C.F.R. Part 103) has been delegated to the Director of the Financial Crimes Enforcement Network.

FinCEN is charged first and foremost with safeguarding the financial system of the United States from abuse by criminals and terrorists. FinCEN works to accomplish its mission through:

- Administration of the Bank Secrecy Act - a regulatory regime that provides for the reporting of highly sensitive financial data that are critical to investigations of financial crime;

³³ Treasury Order Number 105-08 (Apr. 25, 1990).

³⁴ Pub. L. No. 107-56, Title III, Subtitle B, Section 361(a)(2), 115 Stat. 272, 329-332. See Treasury Order 180-01 (Sept. 26, 2002).

- Dissemination of the data reported under the Bank Secrecy Act to law enforcement and, under appropriate circumstances, the intelligence community;
- Analysis of information related to illicit finance - both strategic and tactical analysis; and
- Education and outreach provided to law enforcement and the financial industry on issues relating to illicit finance.

In carrying out this mission, FinCEN serves many complementary roles:

- FinCEN is a regulatory agency. FinCEN administers the Bank Secrecy Act, the principal regulatory statute aimed at addressing the problems of money laundering and other forms of illicit finance, including terrorist financing. FinCEN is responsible for shaping and implementing this regulatory regime and, in concert with the federal functional regulators and the Internal Revenue Service, for ensuring compliance with the regime. The agency also protects the integrity and confidentiality of the information collected under the Bank Secrecy Act.
- FinCEN is a financial intelligence agency. While not a member of the intelligence community, FinCEN is responsible for ensuring the efficient and timely collection, maintenance, analysis, and dissemination of financial information critical to investigations of illicit finance.
- FinCEN is a law enforcement support agency. While FinCEN has no criminal investigative or arrest authority, much of its effort supports the investigation and successful prosecution of financial crime.
- FinCEN is a network. FinCEN does not support one agency or a select group of agencies, but makes its information, products, and services available to all agencies that have a role in investigating illicit finance. FinCEN networks these agencies using technology that identifies when different agencies are searching the same data and facilitates coordination - avoiding investigative overlap and permitting the agencies to leverage resources and information.

From its position within the Treasury Department's Office of Terrorism and Financial Intelligence, FinCEN works to "operationalize" Treasury's policy priorities on these important issues. This coordinated effort contributes to a greater emphasis and understanding of money laundering, terrorist financing, and other forms of illicit finance not only at Treasury, but also throughout the United States Government.

In its role as the administrator of the Bank Secrecy Act, FinCEN:

- Develops and issues regulations to implement the provisions of the BSA and the USA PATRIOT Act;
- Issues interpretive guidance to educate industry about red flags, vulnerabilities, and money laundering and terrorist financing methodologies;
- Conducts outreach and training to regulated industries, regulators, examiners, and law enforcement to improve consistency in the administration and enforcement of the BSA;
- Collects, maintains, and analyzes reports and information filed by financial institutions under the Bank Secrecy Act;
- Disseminates BSA data to law enforcement and regulatory agencies;
- Ensures financial institution compliance with the regulations and consistent application of the regulations across all affected financial services industries; and
- Takes civil enforcement actions in the case of serious non-compliance.

While FinCEN is responsible for ensuring compliance with the Bank Secrecy Act and implementing regulations, FinCEN does not itself examine financial institutions for compliance. Instead, FinCEN has delegated its authority to examine financial institutions for BSA compliance to the primary federal regulators of those financial institutions. FinCEN thereby can leverage the resources and expertise of other Federal agencies and self-regulatory organizations by relying on these agencies to conduct compliance exams. FinCEN has delegated its examination responsibility to the Board of Governors of the Federal Reserve System, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision, the National Credit Union Administration, Securities and Exchange Commission, the Commodity Futures Trading Commission, and the Internal Revenue Service (Small Business/Self-Employed Division).³⁵

FinCEN has an important role in supporting the examination regime created through our delegations. FinCEN's role involves providing prompt Bank Secrecy Act interpretive guidance to regulators, policy makers, and the financial services industry, and ensuring the consistent application of the Bank Secrecy Act regulations across industry lines, most notably through the rule-making process, issuance of guidance, and through FinCEN's Office of Compliance. Through that Office, and pursuant to Memoranda of Understanding executed with FinCEN,

³⁵ See 31 C.F.R. § 103.56(b).

federal agencies to which FinCEN has delegated BSA compliance examination authority periodically provide to FinCEN information related to BSA deficiencies within the institutions they regulate. This information helps FinCEN develop a more accurate picture of compliance in the industry and address compliance issues expeditiously. The information also helps FinCEN fulfill its obligation to administer and to oversee compliance with the BSA, and provides consistency and quality in referrals of potential BSA violations to FinCEN.

At the invitation of the Federal Financial Institutions Examination Council, FinCEN, along with the five Federal banking agencies, has issued interagency Bank Secrecy Act/Anti-Money Laundering examination procedures. These examination procedures emphasize a banking organization's responsibility to establish and implement risk-based policies, procedures, and processes to comply with the BSA and safeguard its operations from money laundering and terrorist financing.

As noted above, FinCEN promotes BSA compliance by all financial institutions through training, education, and outreach. Further, FinCEN supports the examination functions performed by the other agencies by providing them access to information filed by financial institutions and by facilitating cooperation and information sharing among the various financial institution regulators to enhance the effectiveness of Bank Secrecy Act examination and, ultimately, industry compliance.

FinCEN has retained the authority to pursue civil enforcement actions against financial institutions for non-compliance with the Bank Secrecy Act and the implementing regulations. Under the Bank Secrecy Act, FinCEN is empowered to assess civil monetary penalties against, or require corrective action by a financial institution committing negligent or willful violations of the Bank Secrecy Act. Generally, FinCEN identifies potential enforcement cases through: (1) referrals from the agencies examining for Bank Secrecy Act compliance; (2) self-disclosures by financial institutions; and, (3) FinCEN's own inquiry to the extent it becomes aware of possible violations.³⁶

FinCEN's Counter-Terrorism Strategy

An important operational priority for FinCEN is providing counter-terrorism support to law enforcement and the intelligence agencies. FinCEN's comprehensive counter-terrorism strategy draws from its analytic support to law enforcement, regulatory tools and expertise, and international networking capabilities. The strategy has five basic components.

36 It should be noted that under Title 12 of the U.S. Code, the banking regulators have authority to enforce certain regulations that fall under their respective statutes as well as under the Bank Secrecy Act, such as the requirement that depository institutions have anti-money laundering programs. In addition, the Internal Revenue Service has authority to enforce certain Bank Secrecy Act requirements including the IRS/FinCEN Form 8300 reporting for non-financial trades and businesses, and the Report of Foreign Bank and Financial Accounts by individuals and entities.

Analysis of Terrorist Financing Suspicious Activity Reports

FinCEN analyzes suspicious activity reports for both tactical and strategic value. At the tactical level, every report that indicates a connection to terrorism is immediately reviewed and validated and then analyzed with other available information. This information is packaged and referred to the Terrorist Threat Integration Center (TTIC), within FBI's Terrorist Financing Operations Section (TFOS), and other relevant law enforcement agencies. Moreover, this information is stored in a manner that facilitates its access and availability for analysis.

At the strategic level, FinCEN analysts study Bank Secrecy Act data and all other available information to gain an increased understanding of methodologies, typologies, geographic patterns of activity and systemic vulnerabilities relating to terrorist financing. These analysts focus on regional and systemic "hot spots" for terrorist financing, studying and analyzing all sources of information. Such focus can significantly add to the knowledge base of law enforcement.

USA PATRIOT Act Section 311

To safeguard the financial system at home from criminal threats abroad, section 311 of the USA PATRIOT Act authorizes the Secretary of the Treasury to designate foreign financial institutions, jurisdictions, classes of foreign transactions, or types of accounts as being of "primary money laundering concern" and to require U.S. financial institutions to take special measures regarding the designated entities. FinCEN provides analytic, regulatory, and legal resources to support effective implementation of Section 311 by the Treasury Department. FinCEN conducts in-depth analyses, including interagency consultation, and compiles the administrative records to support designations and proposed special measures.

International Cooperation and Information Sharing

FinCEN offers a wide array of information exchange and technical assistance to foreign governments, providing policy recommendations and guidance, analytical training, technological advice, and staff support in order to foster the implementation of anti-money laundering and counter-terrorism financing regimes worldwide. FinCEN works in tandem with other government agencies such as the Departments of State and Justice and the Treasury Department's Office of Technical Assistance in assessing nations' efforts to combat money laundering and terrorism finance, playing a lead role in reporting on countries in the money laundering section of the annual International Narcotics Control Strategy Report. Such assessments serve as a basis for establishing U.S. government priorities in the realm of technical assistance to other nations.

Since June 1995, the U.S. has pursued an aggressive policy of promoting a worldwide network of financial intelligence units in its overall strategy of fighting money laundering and terrorist financing. FinCEN is a founding

member of the Egmont Group of financial intelligence units. The Egmont Group is an international network of 101 countries that have implemented national centers to collect information on suspicious or unusual financial activity from the financial industry, to analyze the data, and to make it available to appropriate national authorities and other financial intelligence units for use in combating terrorist funding and other financial crime. FinCEN, in its FIU capacity, acts as a conduit to process and disseminate requests for information between domestic U.S. law enforcement or regulatory agencies and our counterpart Egmont member FIUs. FinCEN additionally prepares and provides analytical products in response to requests from our counterpart FIUs. The exchange of information is at the heart of the Egmont Group.

Effectively addressing money laundering and terrorist financing requires international cooperation and coordination. FinCEN also supports U.S. bilateral and multilateral efforts to join with other nations in a concerted fashion to combat transnational crime, such as the Financial Action Task Force (FATF),³⁷ as well as FATF-style regional bodies including the Asia/Pacific Group on Money Laundering, Caribbean Financial Action Task Force, Eastern and Southern Africa Anti-Money Laundering Group, Financial Action Task Force for South America, International Group Against Money Laundering,³⁸ and the MONEYVAL Committee of the Council of Europe. FinCEN supports the Department of the Treasury by participating to varying degrees in all of these bodies with the aim of furthering information exchange among members and coordinating training and technical assistance programs.

FinCEN is able to play a unique role in working with other nations interested in establishing FIUs and strengthening ties among existing units. To this end, FinCEN, through its Office of Global Liaison, advises FIUs under development, providing training to FIU personnel on subjects such as suspicious transaction report analysis, charts and graphing, link analysis, money laundering typologies, alternate remittance systems, bank compliance, and other FIU-specific topics.

USA PATRIOT Act Section 314(a) Information Sharing

Section 314(a) of the USA PATRIOT Act of 2001 requires the Secretary of the Treasury to adopt regulations to encourage regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. FinCEN's regulations under Section 314(a)³⁹ enable

37 Formed in 1989 by the G-7 Economic Summit, FATF is dedicated to promoting the development of effective anti-money laundering and counter-terrorism finance laws and programs and enhancing cooperation among its membership and around the world.

38 An organization comprised of West African states under the umbrella of ECOWAS.

39 31 C.F.R. § 103.100.

federal law enforcement agencies to reach out, through FinCEN, to more than 45,000 points of contact at more than 27,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering.

FinCEN receives requests from federal law enforcement and upon review, sends requests to designated contacts within financial institutions across the country once every two weeks via either a secure Internet web site or via facsimile. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records. The financial institutions must query their records for matches, including accounts maintained by the named subject during the preceding twelve months and transactions conducted within the last six months. Financial institutions have two weeks from the transmission date of the request to respond to 314(a) requests. If the institution does not identify any matching accounts or transactions, it need not reply to the 314(a) request.

The 314(a) process enables investigators to canvas financial institutions for potential lead information that they might otherwise never find. This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralized, and evaluated rapidly.

The 314(a) process is not, however, a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has reported a match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents.

To ensure that investigators use the 314(a) process appropriately, FinCEN requires federal law enforcement agencies to submit documentation demonstrating the size or impact of the case, the seriousness of the underlying criminal activity, the importance of the case to a major agency program, and any other facts demonstrating the significance of the case. The requestor also must certify that the investigation arises from credible evidence of terrorist financing or money laundering and, in cases involving money laundering, that all traditional means of investigation have been exhausted.

Regulatory Outreach

FinCEN applies its analytical skills also to provide information to the regulated community to better identify potential vulnerabilities to money laundering and terrorist financing activity. One area of particular focus is money services businesses. Money services businesses continue to require more attention and resources. These operations include small businesses that typically offer money remittance services, check cashing, money orders, stored value products and other informal value transfer systems. Our most recent initiative, an Advance Notice of Proposed Rulemaking issued on March 8, 2006, addresses the issue of access to banking services by money services businesses. This Advance Notice

solicits updated facts and recommendations regarding ongoing concerns about the Bank Secrecy Act, and what additional guidance or regulatory action, if any, would be appropriate to address these concerns. The comments will assist us in determining whether to provide additional guidance to industry and the content of any such guidance.

APPENDIX B – SECTION 6302

INTELLIGENCE REFORM AND TERRORISM PREVENTION ACT OF 2004 PUBLIC LAW NUMBER 108-458

SECTION 6302 REPORTING OF CERTAIN CROSS-BORDER TRANSMITTAL OF FUNDS

Section 5318 of title 31, United States Code, is amended by adding at the end the following new subsection:

(n) Reporting of Certain Cross-Border Transmittals of Funds-

- (1) IN GENERAL- Subject to paragraphs (3) and (4), the Secretary shall prescribe regulations requiring such financial institutions as the Secretary determines to be appropriate to report to the Financial Crimes Enforcement Network certain cross-border electronic transmittals of funds, if the Secretary determines that reporting of such transmittals is reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing.
- (2) LIMITATION ON REPORTING REQUIREMENTS- Information required to be reported by the regulations prescribed under paragraph (1) shall not exceed the information required to be retained by the reporting financial institution pursuant to section 21 of the Federal Deposit Insurance Act and the regulations promulgated thereunder, unless--
 - (A) the Board of Governors of the Federal Reserve System and the Secretary jointly determine that a particular item or items of information are not currently required to be retained under such section or such regulations; and
 - (B) the Secretary determines, after consultation with the Board of Governors of the Federal Reserve System, that the reporting of such information is reasonably necessary to conduct the efforts of the Secretary to identify cross-border money laundering and terrorist financing.
- (3) FORM AND MANNER OF REPORTS- In prescribing the regulations required under paragraph (1), the Secretary shall, subject to paragraph (2), determine the appropriate form, manner, content, and frequency of filing of the required reports.

(4) FEASIBILITY REPORT-

- (A) IN GENERAL- Before prescribing the regulations required under paragraph (1), and as soon as is practicable after the date of enactment of the National Intelligence Reform Act of 2004, the Secretary shall submit a report to the Committee on Banking, Housing, and Urban Affairs of the Senate and the Committee on Financial Services of the House of Representatives that--
- (i) identifies the information in cross-border electronic transmittals of funds that may be found in particular cases to be reasonably necessary to conduct the efforts of the Secretary to identify money laundering and terrorist financing, and outlines the criteria to be used by the Secretary to select the situations in which reporting under this subsection may be required;
 - (ii) outlines the appropriate form, manner, content, and frequency of filing of the reports that may be required under such regulations;
 - (iii) identifies the technology necessary for the Financial Crimes Enforcement Network to receive, keep, exploit, protect the security of, and disseminate information from reports of cross-border electronic transmittals of funds to law enforcement and other entities engaged in efforts against money laundering and terrorist financing; and
 - (iv) discusses the information security protections required by the exercise of the Secretary's authority under this subsection.
- (B) CONSULTATION- In reporting the feasibility report under subparagraph (A), the Secretary may consult with the Bank Secrecy Act Advisory Group established by the Secretary, and any other group considered by the Secretary to be relevant.

(5) REGULATIONS-

- (A) IN GENERAL- Subject to subparagraph (B), the regulations required by paragraph (1) shall be prescribed in final form by the Secretary, in consultation with the Board of Governors of the Federal Reserve System, before the end of the 3-year period beginning on the date of enactment of the National Intelligence Reform Act of 2004.
- (B) TECHNOLOGICAL FEASIBILITY- No regulations shall be prescribed under this subsection before the Secretary certifies to the Congress that the Financial Crimes Enforcement Network has the technological systems in place to effectively and efficiently receive, keep, exploit, protect the security of, and disseminate information from reports of cross-border electronic transmittals of funds to law enforcement and other entities engaged in efforts against money laundering and terrorist financing.

APPENDIX C – FUNDS TRANSFER RULE

§ 103.32

§103.32 Records to be made and retained by persons having financial interests in foreign financial accounts.

Records of accounts required by §103.24 to be reported to the Commissioner of Internal Revenue shall be retained by each person having a financial interest in or signature or other authority over any such account. Such records shall contain the name in which each such account is maintained, the number or other designation of such account, the name and address of the foreign bank or other person with whom such account is maintained, the type of such account, and the maximum value of each such account during the reporting period. Such records shall be retained for a period of 5 years and shall be kept at all times available for inspection as authorized by law. In the computation of the period of 5 years, there shall be disregarded any period beginning with a date on which the taxpayer is indicted or information instituted on account of the filing of a false or fraudulent Federal income tax return or failing to file a Federal income tax return, and ending with the date on which final disposition is made of the criminal proceeding.

[37 FR 6912, Apr. 5, 1972, as amended at 52 FR 11444, Apr. 8, 1987]

§103.33 Records to be made and retained by financial institutions.

Each financial institution shall retain either the original or a microfilm or other copy or reproduction of each of the following:

(a) A record of each extension of credit in an amount in excess of \$10,000, except an extension of credit secured by an interest in real property, which record shall contain the name and address of the person to whom the extension of credit is made, the amount thereof, the nature or purpose thereof, and the date thereof;

(b) A record of each advice, request, or instruction received or given regarding any transaction resulting (or intended to result and later canceled if such a record is normally made) in the transfer of currency or other monetary instruments, funds, checks, investment securities, or credit, of more than

31 CFR Ch. I (7-1-05 Edition)

\$10,000 to or from any person, account, or place outside the United States.

(c) A record of each advice, request, or instruction given to another financial institution or other person located within or without the United States, regarding a transaction intended to result in the transfer of funds, or of currency, other monetary instruments, checks, investment securities, or credit, of more than \$10,000 to a person, account or place outside the United States.

(d) A record of such information for such period of time as the Secretary may require in an order issued under §103.26(a), not to exceed five years.

(e) *Banks.* Each agent, agency, branch, or office located within the United States of a bank is subject to the requirements of this paragraph (e) with respect to a funds transfer in the amount of \$3,000 or more:

(1) *Recordkeeping requirements.* (i) For each payment order that it accepts as an originator's bank, a bank shall obtain and retain either the original or a microfilm, other copy, or electronic record of the following information relating to the payment order:

(A) The name and address of the originator;

(B) The amount of the payment order;

(C) The execution date of the payment order;

(D) Any payment instructions received from the originator with the payment order;

(E) The identity of the beneficiary's bank; and

(F) As many of the following items as are received with the payment order:¹

(1) The name and address of the beneficiary;

(2) The account number of the beneficiary; and

(3) Any other specific identifier of the beneficiary.

(ii) For each payment order that it accepts as an intermediary bank, a

¹For funds transfers effected through the Federal Reserve's Fedwire funds transfer system, only one of the items is required to be retained, if received with the payment order, until such time as the bank that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire message format.

Monetary Offices, Treasury

§ 103.33

bank shall retain either the original or a microfilm, other copy, or electronic record of the payment order.

(iii) For each payment order that it accepts as a beneficiary's bank, a bank shall retain either the original or a microfilm, other copy, or electronic record of the payment order.

(2) *Originators other than established customers.* In the case of a payment order from an originator that is not an established customer, in addition to obtaining and retaining the information required in paragraph (e)(1)(i) of this section:

(i) If the payment order is made in person, prior to acceptance the originator's bank shall verify the identity of the person placing the payment order. If it accepts the payment order, the originator's bank shall obtain and retain a record of the name and address, the type of identification reviewed, the number of the identification document (*e.g.*, driver's license), as well as a record of the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank shall obtain and retain a record of the originator's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

(ii) If the payment order accepted by the originator's bank is not made in person, the originator's bank shall obtain and retain a record of name and address of the person placing the payment order, as well as the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (*e.g.*, check or credit card transaction) for the funds transfer. If the

originator's bank has knowledge that the person placing the payment order is not the originator, the originator's bank shall obtain and retain a record of the originator's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record of the lack thereof.

(3) *Beneficiaries other than established customers.* For each payment order that it accepts as a beneficiary's bank for a beneficiary that is not an established customer, in addition to obtaining and retaining the information required in paragraph (e)(1)(iii) of this section:

(i) If the proceeds are delivered in person to the beneficiary or its representative or agent, the beneficiary's bank shall verify the identity of the person receiving the proceeds and shall obtain and retain a record of the name and address, the type of identification reviewed, and the number of the identification document (*e.g.*, driver's license), as well as a record of the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the beneficiary's bank has knowledge that the person receiving the proceeds is not the beneficiary, the beneficiary's bank shall obtain and retain a record of the beneficiary's name and address, as well as the beneficiary's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person receiving the proceeds, or a notation in the record of the lack thereof.

(ii) If the proceeds are delivered other than in person, the beneficiary's bank shall retain a copy of the check or other instrument used to effect payment, or the information contained thereon, as well as the name and address of the person to which it was sent.

(4) *Retrievability.* The information that an originator's bank must retain under paragraphs (e)(1)(i) and (e)(2) of

§ 103.33

31 CFR Ch. I (7-1-05 Edition)

this section shall be retrievable by the originator's bank by reference to the name of the originator. If the originator is an established customer of the originator's bank and has an account used for funds transfers, then the information also shall be retrievable by account number. The information that a beneficiary's bank must retain under paragraphs (e)(1)(iii) and (e)(3) of this section shall be retrievable by the beneficiary's bank by reference to the name of the beneficiary. If the beneficiary is an established customer of the beneficiary's bank and has an account used for funds transfers, then the information also shall be retrievable by account number. This information need not be retained in any particular manner, so long as the bank is able to retrieve the information required by this paragraph, either by accessing funds transfer records directly or through reference to some other record maintained by the bank.

(5) *Verification.* Where verification is required under paragraphs (e)(2) and (e)(3) of this section, a bank shall verify a person's identity by examination of a document (other than a bank signature card), preferably one that contains the person's name, address, and photograph, that is normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers. Verification of the identity of an individual who indicates that he or she is an alien or is not a resident of the United States may be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a foreign driver's license with indication of home address).

(6) *Exceptions.* The following funds transfers are not subject to the requirements of this section:

(i) Funds transfers where the originator and beneficiary are any of the following:

- (A) A bank;
- (B) A wholly-owned domestic subsidiary of a bank chartered in the United States;
- (C) A broker or dealer in securities;
- (D) A wholly-owned domestic subsidiary of a broker or dealer in securities;

(E) A futures commission merchant or an introducing broker in commodities;

(F) A wholly-owned domestic subsidiary of a futures commission merchant or an introducing broker in commodities;

(G) The United States;

(H) A state or local government; or

(i) A federal, state or local government agency or instrumentality; and

(ii) Funds transfers where both the originator and the beneficiary are the same person and the originator's bank and the beneficiary's bank are the same bank.

(f) *Nonbank financial institutions.* Each agent, agency, branch, or office located within the United States of a financial institution other than a bank is subject to the requirements of this paragraph (f) with respect to a transmittal of funds in the amount of \$3,000 or more:

(1) *Recordkeeping requirements.* (i) For each transmittal order that it accepts as a transmittor's financial institution, a financial institution shall obtain and retain either the original or a microfilm, other copy, or electronic record of the following information relating to the transmittal order:

(A) The name and address of the transmittor;

(B) The amount of the transmittal order;

(C) The execution date of the transmittal order;

(D) Any payment instructions received from the transmittor with the transmittal order;

(E) The identity of the recipient's financial institution;

(F) As many of the following items as are received with the transmittal order;²

(1) The name and address of the recipient;

(2) The account number of the recipient; and

²For transmittals of funds effected through the Federal Reserve's Fedwire funds transfer system by a domestic broker or dealers in securities, only one of the items is required to be retained, if received with the transmittal order, until such time as the bank that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire message format.

Monetary Offices, Treasury

§ 103.33

(3) Any other specific identifier of the recipient; and

(C) Any form relating to the transmittal of funds that is completed or signed by the person placing the transmittal order.

(ii) For each transmittal order that it accepts as an intermediary financial institution, a financial institution shall retain either the original or a microfilm, other copy, or electronic record of the transmittal order.

(iii) For each transmittal order that it accepts as a recipient's financial institution, a financial institution shall retain either the original or a microfilm, other copy, or electronic record of the transmittal order.

(2) *Transmitters other than established customers.* In the case of a transmittal order from a transmitter that is not an established customer, in addition to obtaining and retaining the information required in paragraph (f)(1)(i) of this section:

(i) If the transmittal order is made in person, prior to acceptance the transmitter's financial institution shall verify the identity of the person placing the transmittal order. If it accepts the transmittal order, the transmitter's financial institution shall obtain and retain a record of the name and address, the type of identification reviewed, and the number of the identification document (*e.g.*, driver's license), as well as a record of the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record the lack thereof. If the transmitter's financial institution has knowledge that the person placing the transmittal order is not the transmitter, the transmitter's financial institution shall obtain and retain a record of the transmitter's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record the lack thereof.

(ii) If the transmittal order accepted by the transmitter's financial institution is not made in person, the

transmitter's financial institution shall obtain and retain a record of the name and address of the person placing the transmittal order, as well as the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof, and a copy or record of the method of payment (*e.g.*, check or credit card transaction) for the transmittal of funds. If the transmitter's financial institution has knowledge that the person placing the transmittal order is not the transmitter, the transmitter's financial institution shall obtain and retain a record of the transmitter's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, if known by the person placing the order, or a notation in the record the lack thereof.

(3) *Recipients other than established customers.* For each transmittal order that it accepts as a recipient's financial institution for a recipient that is not an established customer, in addition to obtaining and retaining the information required in paragraph (f)(1)(iii) of this section:

(i) If the proceeds are delivered in person to the recipient or its representative or agent, the recipient's financial institution shall verify the identity of the person receiving the proceeds and shall obtain and retain a record of the name and address, the type of identification reviewed, and the number of the identification document (*e.g.*, driver's license), as well as a record of the person's taxpayer identification number (*e.g.*, social security or employer identification number) or, if none, alien identification number or passport number and country of issuance, or a notation in the record of the lack thereof. If the recipient's financial institution has knowledge that the person receiving the proceeds is not the recipient, the recipient's financial institution shall obtain and retain a record of the recipient's name and address, as well as the recipient's taxpayer identification number (*e.g.*, social security or employer identification

§ 103.33

31 CFR Ch. I (7-1-05 Edition)

number) or, if none, alien identification number or passport number and country of issuance, if known by the person receiving the proceeds, or a notation in the record of the lack thereof.

(ii) If the proceeds are delivered other than in person, the recipient's financial institution shall retain a copy of the check or other instrument used to effect payment, or the information contained thereon, as well as the name and address of the person to which it was sent.

(4) *Retrievability.* The information that a transmitter's financial institution must retain under paragraphs (f)(1)(i) and (f)(2) of this section shall be retrievable by the transmitter's financial institution by reference to the name of the transmitter. If the transmitter is an established customer of the transmitter's financial institution and has an account used for transmittals of funds, then the information also shall be retrievable by account number. The information that a recipient's financial institution must retain under paragraphs (f)(1)(iii) and (f)(3) of this section shall be retrievable by the recipient's financial institution by reference to the name of the recipient. If the recipient is an established customer of the recipient's financial institution and has an account used for transmittals of funds, then the information also shall be retrievable by account number. This information need not be retained in any particular manner, so long as the financial institution is able to retrieve the information required by this paragraph, either by accessing transmittal of funds records directly or through reference to some other record maintained by the financial institution.

(5) *Verification.* Where verification is required under paragraphs (f)(2) and (f)(3) of this section, a financial institution shall verify a person's identity by examination of a document (other than a customer signature card), preferably one that contains the person's name, address, and photograph, that is normally acceptable by financial institutions as a means of identification when cashing checks for persons other than established customers. Verification of the identity of an individual who indicates that he or she is

an alien or is not a resident of the United States may be made by passport, alien identification card, or other official document evidencing nationality or residence (e.g., a foreign driver's license with indication of home address).

(6) *Exceptions.* The following transmittals of funds are not subject to the requirements of this section:

(i) Transmittals of funds where the transmitter and the recipient are any of the following:

- (A) A bank;
- (B) A wholly-owned domestic subsidiary of a bank chartered in the United States;
- (C) A broker or dealer in securities;
- (D) A wholly-owned domestic subsidiary of a broker or dealer in securities;
- (E) A futures commission merchant or an introducing broker in commodities;
- (F) A wholly-owned domestic subsidiary of a futures commission merchant or an introducing broker in commodities;

- (G) The United States;
- (H) A state or local government; or
- (I) A federal, state or local government agency or instrumentality; and

(ii) Transmittals of funds where both the transmitter and the recipient are the same person and the transmitter's financial institution and the recipient's financial institution are the same broker or dealer in securities.

(g) Any transmitter's financial institution or intermediary financial institution located within the United States shall include in any transmittal order for a transmittal of funds in the amount of \$3,000 or more, information as required in this paragraph (g):

(i) A transmitter's financial institution shall include in a transmittal order, at the time it is sent to a receiving financial institution, the following information:

(i) The name and, if the payment is ordered from an account, the account number of the transmitter;

(ii) The address of the transmitter, except for a transmittal order through Fedwire until such time as the bank that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire format;

Monetary Offices, Treasury

§ 103.33

(iii) The amount of the transmittal order;
 (iv) The execution date of the transmittal order;
 (v) The identity of the recipient's financial institution;
 (vi) As many of the following items as are received with the transmittal order:³

(A) The name and address of the recipient;

(B) The account number of the recipient;

(C) Any other specific identifier of the recipient; and

(vii) Either the name and address or numerical identifier of the transmittor's financial institution.

(2) A receiving financial institution that acts as an intermediary financial institution, if it accepts a transmittal order, shall include in a corresponding transmittal order at the time it is sent to the next receiving financial institution, the following information, if received from the sender:

(i) The name and the account number of the transmittor;

(ii) The address of the transmittor, except for a transmittal order through Fedwire until such time as the bank that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire format;

(iii) The amount of the transmittal order;

(iv) The execution date of the transmittal order;

(v) The identity of the recipient's financial institution;

(vi) As many of the following items as are received with the transmittal order:⁴

³For transmittals of funds effected through the Federal Reserve's Fedwire funds transfer system by a financial institution, only one of the items is required to be included in the transmittal order, if received with the sender's transmittal order, until such time as the bank that sends the order to the Federal Reserve Bank completes its conversion to the expanded Fedwire message format.

⁴For transmittals of funds effected through the Federal Reserve's Fedwire funds transfer system by a financial institution, only one of the items is required to be included in the transmittal order, if received with the sender's transmittal order, until such time as the bank that sends the order

(A) The name and address of the recipient;

(B) The account number of the recipient;

(C) Any other specific identifier of the recipient; and

(vii) Either the name and address or numerical identifier of the transmittor's financial institution.

(3) *Safe harbor for transmittals of funds prior to conversion to the expanded Fedwire message format.* The following provisions apply to transmittals of funds effected through the Federal Reserve's Fedwire funds transfer system or otherwise by a financial institution before the bank that sends the order to the Federal Reserve Bank or otherwise completes its conversion to the expanded Fedwire message format.

(i) *Transmittor's financial institution.* A transmittor's financial institution will be deemed to be in compliance with the provisions of paragraph (g)(1) of this section if it:

(A) Includes in the transmittal order, at the time it is sent to the receiving financial institution, the information specified in paragraphs (g)(1)(i) through (v), and the information specified in paragraph (g)(1)(vi) of this section to the extent that such information has been received by the financial institution, and

(B) Provides the information specified in paragraphs (g)(1)(i), (ii) and (vii) of this section to a financial institution that acted as an intermediary financial institution or recipient's financial institution in connection with the transmittal order, within a reasonable time after any such financial institution makes a request therefor in connection with the requesting financial institution's receipt of a lawful request for such information from a federal, state, or local law enforcement or financial regulatory agency, or in connection with the requesting financial institution's own Bank Secrecy Act compliance program.

(ii) *Intermediary financial institution.* An intermediary financial institution will be deemed to be in compliance

to the Federal Reserve Bank completes its conversion to the expanded Fedwire message format.

§ 103.34

31 CFR Ch. I (7-1-05 Edition)

with the provisions of paragraph (g)(2) of this section if it:

(A) Includes in the transmittal order, at the time it is sent to the receiving financial institution, the information specified in paragraphs (g)(2)(iii) through (g)(2)(vi) of this section, to the extent that such information has been received by the intermediary financial institution; and

(B) Provides the information specified in paragraphs (g)(2)(i), (ii) and (vii) of this section, to the extent that such information has been received by the intermediary financial institution, to a financial institution that acted as an intermediary financial institution or recipient's financial institution in connection with the transmittal order, within a reasonable time after any such financial institution makes a request therefor in connection with the requesting financial institution's receipt of a lawful request for such information from a federal, state, or local law enforcement or regulatory agency, or in connection with the requesting financial institution's own Bank Secrecy Act compliance program.

(iii) *Obligation of requesting financial institution.* Any information requested under paragraph (g)(3)(i)(B) or (g)(3)(ii)(B) of this section shall be treated by the requesting institution, once received, as if it had been included in the transmittal order to which such information relates.

(4) *Exceptions.* The requirements of this paragraph (g) shall not apply to transmittals of funds that are listed in paragraph (e)(6) or (f)(6) of this section.

(Approved by the Office of Management and Budget under control number 1505-0063)

[37 FR 6912, Apr. 5, 1972, as amended at 52 FR 11444, Apr. 8, 1987; 54 FR 33679, Aug. 16, 1989; 60 FR 229, 238, Jan. 3, 1995; 61 FR 14385, 14388, Apr. 1, 1996; 61 FR 18250, Apr. 25, 1996; 68 FR 65399, Nov. 20, 2003]

§ 103.34 Additional records to be made and retained by banks.

(a)(1) With respect to each certificate of deposit sold or redeemed after May 31, 1978, and before October 1, 2003, or each deposit or share account opened with a bank after June 30, 1972, and before October 1, 2003, a bank shall, within 30 days from the date such a transaction occurs or an account is opened,

secure and maintain a record of the taxpayer identification number of the customer involved; or where the account or certificate is in the names of two or more persons, the bank shall secure the taxpayer identification number of a person having a financial interest in the certificate or account. In the event that a bank has been unable to secure, within the 30-day period specified, the required identification, it shall nevertheless not be deemed to be in violation of this section if (i) it has made a reasonable effort to secure such identification, and (ii) it maintains a list containing the names, addresses, and account numbers of those persons from whom it has been unable to secure such identification, and makes the names, addresses, and account numbers of those persons available to the Secretary as directed by him. A bank acting as an agent for another person in the purchase or redemption of a certificate of deposit issued by another bank is responsible for obtaining and recording the required taxpayer identification, as well as for maintaining the records referred to in paragraphs (b)(11) and (12) of this section. The issuing bank can satisfy the recordkeeping requirement by recording the name and address of the agent together with a description of the instrument and the date of the transaction. Where a person is a non-resident alien, the bank shall also record the person's passport number or a description of some other government document used to verify his identity.

(2) The 30-day period provided for in paragraph (a)(1) of this section shall be extended where the person opening the account has applied for a taxpayer identification or social security number on Form SS-4 or SS-5, until such time as the person maintaining the account has had a reasonable opportunity to secure such number and furnish it to the bank.

(3) A taxpayer identification number required under paragraph (a)(1) of this section need not be secured for accounts or transactions with the following: (i) Agencies and instrumentalities of Federal, state, local or foreign governments; (ii) judges, public officials, or clerks of courts of record as custodians of funds in controversy or

APPENDIX D – FUNDAMENTALS OF THE FUNDS TRANSFER PROCESS

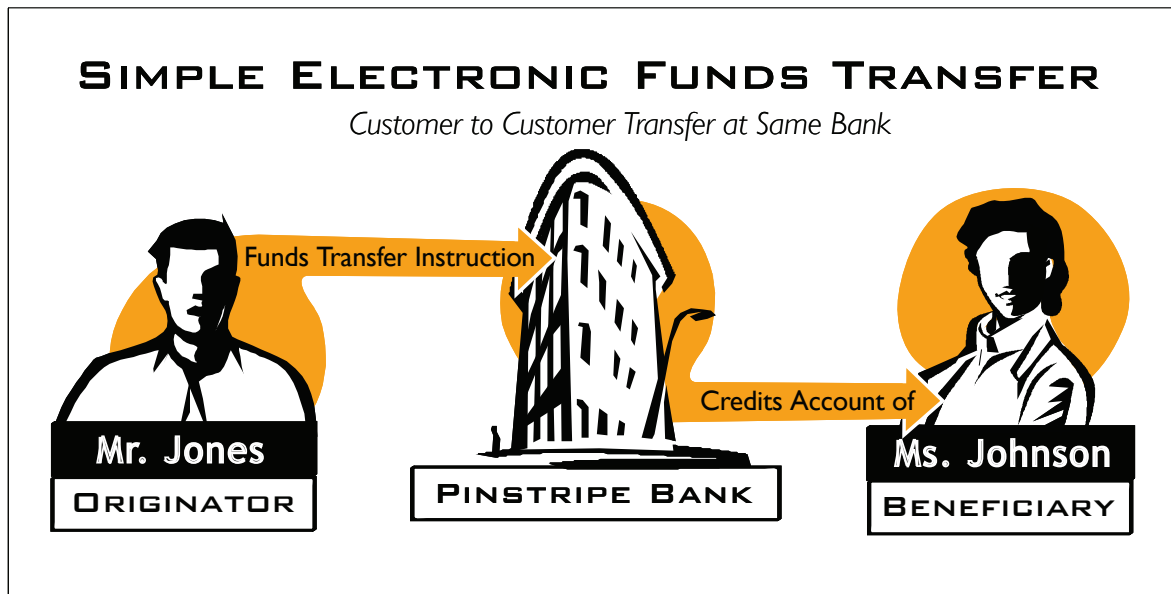
Essentially, an electronic funds transfer is a transaction by which funds move from one institution to another or one account to another at the direction of an institution's customer and through the transmission of electronic instruction messages that cause the institutions to make the required bookkeeping entries and make the funds available. Funds transfers are the primary mechanism used by the business community for fast and reliable transfer of funds between two parties.

The funds transfer process generally consists of a series of electronic messages sent between financial institutions directing each to make the debit and credit accounting entries necessary to complete the transaction. A funds transfer can generally be described as a series of payment instruction messages, beginning with the originator's (sending customer's) instructions, and including a series of further instructions between the participating institutions, with the purpose of making payment to the beneficiary (receiving customer).

The "players" that may be involved in a funds transfer transaction include:

- Originator, e.g., individual, business entity - the initiator of a funds transfer;
- Beneficiary - the ultimate party to be credited or paid as a result of a funds transfer;
- Originator's Financial Institution - the financial institution receiving the transfer instructions from the originator and transmitting the instructions to the next party in the funds transfer;
- Beneficiary's Financial Institution - the financial institution that is to credit or pay the beneficiary party; and
- Additional Financial Institutions - other institutions that may be required to effect the transaction.

The simplest funds transfers occur between two customers of a single financial institution. The originating customer simply instructs the institution to transfer funds to the beneficiary customer. The institution makes the required book entries in its accounting system and the transfer is complete. Such transfers occur primarily in purely domestic transfers, but could conceivably occur within a single institution with both U.S. and foreign branches.



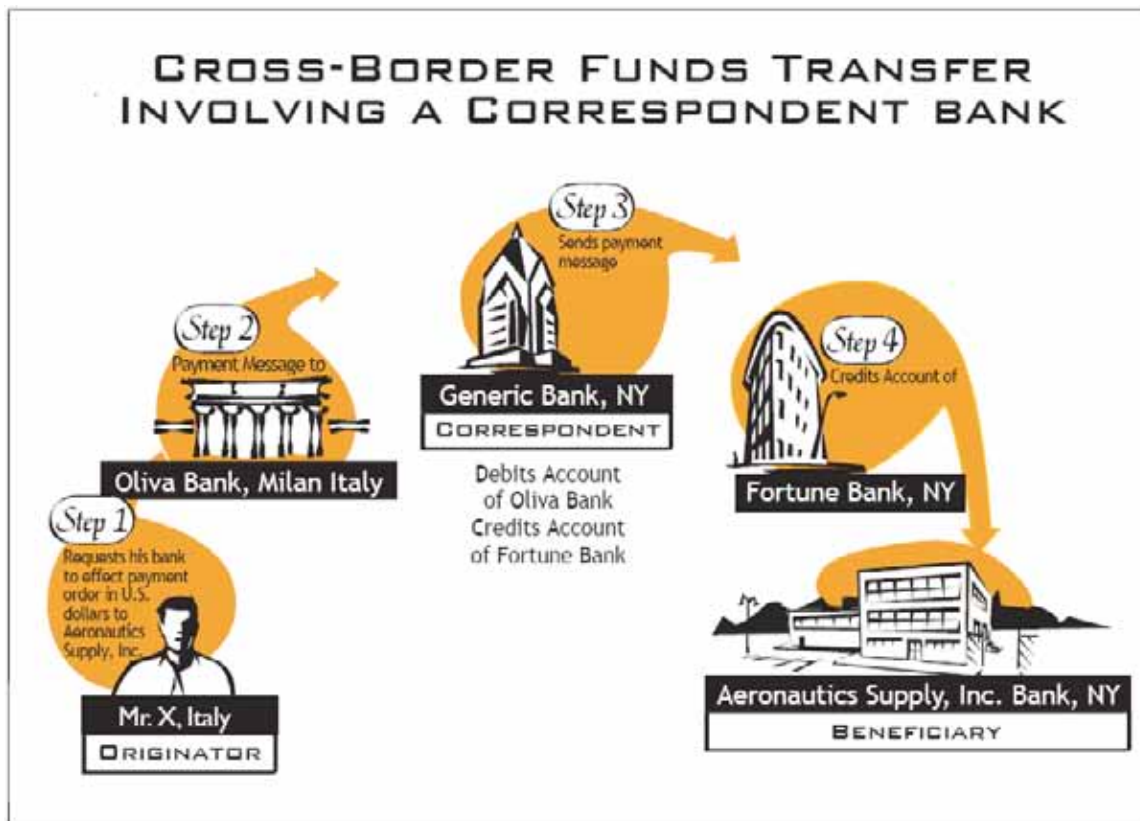
Scenarios that are more complicated appear when the number of institutions involved increases. These more complicated scenarios are far more common in the cross-border context, especially if an originator's institution does not have a branch in the beneficiary's foreign location. In this case, one financial institution may rely upon established business relationships with additional financial institutions to complete the transaction. Such relationships are "correspondent relationships."⁴⁰ A correspondent relationship, simply put, is the provision of banking services by one financial institution to another financial institution. For example, in the case that two institutions that need to complete a transaction both maintain accounts at a third institution, that third institution may transfer the funds from one's account to the other's to facilitate the customers' transfer.⁴¹ When coupled with electronic communications systems, such correspondent relationships expedite the transfer of funds across international borders and within countries.

To complete this kind of transfer, the customer's bank must identify another bank with which it maintains a "correspondent" relationship. In this case, a secure message between the banks can result in a "book transfer" where funds

40 The financial industry commonly uses many technical terms to describe these additional financial institutions. These terms include "intermediary" financial institution, "instructing" financial institution, "sender's correspondent," and "receiver's correspondent." In this study, we use the term "correspondent" to describe these additional financial institutions.

41 For example, America's Community Bankers, in its response to FinCEN's March 2006 industry survey, noted, "Most community banks use a correspondent bank to provide cross-border transactions. As a result, most community banks do not deal directly with institutions located outside the United States. Any reporting requirement should be limited to institutions that transmit funds directly to a foreign bank. The Department of the Treasury would still receive data about cross-border transfers originated by community banks, but that information would come from the correspondent."

are simultaneously debited from one account and credited to another. In the simplest example, the originator instructs her bank to transfer funds to the beneficiary and the bank sends an instruction to its correspondent, which makes the funds available to the beneficiary. When both the originator's and beneficiary's institutions have a correspondent relationship with the same third-party institution, the originator's institution can send the funds transfer through this "mutual correspondent."



Two banks that do not have a correspondent relationship can still transfer funds if they can establish a chain of banks that do have such a relationship. When the originator and beneficiary financial institutions do not maintain relationships with a mutual correspondent financial institution, they must rely upon additional correspondent financial institutions to complete the funds transfer. The additional "correspondent" financial institutions are essential pieces of the end-to-end funds transfer. Examples of these kinds of transfers appear in the discussion of the major funds transfer payment and messaging systems below. This process is eased by the existence of large "money center" banks that maintain correspondent relationships with many smaller banks and with each other. Importantly, a relatively small number of major money center banks specialize in facilitating international funds transfers through their network of correspondent relationships, and thus form a key link in the vast majority of all international funds transfers.

Cross-border electronic funds transfers of the type considered by this study flow primarily through banks.⁴² However, money remitters also provide valid and legitimate financial services in this area. Generally, remitters receive from their customers cash, for which the remitter transfers corresponding value to designated beneficiaries for a fee. Money remitters generally tend to engage in low dollar transactions, and traditionally serve the non-banking segment of the population -- notably new immigrants, permit-holding or clandestine foreigners, or any other person not having a bank account -- and frequently transfer funds to less advanced regions of the world where banking services are scarce.

Primary Industry Funds Transfer Systems in Operation

The actual exchange of data and funds necessary to complete a funds transfer transaction relies upon electronic processing, settlement, and communication systems.⁴³ This study focuses primarily upon the communication aspect of these systems. While the various payment and messaging systems offer differing levels of functionality, the instruction messages underlying all of these functions are the primary source of the data at issue in this study.⁴⁴ From a financial intelligence perspective, it is the information about the transaction rather than the movement of any actual funds that advances the effort to combat illicit finance. The payment instructions themselves identify the parties to the transaction and sometimes even more detailed information.

For the purposes of this study, FinCEN examined the operations of three payment or messaging systems in operation in the United States -- Fedwire, CHIPS, SWIFT -- and proprietary systems, primarily those used by money services businesses.

Fedwire

The Federal Reserve Banks own and operate the Fedwire funds transfer system that serves as the primary domestic electronic funds transfer system in the United States. The Fedwire system handles both the transmission of funds transfer instruction messages among financial institutions, as well as the settlement of the payment among the Fedwire participants. The Fedwire

42 This study, due to the limitations imposed by Section 6302 and the scope of the current funds transfer rule, does not examine the use of internet-based payment systems, stored value cards, ATM networks, etc. A significant number of "electronic funds transfers" traverse such systems, but would not fall within the scope of the proposed reporting requirement.

43 For purposes of this report, the term "settlement" refers to the actual debiting and crediting of accounts of the participant financial institutions. Communication between the participant financial institutions supports the settlement process as a means by which the institutions advise one another of actual debits and credits.

44 For example, Fedwire and CHIPS involve both the transmission of instruction messages and the settlement between institutions. SWIFT, on the other hand, does not effect the actual movement of any funds, but consists entirely of instructions for transfers that the institutions must complete by other means.

funds transfer system is a real time gross settlement system. In general, a system operates in “real time” if it processes each transaction immediately upon receipt.⁴⁵ A Fedwire transfer is irrevocable once the Federal Reserve credits the amount of the payment to the receiving bank’s account or delivers the payment order to the receiving bank, whichever is earlier.⁴⁶ The Federal Reserve Bank makes final payment to the receiving bank at the time the transfer is complete regardless of whether the Reserve Bank has received payment. On an average day in 2005, Fedwire processed approximately 528,000 transactions valued at \$2.1 trillion.⁴⁷ More than 7,000 institutions use Fedwire.

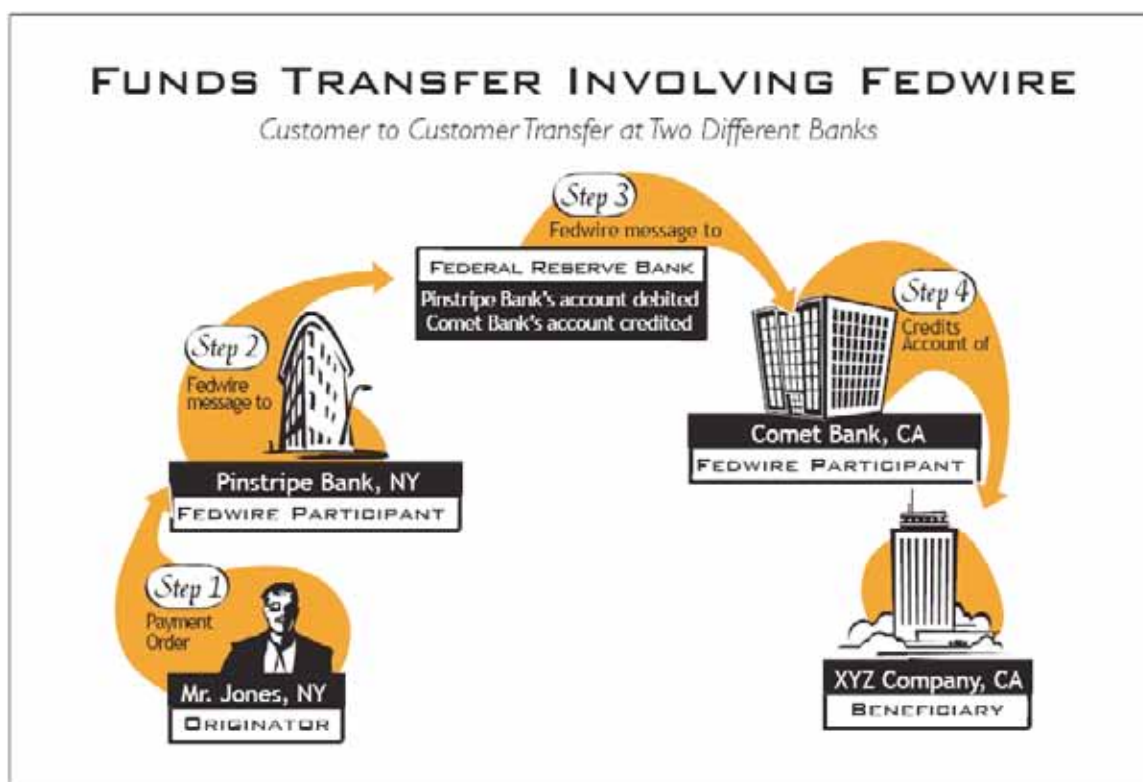
The Fedwire system is available only to U.S. financial institutions and does not permit a participating U.S. financial institution to transmit instructions or transfer funds directly to a non-U.S. financial institution.⁴⁸ The illustration below shows the flow of instructions and funds in a very simple Fedwire transfer.

45 This is in contrast to a batch-processing, store-and-forward system, such as the “Automated Clearinghouse” or “ACH” payment system. The ACH system operators process ACH “files” that contain multiple payment messages from a single originator (i.e., corporate payroll payments), called “batched messages.” An ACH operator processes the batched file for settlement at scheduled intervals, such as one to two days after it receives the batched file. The terms of Section 6302 of the Intelligence Reform Act defined the current study in such a way as to exclude ACH payments from the scope of the study.

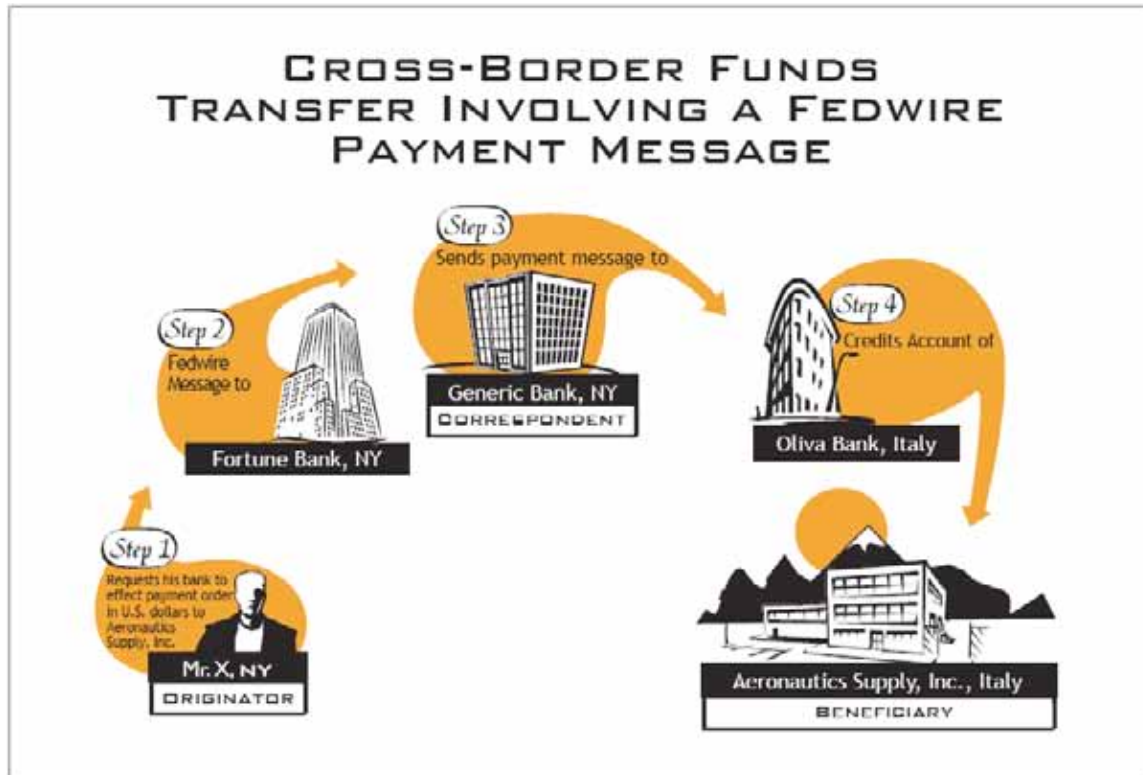
46 “Sending Bank” refers to the financial institution that actually sends the message into the Fedwire system. The Sending Bank may be a correspondent bank of an originator’s bank if the originator’s bank is not a Fedwire participant. “Receiving Bank” refers to the financial institution actually receiving the funds transfer from the Fedwire system. The Receiving Bank may be a correspondent bank of the beneficiary’s bank if the beneficiary’s bank is not a Fedwire participant.

47 See <http://www.federalreserve.gov/paymentsystems/fedwire/fedwirefundstrfann.htm>. See also, 91st Annual Report 2004, Board of Governors of the Federal Reserve System, p. 285.

48 Note that a foreign financial institution in fact, can gain access to the Fedwire system through a U.S. branch of the institution. That U.S. branch would be a U.S. financial institution for the purposes of the Bank Secrecy Act and its legal and regulatory requirements. In addition, certain foreign central banks receive funds transfers through the Fedwire funds transfer system.



It is important to note, however, that a Fedwire instruction may serve as one segment of a cross-border funds transfer. Fedwire can come into play to settle/clear the payment in U.S. dollars as illustrated below:



CHIPS

Like Fedwire, the Clearing House Interbank Payments System (CHIPS) handles both the transmission of funds transfer instruction messages among financial institutions, as well as the settlement of the payment between the institutions. CHIPS is operated by The Clearing House Payments Company, L.L.C.⁴⁹ CHIPS is the United States' main electronic funds-transfer system for processing international U.S. dollar funds transfers made among international banks. Like Fedwire, CHIPS is a real-time final settlement system. In other words, CHIPS settles the transactions at the time CHIPS transmits the payment order; meaning that the sending participant's obligation to pay the amount of the payment order to the receiving participant is discharged at the time CHIPS releases the payment message.⁵⁰

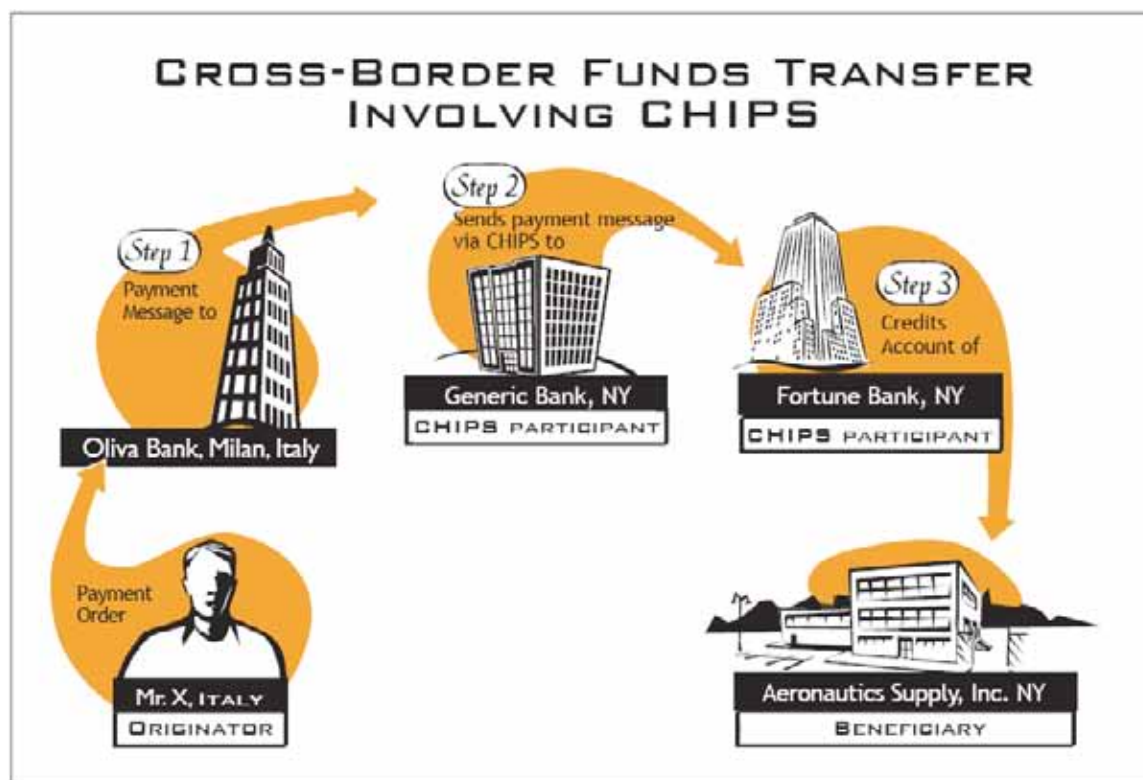
CHIPS claims to handle more than 90% of all U.S. dollar-based funds transfers moving between countries around the world. According to recent information provided by CHIPS, the system directly serves 46 banks representing 19

49 See <http://www.chips.org/home.php>

50 The "sending participant" refers to the bank actually inputting/sending the payment message to CHIPS. The "receiving participant" refers to the bank actually receiving the payment message from CHIPS.

countries. Recent figures reveal an approximate average of 280,000 transactions per day with a total monetary value of \$1.4 trillion.⁵¹

Access to the CHIPS payment system is conditional upon a financial institution's U.S. presence. In other words, the financial institutions using CHIPS must operate a U.S. branch or office for the use of the system. Accordingly, the CHIPS system does not permit a participating U.S. financial institution to transmit instructions or transfer funds directly to a non-U.S. financial institution. As in the case of Fedwire, it is important to note that a CHIPS instruction may serve as one segment of a cross-border funds transfer, as illustrated below:



SWIFT

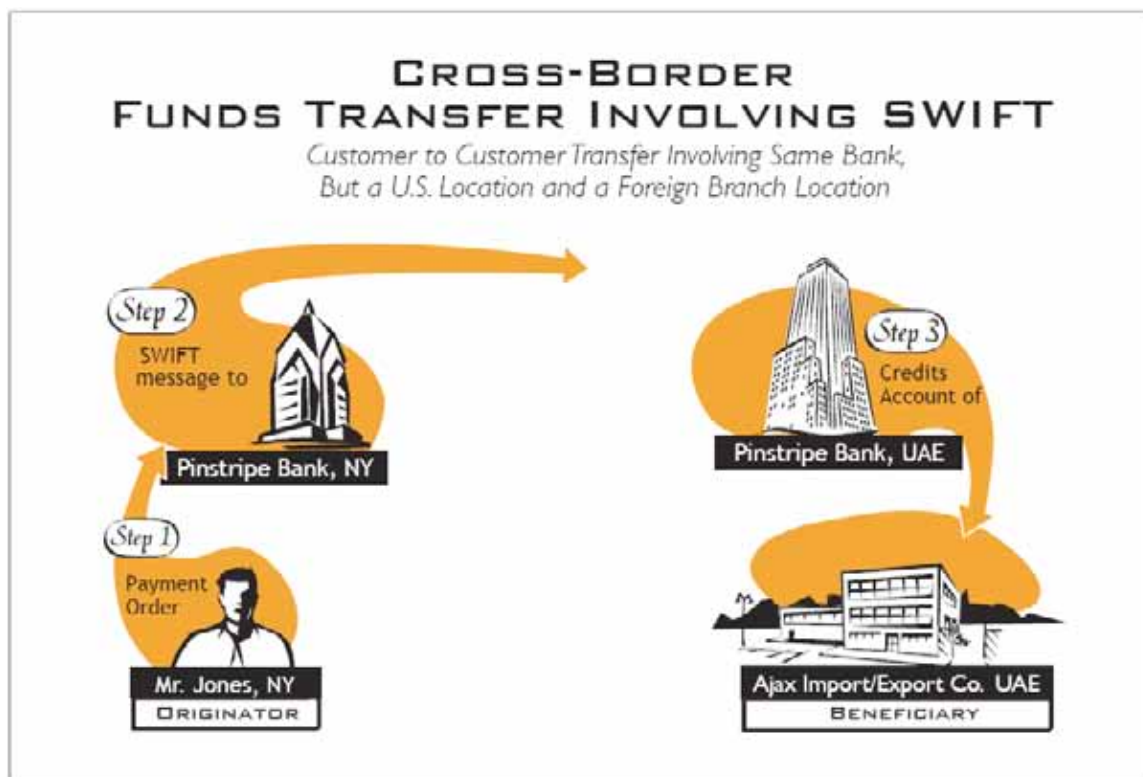
The Society for Worldwide Interbank Financial Telecommunication (SWIFT) provides secure electronic financial messaging services to financial institutions. SWIFT, which is a cooperative society owned by its member banks, is a unified international financial transaction messaging service.⁵² SWIFT represents an extensive telecommunications network by which a financial institution in one country can communicate with its branches or correspondent institutions

⁵¹ See, generally, CHIPS Annual Statistics from 1970 to 2006, available at <http://www.chips.org/about/pages/000652.php>

⁵² See <http://www.swift.com/>

anywhere in the world. In contrast to Fedwire and CHIPS, SWIFT is a messaging system for funds transfer instructions, rather than a financial settlement system. Recent figures reveal that approximately 7,600 SWIFT members and participants located in over 200 countries exchange approximately nine million messages per day. SWIFT's worldwide user community includes banks, broker/dealers and investment managers, as well as their market infrastructures in payments, securities, treasury, and trade. As of 2004, there were 574 U.S. financial institutions connected to SWIFT; those institutions sent approximately 383 million and received approximately 427 million SWIFT payments messages.⁵³ SWIFT processes over 2 billion messages per year. Daily overall volume of messages sent using the SWIFT system has tripled over seven years, with peak days of over 10 million messages in 2004. SWIFT messages direct the transfer of nearly \$5 trillion worldwide each day.

In contrast to Fedwire and CHIPS, a SWIFT message may travel directly from a U.S. financial institution to a foreign institution or vice versa. In practice, SWIFT is the primary method for international funds transfer messages.



⁵³ The SWIFT messaging system uses many different types of message formats to complete specific kinds of transactions. The primary message format used for customer payment messages is the SWIFT “MT-103” which represents a “Single Customer Credit Transfer,” or in simpler terms, a transaction conducted by an institution not on its own behalf, but on behalf of its customer. These figures include MT-103 customer payments as well as other forms of payment messages that are not a subject of this study. We could find no more detailed breakdown of SWIFT MT-103 traffic.

Interplay Between Funds Transfer Systems

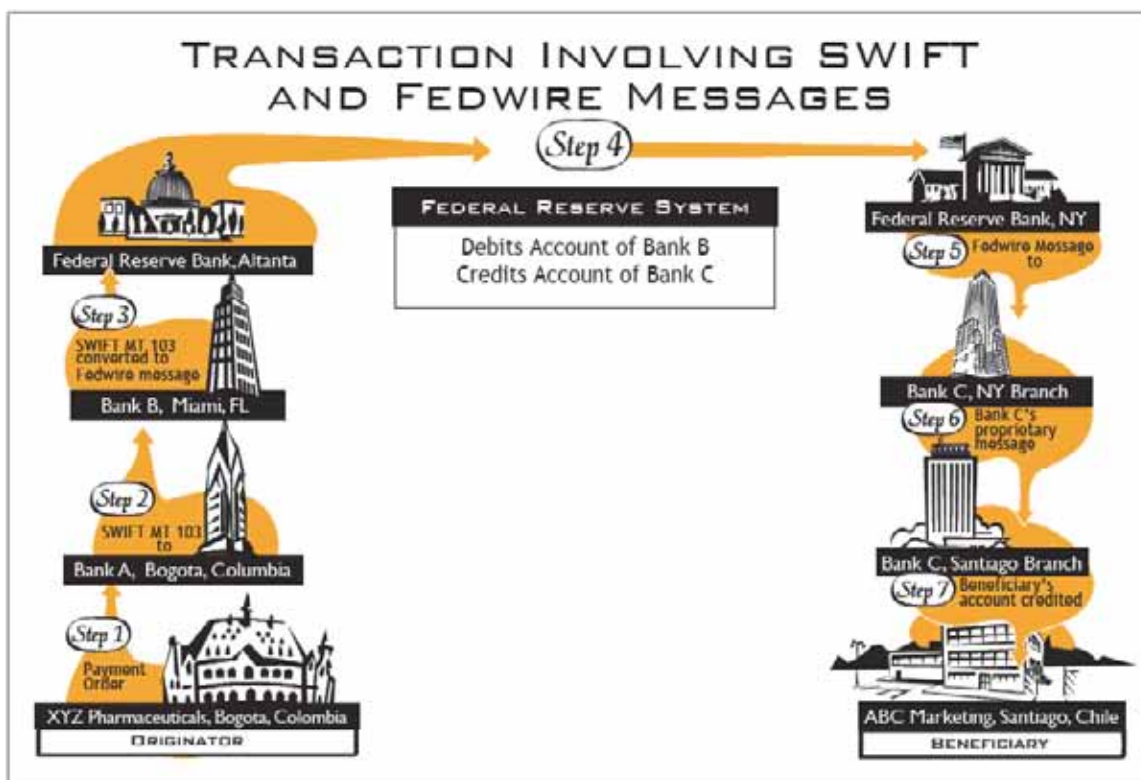
The aforementioned systems serve different functions and roles in the funds transfer transaction process. Financial institutions often use the Fedwire and CHIPS systems to handle both the message traffic and the actual movement and settlement of the funds. Institutions typically use the SWIFT system for communicating message instructions among financial institutions relating to the funds transfer.

Funds transfers often involve a combination of SWIFT and Fedwire messages or SWIFT and CHIPS or other instruction messages in the same transaction. For example, a U.S. institution may receive a SWIFT message from a foreign institution and map the message into a Fedwire or CHIPS message before passing it along to the additional U.S. financial institutions serving as correspondents.⁵⁴

When a funds transfer requires multiple correspondents' participation and involves more than one message system, one or more of the institutions translates or "maps over" the data from one message format to another. An estimated 70% of the traffic on the CHIPS system, for example, originates from SWIFT message traffic.⁵⁵

54 Whether an institution employs Fedwire or CHIPS as a settlement system in a transaction may depend, for example, upon whether the financial institutions involved are participants of CHIPS or Fedwire.

55 Global Payments: Moving U.S. Dollars, Teleseminar, March 30, 2005, available through <http://www.paymentsuniversity.com/home.php>



Money Transmitters

In addition to the banking industry, certain money services businesses (MSBs) operate as retail money transmitters. The term “money services business” refers to five distinct types of financial services providers that perform valuable services to a wide array of individuals, many of whom do not have ready access to or for their own reasons may eschew relationships with depository institutions.⁵⁶ Of primary concern for the purposes of this study are money transmitters.

Money transmitters provide many of the same attractions as the major bank-based electronic funds transfer systems. Money transmitters often maintain agent relationships with businesses around the globe, permitting rapid, secure transfer of funds. In addition, because money transmitters do not have account relationships with their customers, they are not required to perform customer identification and verification other than pursuant to the Funds Transfer and Travel Rules and the CTR requirements. While there are many such businesses, it is estimated that a relative handful of large money transmitters (i.e., 3-10) account for as much as 97% of the total volume of money remittances to or from the U.S.⁵⁷ through money transmitters.

⁵⁶ See 31 C.F.R. § 103.11(uu) for the definitions of “money services business” and “money transmitter” under the Bank Secrecy Act.

⁵⁷ Non-Bank Financial Institutions: A Study of Five Sectors, Coopers & Lybrand, L.L.P. (Feb. 28, 1997).

The few largest U.S. money transmitters provide money transfer services for consumers and businesses worldwide. Through hundreds of thousands of independently owned businesses (“send and receive agents”), these institutions provide money transfer services in approximately 200 countries and territories worldwide. Each day, these institutions process hundreds of thousands of money transfers involving U.S.-based customers.

The largest money transmitters maintain centralized data collection systems for all transactions and process all transactions by their agents through central processing systems located in the United States. Every send and receive agent collects the relevant information from its customers, including the data elements required by the Funds Transfer rule as appropriate, and submits the funds transfer instructions through a centralized system which in turn transmits the instructions to another appropriate send and receive agent for delivery of the funds.

It is possible for investigators to obtain information about funds transfers made through these money transmitters pursuant to a subpoena or other legal process. In response, the companies conduct a computer-based search based on key identifying information and generate a summary report containing basic information about the identified transactions. The information generally includes the send and receive agents, the date and amount of the transfer, and the parties to the transaction. The large money transmitters typically can retrieve additional detailed information in response to follow-up requests from investigators. In addition, these companies can conduct aggregate searches of larger volumes of transfer data in response to a proper legal request from law enforcement.

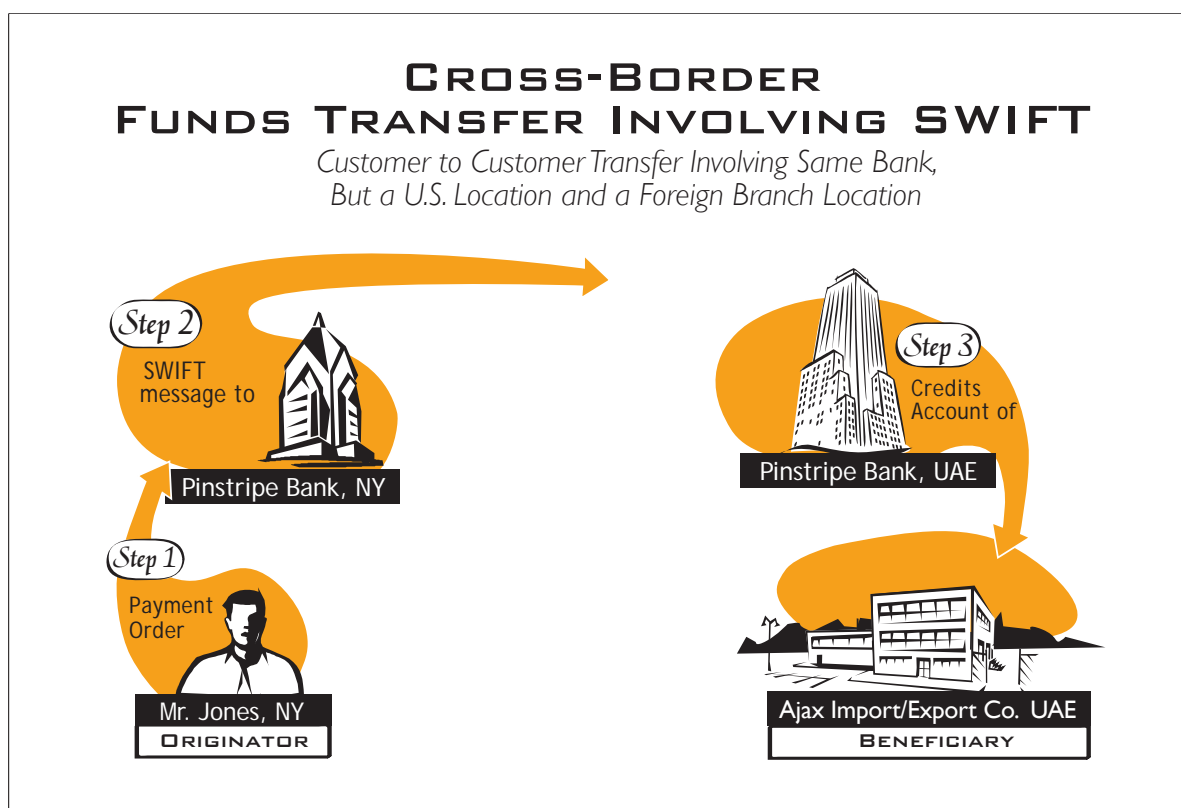
While money transmitters offer an alternative to banks, many must retain the services of a depository institution in order to conduct their own business.⁵⁸ In this situation, a money transmitter collects currency from its customers, sends transfer instructions to affiliates in other locations, deposits the currency into a bank account, and effects one or more electronic funds transfers through the bank to settle its accounts with the affiliates.

Proprietary Transfer Systems and Other Issues

Whether a depository institution, a money transmitter, or otherwise, a financial institution, may also use proprietary or internal systems to handle all or part of

⁵⁸ Note, however, that this is not true of all “money transmitters.” As the 9/11 Commission noted, “A hawala, at least in its “pure” form, does not use a negotiable instrument or other commonly recognized method for the exchange of money. Hawaladars instead employ a variety of means, often in combination, to settle with each other: they can settle preexisting debt, pay to or receive from the accounts of third parties within the same country, import or export goods (both legal goods, with false invoicing, or illegal commerce, such as drug trafficking) to satisfy the accounts, or physically move currency or precious metal or stones.” Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States. p. 68

an electronic funds transfer, i.e., between branches of the same institution. Such systems pose a special challenge because of the wide range of potential message formats, communications protocols, and data structures involved. For example, a U.S.-based correspondent involved in a cross-border transfer may have a foreign branch that can complete the transfer without involving additional institutions. In such a case, the U.S.-based correspondent may employ the institution's internal systems to transmit the instructions to its foreign branch. In such a case, the instruction may have traversed the Fedwire or CHIPS systems, but never traversed any other messaging systems not within the direct control of the correspondent institution.



“U-Turn” Transactions

It also occurs that funds transfers from one foreign location to another foreign location may involve a U.S.-based bank serving as a correspondent bank. In this type of transaction, there is no originator or beneficiary within the United States, but a U.S. financial institution handles some segment of the funds transfer. As a result, these U.S.-based banks may be privy to the specific details of such transactions and maintain related internal records of these transactions.

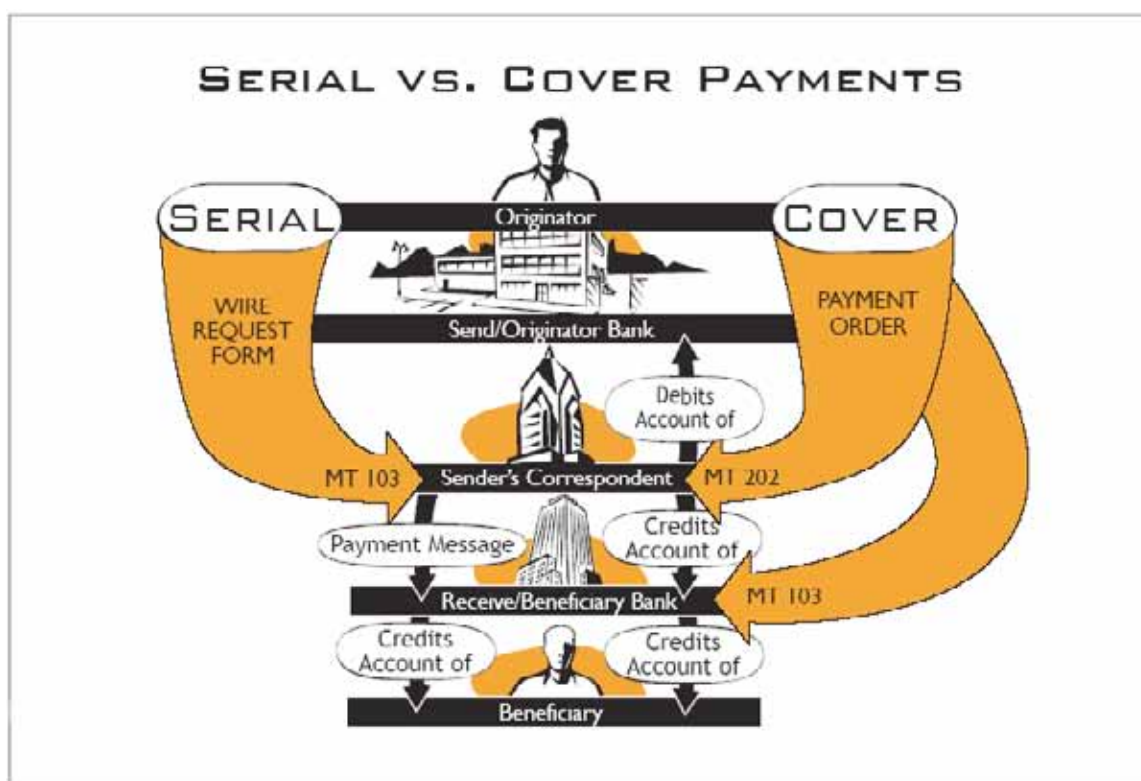
“Serial” Payment and “Cover” Payment Methods

In examining these foreign location-to-foreign location funds transfers involving U.S.-based correspondent banks, there are two primary methods of payment: the “Serial” payment method and the “Cover” payment method.

In the serial payment method, one financial institution transmits the funds transfer instructions (i.e., a SWIFT MT 103 message) to the next financial institution in the overall “payment chain.” Each institution in the communication chain receives the same level of detail about the transaction at each step.

In contrast, the “Cover” payment method divides the message into two parts. The originator’s bank sends the detailed funds transfer instruction directly to the beneficiary’s bank. In this case, no U.S. institution receives the instruction that identifies the originator and beneficiary of the transaction. The originator’s bank also sends a second “cover” payment instruction (i.e., a SWIFT MT 202 message) that directs the transfer of the funds from the originator’s bank to the beneficiary’s bank as a financial institution-to-financial institution settlement payment.

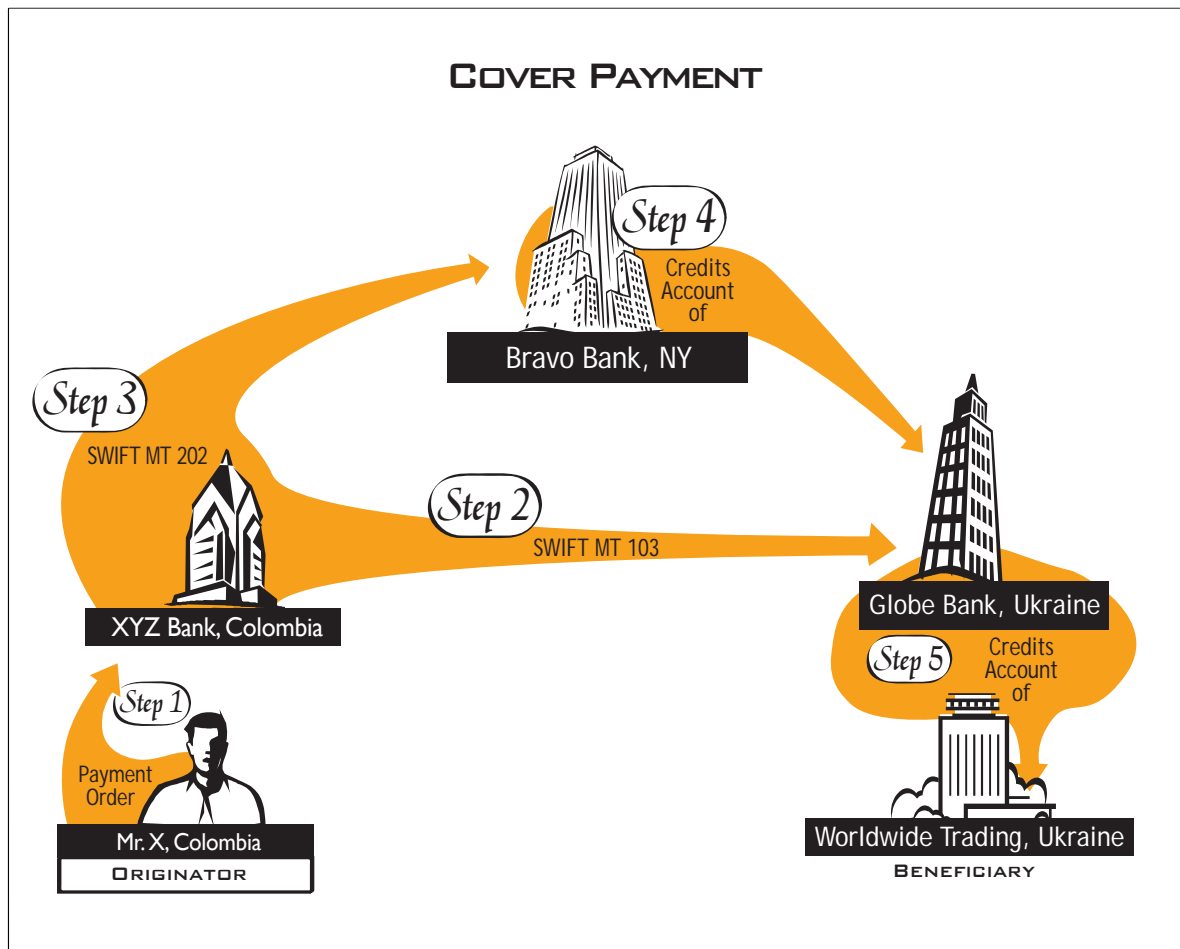
The following diagram illustrates the basic comparison between the two methods:



When the “Cover” payment method is used, a U.S.-based correspondent bank will receive the cover payment message identifying only the foreign institutions involved, but not the originator and beneficiary. Although this particular message may not contain the customer-related details that could appear in a serial payment, the cover payment message could, nevertheless, be useful for broader analyses. This may include, for example, examining these cover

payment messages to monitor and detect sudden and unusual spikes in overall funds flows to, through, and from certain banks and/or countries possibly resulting in findings warranting further exploration from either the regulatory or law enforcement perspectives.

The illustration below represents the use of the Cover payment method.



APPENDIX E – CROSS-BORDER FUNDS TRANSFER REPORTING IN CANADA AND AUSTRALIA

Systems for the collection, storage, processing, analysis, and dissemination of cross-border electronic funds transfers are in place. Both the Australian and Canadian governments, through their financial intelligence units, have imposed cross-border electronic funds transfer reporting requirements on their financial services industries. What follows is a discussion of the similarities, and differences between the American recordkeeping requirement and the Australian, and Canadian reporting regimes.

Canada

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) is Canada's financial intelligence unit. The Centre was created to detect and deter money laundering by providing critical information to support the investigation or prosecution of money laundering offences. In December 2001, FINTRAC's mandate expanded to include the detection and deterrence of terrorist financing. FINTRAC collects reports from Canadian financial institutions and others related to, among other things, suspicious transactions, large currency transactions, and cross border movement of currency and monetary instruments valued at \$10,000 (CAN) or more. In addition, FINTRAC collects reports related to any cross-border electronic funds transfer in an amount of \$10,000 (CAN) or more.

FINTRAC analyzes the reports it collects for unusual patterns of transactions that resemble money laundering or terrorist financing activity. Subsequently, FINTRAC checks other databases to which it has access, including databases maintained for law enforcement and national security purposes, as well as public and commercial databases. When FINTRAC concludes that it has reasonable grounds to suspect that information in its possession "would be relevant to investigating or prosecuting a money laundering offence or a terrorist activity financing offence," it discloses designated information, as defined in Canadian law, to the appropriate police force or to the Canadian Security Intelligence Service (CSIS).

FINTRAC first required the reporting of cross-border electronic funds transfers ("EFT" reporting) in June 2002. Initially, FINTRAC required only reports of international funds transfers made using certain SWIFT messages. Effective March 31, 2003, FINTRAC expanded the international EFT reporting requirement to cover all forms of international EFT regardless of system or

message format (See below for the specific legal requirements in Canada). FINTRAC receives almost all of its international EFT reports electronically; FINTRAC's regulations permit for paper filing where the reporting institution can certify that they lack the capability to file electronically, but FINTRAC officials noted that this rarely happens.

To facilitate the electronic filing of these reports, FINTRAC established a "batch file transfer format" that informs financial institutions of the appropriate report content and form. In turn, reporting institutions must implement their own systems for converting the institutions' non-SWIFT data to the proper format prior to submission. For non-SWIFT EFTs FINTRAC has also developed an online form that is generally used by smaller institutions. For both SWIFT and non-SWIFT messages, FINTRAC has established minimum mandatory data fields (17 fields for outgoing SWIFT messages; 8 fields for incoming SWIFT messages; 11 fields for both outgoing and incoming non-SWIFT messages) that must be included in the report (again, FINTRAC dictates the format of the batch submission, but distinguishes between mandatory fields and those fields).⁵⁹

More than 300,000 entities and persons are potentially subject to the EFT reporting requirement in Canada, but many do not conduct business that reaches the thresholds in the law and thus, need not report. In addition, not all types of regulated institutions are currently required to report. However, the Department of Finance has issued a public consultation paper recommending that Parliament amend existing law to require all regulated entities to report cross-border EFTs. As noted above, FINTRAC permits reporting institutions to report by batch file and by single report through either a web-based interface or client software distributed by FINTRAC. Currently 56 entities report via the batch process, with the others using the online reporting mechanism.

- In total, FINTRAC receives approximately 590,000 international EFT transaction records per month.
- In '03-04, FINTRAC received 2.7 million SWIFT EFT reports and 3.9 million non-SWIFT EFT Reports
- In '04-'05, FINTRAC received 3 million SWIFT EFT reports and 4.1 million non-SWIFT EFT Reports
- 60% of all the FINTRAC reports are submitted by banks
- FINTRAC's international EFT data store contains approximately 15.6 million records

⁵⁹ See http://www.fintrac.gc.ca/publications/guide/archive/Guide8/81_e.asp#1a

Australia

The Australian Transaction Reports and Analysis Centre (AUSTRAC) is the financial intelligence unit of the Australian government. The Centre was created to detect and deter money laundering by providing critical information to support the investigation or prosecution of money laundering offences and oversee compliance with the reporting requirements of the *Financial Transaction Reports Act 1988 (FTR Act)*. Under the FTR Act, AUSTRAC collects reports from Australian financial institutions related to, among other things, suspicious transactions, large currency transactions, and cross border currency transactions. AUSTRAC also issues guidelines and circulars to those entities that report to it, called “cash dealers,” about their obligations under the FTR Act and Financial Transactions Reports Regulations. In addition, AUSTRAC collects reports related to any cross-border electronic funds transfer in any amount.

AUSTRAC first required the reporting of cross-border electronic funds transfers (“IFTI” reporting) in 1992.⁶⁰ Generally, AUSTRAC requires the institutions “who are senders of IFTIs transmitted out of Australia; or who are receivers of IFTIs transmitted into Australia” submit reports of those transactions.

AUSTRAC accepts IFTI reports in one of two formats. First, AUSTRAC accepts reports containing properly formatted SWIFT instruction messages from those institutions that use the SWIFT system. Second, AUSTRAC established a batch file transfer format and requires the reporting institutions to implement their own systems for converting the institutions’ non-SWIFT data to the proper format prior to submission. For both SWIFT and non-SWIFT messages, AUSTRAC has established minimum mandatory data fields that must be included in the report.

AUSTRAC permits reporting institutions to report by batch file and by single report through a web-based interface operated by AUSTRAC. This interface enables institutions to upload prepared files automatically, provides an interface for the manual upload of prepared batch files, and provides a form for extremely low volume reporting institutions to submit their data. In addition, AUSTRAC developed and distributes to financial institutions a Microsoft Excel macro that will convert certain electronic records to the prescribed data format for upload to the AUSTRAC systems. AUSTRAC officials told us that the largest four institutions in Australia account for approximately 80% of the IFTI reporting, while a second tier of approximately 20 institutions account for the majority of the remaining reports.

60 The IFTI reporting provisions are set out in section 3 and sections 17B to 17F of the FTR Act. The prescribed details in relation to IFTIs are contained in Regulation 11AA of the *Financial Transaction Reports Regulations 1990* (FTR Regulations); see also AUSTRAC Information Circular No. 2, available at http://www.austrac.gov.au/resources/publications/information_circular/pdf/AIC%2002%20-%20International%20Funds%20Transfer%20Instructions.pdf

In total, AUSTRAC receives approximately 9 to 10 million IFTI records per year.

- In '03-'04, AUSTRAC received approximately 4 million inbound and approximately 4.5 million outbound IFTI reports
- In '04-'05, AUSTRAC received 4.2 million inbound IFTI reports and approximately 5.5 million outbound IFTI reports
- The most recent figures reveal that in the course of a year, approximately 78% of the IFTI reports are in SWIFT format and 22% in non-SWIFT format
- AUSTRAC's data store contains approximately 70 million records dating from 1995 to present; 55 million of those are IFTI reports

Applicable United States Regulations

Under the funds transfer rule (31 C.F.R. § 103.33), for each payment order that it receives, a financial institution operating in the United States must obtain and retain the following information on funds transfers of \$3,000 or more:⁶¹ (a) name and address of the originator; (b) the amount of the funds transfer; (c) the date of the request; (d) any payment instructions received from the originator with the payment order; (e) the identity of the beneficiary's bank; (f) and as much information pertaining to the beneficiary as is received, such as name and address, account number, and any other identifying information. Intermediary and beneficiary banks receiving a payment order are required to keep an original or a copy of the payment order. An originator bank is required to verify the identity of the person placing a payment order if the customer places the order in person and if the person is not already a customer. Similarly, if a beneficiary bank delivers the proceeds to the beneficiary in person, the beneficiary bank is required to verify the identity of that person if not already a customer.

In addition, a bank must retain a copy of the identifying items that it received with the payment order, such as the name, address, and account number of the beneficiary. The Funds Transfer Rule contains an important provision known as the "Travel Rule," which requires the payment message, when it is sent to a receiving financial institution, to include the following information:

- the name and address of the originator;
- the amount of the transfer;

61 The U.S. Department of the Treasury is reviewing the current threshold, particularly in light of international standards. See Interpretive Note to FATF Special Recommendation VII (requiring countries to mandate that cross-border wire transfers contain accurate and meaningful originator information. Countries may adopt a de minimus threshold of no higher than USD or EUR 1,000. Countries are expected to be in compliance with the Special Recommendation by December 2006.); See 71 Fed.Reg. 35564 (June 21, 2006).

- the execution date of the transfer;
- any payment instructions received;
- the name and address of the beneficiary (if available);
- the account number of the beneficiary (if available);
- any other specific identifiers of the beneficiary (if available); and
- the beneficiary's financial institution.

An originator's financial institution operating in the United States also must include in the payment message as many of the identifying items as it receives with the payment message, such as the name, address, and account number of the beneficiary. This information must be included in, or "travel" with, every subsequent payment message.

Comparison of Funds Transfer Reporting and Recordkeeping

	Canada	Australia	U.S. Recordkeeping
Collecting since	2002	1992	n/a
Value Threshold	\$10,000 CAN	N/A	\$3,000 USD
Types of Reporting Institutions	Depository Institutions Money Transmitters Currency Exchangers	Depository Institutions Money Transmitters	Depository Institutions Nonbank financial institutions
Specific Institutions Required to Report	All institutions, including correspondents	First In/Last Out	All institutions, including correspondents
No. of Regulated Institutions	~14,000*	315	>200,000
No. Reporting EFTs	Unknown	212	n/a
Reporting Form/Manner	SWIFT MT-103 Online Form Prepared Report	SWIFT MT-103 Online Form Prepared Report	n/a
Annual Volume	7.1 million	9-10 million	350-500 million (est'd)
% SWIFT/non-SWIFT	42% SWIFT 58% non-SWIFT	78% SWIFT 22% non-SWIFT	67% SWIFT 33% non-SWIFT**
Primary Filers/% of Total	Unknown	4/80%	n/a
LE access to the data	None – by referral from FINTRAC only	Direct Query Access	Direct Query Access

* Statistics on Payment and Settlement Systems in Selected Countries, Figures for 2004, Bank for International Settlements, March 2006, pp. 16-17.

**Estimated.

The primary differences between Canada's, Australia's, and the United States' reporting frameworks are that the U.S. does not currently require reporting of funds transfer information, and that the number of regulated financial institutions and the volume of cross-border funds transfers is greater in the U.S. than in Canada or Australia. This latter difference suggests that the burden on FinCEN related to the collection, storage, processing, analysis, and dissemination of cross-border funds transfer reports is substantially higher than on FINTRAC and AUSTRAC.

Funds Reporting Requirements in Canada and Australia

Canada

Legal Source

Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations - November 06, 2003

http://www.fintrac.gc.ca/reg/ConsolReg_031106-2_e.asp

Definition of Transfers to be Reported

“electronic funds transfer,” means the transmission - through any electronic, magnetic, or optical device, telephone instrument, or computer - of instructions for the transfer of funds, other than the transfer of funds within Canada. In the case of SWIFT messages, only SWIFT MT 100 and SWIFT MT 103 messages are included. (télévirement)

“Interpretation” 1(2) http://www.fintrac.gc.ca/reg/ConsolReg_031106-2_e.asp

“Interpretation” 1(2) http://www.fintrac.gc.ca/reg/ConsolReg_031106-2_e.asp

“Financial entity” means an authorized foreign bank within the meaning of section 2 of the Bank Act in respect of its business in Canada or a bank to which that Act applies, a cooperative credit society, savings and credit union or caisse populaire that is regulated by a provincial Act, an association that is regulated by the Cooperative Credit Associations Act, a company to which the Trust and Loan Companies Act applies and a trust company or loan company regulated by a provincial Act. It includes a department or agent of Her Majesty in right of Canada or of a province where the department or agent is carrying out an activity referred to in section 45. (entité financière) Persons or Entities Engaged in the Business of Foreign Exchange Dealing

“Money services business” means a person or entity that is engaged in the business of remitting funds or transmitting funds by any means or through any person, entity or electronic funds transfer network, or of issuing or redeeming money orders, traveller's cheques or other similar negotiable instruments. It includes a financial entity when it carries out one of those activities with a

person or entity that is not an account holder. (entreprise de transfert de fonds ou de vente de titres négociables)

U.S. Equivalent Financial Institutions – Banks and Money Services Businesses

Reporting Requirement

http://www.fintrac.gc.ca/reg/ConsolReg_031106-2_e.asp

“*Financial Entities*” – Section 12(b) and 12(c) of Proceeds of Crime Act

“*Persons or Entities Engaged in the Business of Foreign Exchange Dealing*”

– Section 24(b) and 24(c) of Proceeds of Crime Act

“*Money Services Businesses*” – Section 28(b) and 28(c) of Proceeds of Crime Act

The text of the reporting requirement for the above three entities is substantively similar to each other, as follows:

12. (1) Subject to subsection (5), section 50 and subsection 52(1), every financial entity shall report the following transactions and information to the Centre:

The sending out of Canada, at the request of a client, of an electronic funds transfer of \$10,000 or more in the course of a single transaction, together with the information referred to in Schedule 2 or 5, as the case may be; and

The receipt from outside Canada of an electronic funds transfer, sent at the request of a client, of \$10,000 or more in the course of a single transaction, together with the information referred to in Schedule 3 or 6, as the case may be.

(2) For greater certainty, paragraph (1)(b) does not apply when the financial entity sends an electronic funds transfer to a person or entity in Canada, even if the final recipient is outside Canada.

(3) Paragraph (1)(b) applies in respect of a financial entity that orders a person or entity to which subsection (1), 24(1) or 28(1) applies to send an electronic funds transfer out of Canada, at the request of a client, unless it provides that person or entity with the name and address of that client. (SOR/2003-358, subs.5(1))

(4) For greater certainty, paragraph (1)(c) does not apply when the financial entity receives an electronic funds transfer from a person or entity in Canada, even if the initial sender is outside Canada.

Exceptions to General Requirement

Transfers made by a financial institution on its own behalf are exempt. See sections 12, 24, and 28, which restrict reporting to transactions made “at the request of a client.”

http://www.fintrac.gc.ca/reg/ConsolReg_031106-2_e.asp

Reporting Threshold

\$10,000 Canadian

Australia

Legal Source

Financial Transaction Reports Act 1988 – as of 6 February 2004

<http://scaleplus.law.gov.au/html/pasteact/0/59/top.htm>

Definition of Transfers to be Reported

International funds transfer instruction means an instruction for a transfer of funds that is transmitted into or out of Australia electronically or by telegraph, but does not include an instruction of a prescribed kind. (ED – see exceptions, below)

“Interpretation” Sec. 3 <http://scaleplus.law.gov.au/html/pasteact/0/59/0/PA000070.htm>

Financial Institutions subject to Reporting Requirement

“Interpretation” Sec. 3 <http://scaleplu.law.gov.au/html/pasteact/0/59/0/PA000070.htm>

All “*cash dealers*” including:

- (a) A financial institution;
- (b) A body corporate that is, or, if it had been incorporated in Australia, would be, a financial corporation within the meaning of paragraph 51(xx) of the Constitution;
- (c) An insurer or an insurance intermediary;
- (d) A financial services licensee (as defined by section 761A of the Corporations Act 2001) whose licence covers either or both of the following:
 - (i) Dealing in securities (as defined by subsection 92(1) of the Corporations Act 2001);
 - (ii) Dealing in derivatives (as defined by section 761A of the Corporations Act 2001);
- (f) A Registrar or Deputy Registrar of a Registry established under section 14 of the Commonwealth Inscribed Stock Act 1911;
- (g) A trustee or manager of a unit trust;
- (h) A person who carries on a business of issuing, selling or redeeming travellers cheques, money orders or similar instruments;

- (j) A person who is a bullion seller.
- (k) A person (other than a financial institution or a real estate agent acting in the ordinary course of real estate business) who carries on a business of:
 - (i) collecting currency, and holding currency collected, on behalf of other persons; or
 - (ia) exchanging one currency for another, or converting currency into prescribed commercial instruments, on behalf of other persons; or
 - (ib) remitting or transferring currency or prescribed commercial instruments, or making electronic funds transfers, into or out of Australia on behalf of other persons or arranging for such remittance or transfer; or
 - (ii) preparing pay-rolls on behalf of other persons in whole or in part from currency collected; or
 - (iii) delivering currency (including payrolls);
- (l) A person (other than a financial institution or a real estate agent acting in the ordinary course of real estate business) who carries on a business in Australia of:
 - (i) on behalf of other persons, arranging for funds to be made available outside Australia to those persons or others; or
 - (ii) on behalf of persons outside Australia, making funds available, or arranging for funds to be made available, in Australia to those persons or others;
- (m) A person who carries on a business of operating a gambling house or casino; and
- (n) A bookmaker, including a totalisator agency board and any other person who operates a totalisator betting service.

“Financial institution” means (from (a), above):

an Authorized Deposit-taking Institution (ADI):

A body corporate that is an ADI for the purposes of the Banking Act 1959;

The Reserve Bank of Australia; or

A person who carries on State banking within the meaning of paragraph 51(xiii) of the Constitution.

Or (from (b), above), a co-operative housing society.

U.S. Equivalent Financial Institutions – Banks, Securities Brokers/Dealers, Futures Commission Merchants, Money Services Businesses, Casinos

Reporting Requirement

FTR Act - Section 17B - Reports of international funds transfer instructions
<http://scaleplus.law.gov.au/html/pasteact/0/59/0/PA000300.htm>

(1) If:

A cash dealer in Australia is:

- (i) the sender of an international funds transfer instruction transmitted out of Australia; or
 - (ii) the recipient of an international funds transfer instruction transmitted into Australia;
- and

at least one of the following applies:

- (i) the cash dealer is acting on behalf of, or at the request of, another person who is not an ADI;
- (ii) the cash dealer is not an ADI;

the dealer must, before the reporting time, prepare a report of the instruction.

(2) The report must be in the approved form and include the prescribed details.

(3) Subject to subsection (4), the report must be sent to the Director in the approved way and form before the reporting time.

(4) The Director may, by notice in the Gazette, declare that subsection (3) does not apply in relation to a cash dealer in relation to a report or a class of report. (ED - i.e. AUSTRAC can declare certain transactions exempt; they have declared several categories – see below).

(5) If, because of the operation of subsection (4), subsection (3) does not apply in relation to a report, the cash dealer must retain the report for 7 years.

(6) For the purposes of this section, if a cash dealer transmits an instruction on behalf of, or at the request of, another person, the cash dealer is taken to be the sender of the instruction.

(7) For the purposes of this section, if a person, not being a cash dealer, transmits an instruction on behalf of, or at the request of, a cash dealer, the cash dealer is taken to be the sender of the instruction.

(8) In this section:

reporting time, in relation to an instruction, means:

- (a) if the instruction is transmitted into Australia—14 days after the day that the transmission is received or such later time as is specified in the regulations;

(b) if the instruction is transmitted out of Australia—14 days after the day that the instruction is transmitted or such later time as is specified in the regulations.

Exceptions to General Requirement

Transfers conducted by a bank on its own behalf are exempted. All other financial institutions (“cash dealers”) must report transfers that they conduct on their own behalf. See section 17B(1)(b) requirements.

<http://scaleplus.law.gov.au/html/pasteact/0/59/0/PA000300.htm>

In addition, AUSTRAC Information Circular #2 sets forth the following exceptions to the general reporting requirement:

http://www.austrac.gov.au/resources/publications/information_circular/pdf/AIC%2002%20-%20International%20Funds%20Transfer%20Instructions.pdf

IFTIs which only involve ADIs (ED – i.e. banks) acting solely on their own behalf, such as where there is a transfer of funds to effect ADI-to-ADI settlements, need not be reported. The exclusion of an ADI’s own transactions and ADI-to-ADI settlements is provided as those ADIs are caught by stringent regulatory and supervisory requirements of the Banking Act 1959. The legislation does, however, provide for the Director of AUSTRAC to allow exclusion of transactions of other cash dealers, which are similar to those types of transactions which have specifically been excluded for ADIs. The Director of AUSTRAC has granted exemptions to some cash dealers, on a case by case basis, in the following terms:

1. Transactions conducted by a cash dealer on its own behalf, i.e. transactions where the cash dealer is not acting on behalf of, or at the request of another person, where:

1a) The cash dealer has authority from the Reserve Bank of Australia to deal in foreign exchange; and/or

1b) The cash dealer has applied to the Reserve Bank of Australia to be considered for Bank ‘branch’ status.

2. Telex transactions transmitted or received by the cash dealer which cannot be reported to AUSTRAC in an electronic format, where:

After excluding reports covered by all other declarations of the Director in respect of that cash dealer, the cash dealer would still be required to report 10,000 or more IFTI telex transactions per year and those telexes are not capable of being reported in an electronic format but will be capable of being reported electronically to AUSTRAC within 5 years of the first exemption date.

3. Other classes of reports for which the cash dealer seeks exemption.

The Director has considered for declaration in the Government Gazette, classes of reports in addition to those referred to in 1 and 2 above. The cash dealer is required to retain those exempted reports for a period of seven (7) years.

Reporting Threshold

No Threshold – institutions must report all cross-border funds transfers

APPENDIX F – POTENTIAL ANALYTICAL VALUE OF CROSS-BORDER FUNDS TRANSFER REPORTS

Basic cross-border funds transfer messages generally include, for example:

- Date;
- Amount;
- Customer parties, and even possibly associates, and identifiers, e.g., account numbers, addresses, phone numbers;
- Customer parties' financial institutions and additional financial institutions involved in the transaction flow;
- Customer-to-customer and financial institution-to-financial institution information; and/or
- Transaction reference information.

The message formats used by the primary systems are relatively standardized. On the other hand, the specific format of an internal funds transfer database record that is maintained by a financial institution may vary from financial institution-to-financial institution and also be based upon the internal record, tracking, storage, and accounting procedures of a financial institution. These internal database records may be somewhat more difficult to decipher without the direct assistance of officials from that particular financial institution.

Any reporting requirement would provide a means of centralizing cross-border electronic funds transfer information in a single format and linking it with other highly relevant financial intelligence.⁶² The value of the cross-border funds transfer data lies partially in the revelation of additional identifiers (personal information, phone numbers, bank and branch identification codes, etc.).

⁶² Many in industry and government have raised the question of what changes, if any, the proposed collection system would require to the established funds transfer messaging systems (i.e., CHIPS, SWIFT, Fedwire). In its response to FinCEN's industry survey issued in March 2006, the American Bankers Association stated that "Imposing a new requirement to include this type of information for all wire transfers would require substantial changes to US payment systems." Such changes were not necessary to the implementation of the corresponding requirements in either Canada or Australia. We conclude that not only would no such change be required, but that if such a change were necessary in order to make such a system work, the system would not be feasible.

Individual Targeting/Research of Known Subjects

Many analysts will rely primarily on the capacity to search electronic funds transfer data for specific names or account numbers and receive results within seconds. This kind of query and reporting function allows analysts to construct a customized query in response to a specific need. Many commercial software tools provide the query and reporting capabilities for retrieving structured data.

Typical commercially available search tools allow users to perform the following functions:

- **Exact Key Word Searches** – The query will return only results that exactly match the search criteria. This type of query is usually sufficient, however, it does not work well if the analyst is looking for approximate results.
- **Searching with Wildcards** – Wildcards searches overcome some of the errors and variation in the name, address, or other fields. It is very easy to use; however, users may find the results overwhelming because such searches often return too many irrelevant results that are hard to manage.

Many commercial software tools or database systems include search engine tools that provide advanced text search capability. FinCEN analysts employ these tools to conduct complex character matching and pattern matching to find more search results. FinCEN analysts have more than fifteen different searching algorithms designed to assist in their discovery of new data including basic “exact” and “first x characters match” and “last x characters match.” They also have access to complex quantitative string matching algorithms such as Jaro-Winkler, Levenshtein Distance, or Monge-Elkan algorithms which measure the similarity between two strings of information. These tools can provide unified results from multiple, simultaneous searches across data sources.

As the technology continues evolving, FinCEN would have many options among commercially available search tools that can satisfy its specific needs to identify more connections in the BSA data, funds transfers and other reports and documents.

Data Matching Against Other Data Sources

FinCEN currently uses a large number of databases to identify and analyze financial data. FinCEN information comes from four primary sources:

- the Bank Secrecy Act Database that contains SARs, CTRs, Currency and Monetary Instruments Reports, Foreign Bank Account Reports, and other reports;
- several databases of criminal reports sourced from, among others, the Immigration and Customs Enforcement’s TECS II system, the

FBI's National Criminal Information Center, the Drug Enforcement Administration's Narcotics and Dangerous Drugs Information and NDIC Systems, the United States Secret Service database, and the United States Postal Inspection Service;

- FinCEN's own database of investigations and queries conducted through FinCEN's systems; and
- Commercial database services from organizations such as Dun & Bradstreet, LEXIS/NEXIS, and credit bureaus,⁶³ as well as commercially available lists of "Politically Exposed Persons."⁶⁴

In addition, FinCEN analysts have access to other lists and databases maintained by federal government agencies that they may use to cross-reference BSA data, or as the basis of a search of the data. These sources include the Office of Foreign Assets Control's list of Specially Designated Nationals, the Social Security Administration's Death Master File, and the State Department's list of Designated Foreign Terrorist Organizations.

These additional data sources and the BSA data repository FinCEN currently maintains make it possible to conduct link analysis on funds transfers. FinCEN and many of its partner agencies in the law enforcement community have already assembled the data, technology, and expertise necessary to apply link analysis techniques.

Link Analysis

Link analysis is a technique used to explore associations among a large collection of data of different types. Link analysis requires a variety of readily available data, some of which provide indicators of money laundering activity (i.e., SARs, law enforcement data, case files, etc.). In the case of financial data, the connections might include names, addresses, phone numbers, bank accounts, businesses, funds transfers, and cash deposits. Combining and linking these pieces of data from multiple sources adds layers of understanding to the behavior that the data represents.

Link analysis depends on the integration of one or more sets of data records. Within each data set, each record has several data fields containing information. These might be records of an individual (with fields of name, address, and phone number), bank account (account number, owner, bank), or business (name, owners' names, board members, address). As noted, FinCEN already collects multiple Bank Secrecy Act reports, each containing specific data fields. While

⁶³ FinCEN only has access to credit bureau header information, not full credit reports. Header information typically consists of identifying information such as name, address, SSN, etc.

⁶⁴ See <https://www.world-check.com> and <http://www.worldcompliance.com>. Many government agencies and financial institutions employ such lists for intelligence and risk management purposes respectively.

there are many differences between them, there are also many fields common to the various reports. Likewise, even the limited pieces of data necessary to a funds transfer message overlap some of the information collected in these reports. Link analysis looks for matching fields in each of these records. For example, two reports identifying two separate individuals but each associating its subject with the same phone number as the other, could indicate that two persons know each other well, or even live at the same address.

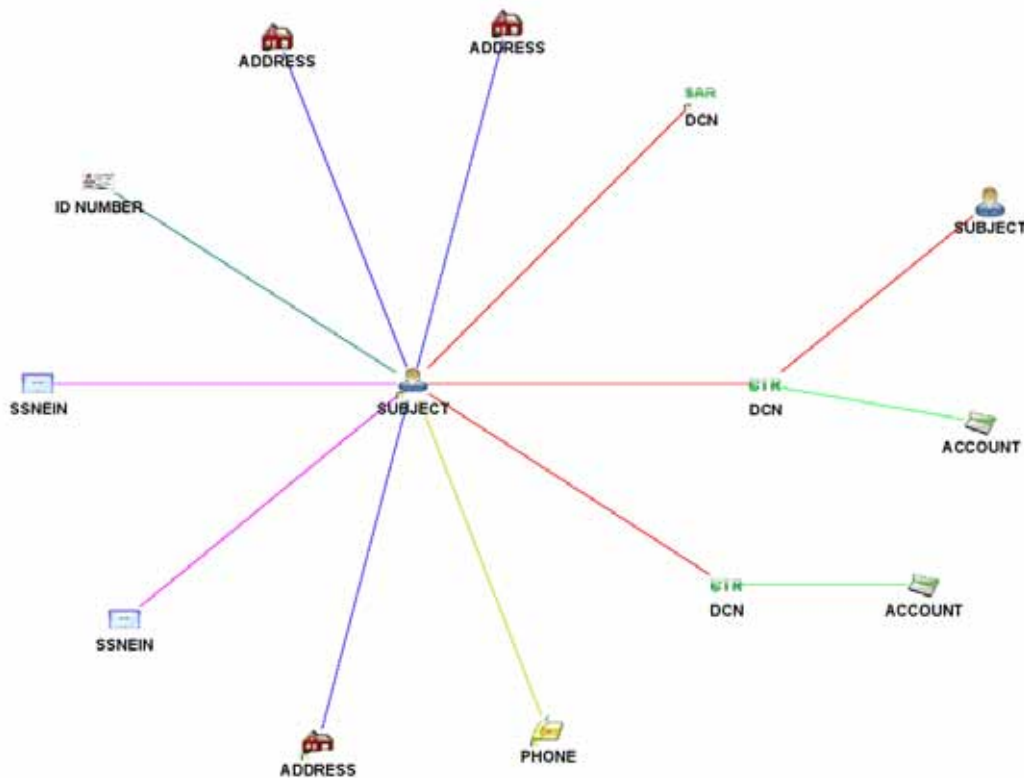
Link analysis can integrate many disparate sources of information. As noted, with the exception of SARs, the individual reports that FinCEN currently receives, and even the records that might be available through cross-border funds transfer reporting, provide few indicators of suspicion. However, link analysis provides a way of combining these different records so that analysts may detect the patterns and relationships between the different sets of data. FinCEN employs link analysis to identify relationships between the various BSA reports it currently collects.

FinCEN analysts use visualization software tools to develop a comprehensive and graphical representation of the link analysis results. The visualization tools assist the user in interpreting, identifying, and analyzing relationships from data by providing a visual mechanism that reflects relationships. These commercial software products help the users to visualize the correlation and association quickly through graphic representations, thereby reducing the amount of text that analysts must review and analyze. This tool provides a capability to represent the geographic relationships described in textual documents spatially.

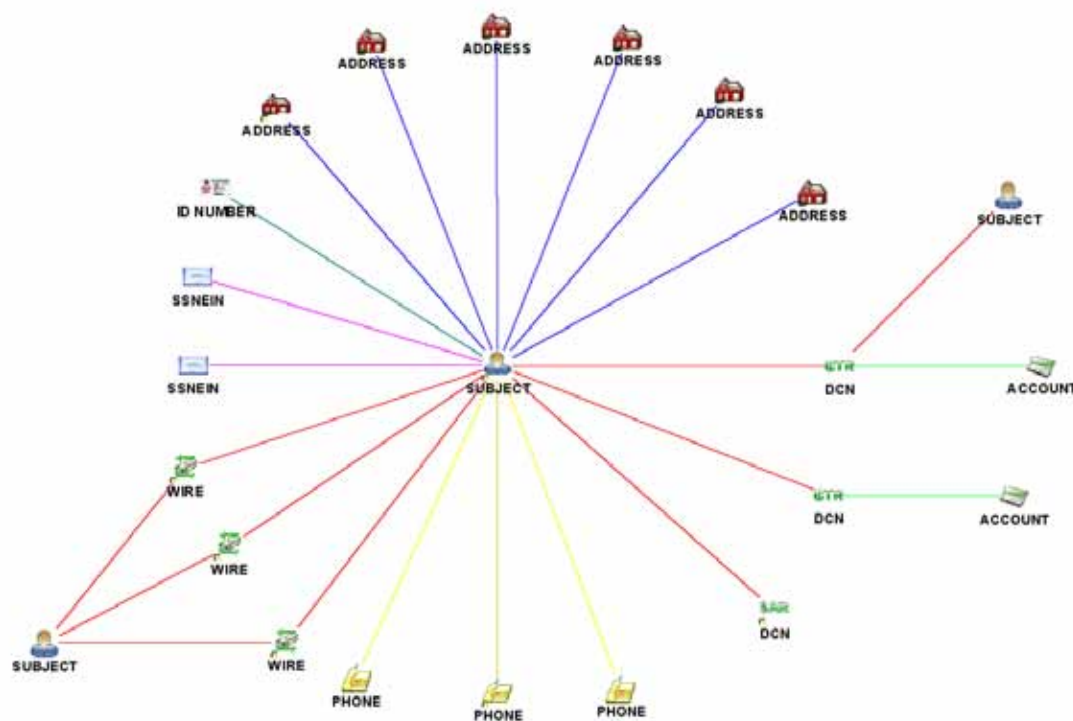
FinCEN has adapted an advanced analytical and visualization application that enables internal analysts to search and analyze the BSA data residing in more than a dozen databases. The link analysis tool compares transactions with each other and relates transactions to each other, for all transactions and transaction types, based on any reported item of information in a BSA filing. The tool has an icon-based, point and click interface with three-dimensional displays, multiple link chart views, easy exporting of subsets of data to other software packages, and allows for user annotations that can be private or shared. It enables graphical interaction with data to quickly expose patterns and discover new relationships. The tool relies upon an open architecture approach making it possible for FinCEN to customize it to support the additional funds transfer data.

The illustration below represents the kind of links and relationships FinCEN can identify by analyzing its current data sets. The example derives from actual analysis of a sample of BSA data currently maintained at FinCEN and represents the full extent of the links identified in that data. The illustration reflects that currently collected BSA data contained three BSA reports about the subject – two CTRs and one SAR. The contents of these reports reveal

that the subject offered three different addresses, two different bank accounts, and notably, two different Social Security Numbers when conducting the transactions. In addition, one of the CTR reports reveals a transaction or relationship between the subject and another person.

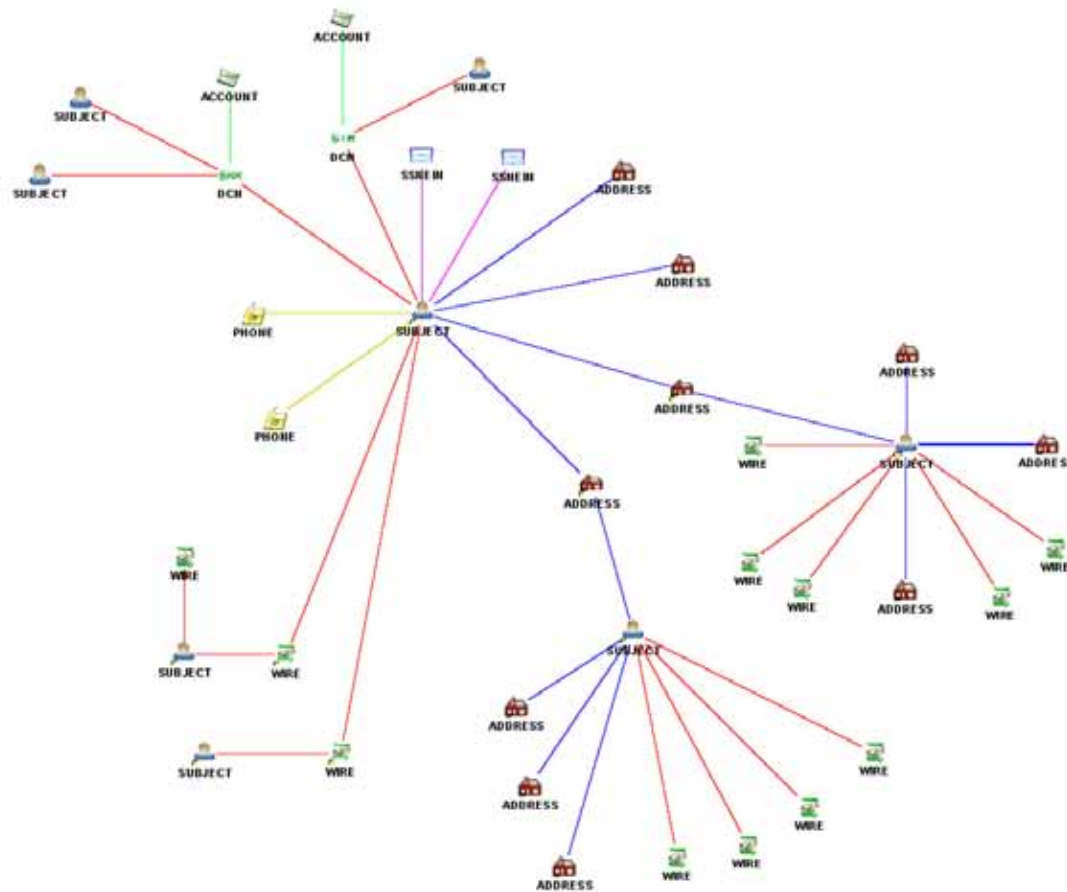


The addition of another set of data for the link analysis provides a richer context for the analysis, and a broader set of data containing potential links. Building upon the example illustrated above by adding electronic funds transfer data results in a far more detailed picture. The funds transfer data permits an analyst to identify additional relationships and parties and new accounts. Beginning with the chart above, which reflects the current BSA reporting, and adding electronic funds transfer data, reveals three additional addresses and two additional phone numbers that provide new investigative leads. It also reveals three specific electronic funds transfers between the subject and a previously unidentified associate not revealed in the current BSA reports.



Link analysis can help determine the focus of investigations and the proper allocation of resources. For example, if an analyst is researching a specific transaction by a specific person, link analysis across multiple financial data sources may reveal relationships between that subject and other persons. In turn, if the investigators already suspect those persons of involvement in illegal activity, additional investigation may be warranted. If, on the other hand, those relationships support the conclusion that the transaction fits a recognizable pattern of legitimate activity, the investigators need not expend any further resources.

In the following example, at least two associates of the primary subject would be unidentifiable absent the funds transfer information. In addition, each of those transfers provides a new starting point for further research.



Link analysis can identify and display the relationships between data sources. However, human analysts and investigators must make the judgments about whether those patterns reflect legitimate activities and relationships or suspicious financial activity. An additional layer of linking to other database records (e.g., criminal records, active or past investigations, etc.) can take the analysis one step further.

One challenge in this area is to have well-trained analysts to be able to thoroughly analyze the patterns discovered during the mining process and make sense of it. Some patterns are not statistically strong and some are very strong. The stronger the pattern is, the better chance that pattern will form a basis for exploitation. On the other hand, if the pattern is not strong today but its strength is increasing over time, then, this kind of pattern may be of great interest because it may be a clue as how to anticipate the illegal activity. Another problem is “false positives.” False positives may occur simply because there is so much data or, in the context of electronic funds transfer data, due to the lack of unique identifiers such as Social Security Numbers within the data. All these scenarios require experienced analysts to provide their knowledge to interpret the outcomes properly.

Cluster Analysis

Cluster analysis is another analytical method that FinCEN uses to determine underlying groupings that are not otherwise apparent in the data. The first step is the creation of basic clusters. For example, a subject may list an address and a phone number. Then a separate subject lists a different address but the same phone number. The clustering process would link these two subjects together based on the common phone number. In addition to names, phone numbers, and addresses, an analyst could repeat this process with driver's licenses, identification numbers, bank accounts, and any other data available. This type of clustering allows the analyst to determine the extent of the underlying connections within the data.

A more advanced form of clustering is to create a hypothesis regarding the anomaly an analyst is investigating. For example, in the United States there is a one-to-one relationship between individuals to Social Security numbers. There should never be more than one person identified with a Social Security number and a single person should never use multiple Social Security numbers. An analyst could retrieve, for example, all of the clusters of people and Social Security numbers where the cluster is "greater than five." This "greater than five" means any combination of people and Social Security numbers (one person connected to four Social Security numbers, two people connected to three Social Security numbers, etc.) This type of clustering allows the analyst to test a hypothesis to determine if the data supports the hypothesis.

As another example, analysts could design a cluster analysis of funds transfers based on discovering a pattern of activity that appears innocuous. An analyst could set a cluster analysis to alert on many different senders all wiring funds to the same recipient. The difference between this type of query and others is that this query focuses on identifying a pattern of activity rather than on a specific target. This alert could discover informal value transfer systems (hawalas), terrorist fundraising and other types of activity by identifying patterns of activity that appear not to have a legitimate business purpose.

Using the available BSA data, including cross-border funds transfers, cluster analysis might reveal patterns in the types of accounts, individuals, or organizations involved in certain cross-border transactions. For example, the currency and wire transactions of manufacturing firms might cluster closely together in comparison to other firms. Similarly, insurance companies might resemble each other closely in terms of their financial transactions. These clusters help analysts and investigators to identify predictable and recognizable patterns of legitimate transactions, and thereby identify patterns of financial transactions that are atypical. Identification of atypical transactions provides possible indicators of illicit activity. This quickly focuses the effort of the analyst or investigator by identifying those clusters that represent unusual activity that warrants attention. The analyst can then examine them more closely to determine whether the pattern represents suspicious activity.

Geographic Analysis

Geographic Information Systems (GIS) provide another visual interface by which analysts and managers can discover and assess patterns and relationships within massive amounts of data. GIS provides analysts with “situational awareness” and enables them to develop a fuller understanding of the data by illustrating the status of the data (i.e. how many Suspicious Activity Report documents did financial institutions file last month compared to previous months nationwide). It can even display emerging trends such as the filing of Suspicious Activity Reports by foreign locations of U.S. institutions. In addition, GIS-based situational awareness could identify the last reported location of all suspects named on Terrorist Financing Suspicious Activity Reports filed in the United States. Using temporal analysis, analysts can track relative increases and decreases in Suspicious Activity Reports on Terrorist Financing and understand how this type of data is changing over time – whether related to the location of the suspect or the location of the filer. Analysts can compare this information to relevant news reports and sensitive information provided by law enforcement.

Analysts can conduct even deeper analysis of the data by layering data called “themes.” These themes serve as overlays on a map and can add information such as average income, crime rates, financial institutions, ATM locations, roads, ports, immigration rates, or any other relevant data desired. This data can then be overlaid on top of Bank Secrecy Act and funds transfer data for consistency and hypothesis testing (i.e. if there are multiple similar locations where all of the layers are displaying the same relative activity, then the analyst could examine why one particular area is showing a huge increase in cross border funds transfers).

GIS can be both historical and predictive. Most traditional analyses relate to events that have already occurred while predictive modeling and forecasting attempts to understand the patterns of the past and making certain assumptions about the future environment. On this basis, analysts can attempt to predict the outcome at a certain point in the future. While these methods are not perfectly accurate, they are still valuable to quantitatively estimate the future situation and test hypotheses. These estimates can assist in strategic and tactical planning for those agencies that will take advantage of the BSA and funds transfer data.

There also are more specifically targeted controls like the United States Geographic Targeting Order (GTO). This authority (31 U.S.C. § 5326) allows the Department of the Treasury to impose stricter reporting and recordkeeping requirements on financial institutions for a limited period and in a specific geographic area. For example, the Department of the Treasury issued the first Colombian GTO in August 1996, and applied it to 12 money transmitters and 1,600 agents in the metropolitan area of New York, requiring them to report all cash transfers of over US\$750 to Colombia. Treasury renewed the initial order, which was valid for 60 days, six times to terminate in October

1997. It also extended the orders' coverage to 23 licensed transmitters and about 3,500 agents. The result of the Colombian GTOs was an immediate and spectacular reduction in the flow of drug trafficking proceeds to Colombia (down 30 percent in volume). About 900 money transmitters ceased their activity. Wire transfer data is especially conducive to this type of geographic analysis because, unlike our current BSA documents, wire transfer data provides a dynamic geospatial picture of money flow, in many cases indicating both the origin and final destination of the funds transfer.⁶⁵

Anomalies uncovered in funds transfers originating in money remitters located in the Washington Heights neighborhood of New York City to Colombia was one of the primary justifications for the Colombian GTOs. Geospatial analysis of BSA Data and more importantly, funds transfer data, can help analysts identify domestic areas of significant money laundering concern in support of U.S. GTO actions. Funds transfer data is especially conducive to this type of geographic analysis.

Benefits to Law Enforcement Operations

Obtaining useful information from financial institutions requires investigators to determine the most mutually productive search parameters, identify transactions relevant to a particular investigation, and determine whether the request is technically feasible for that financial institution. As the National Commission on Terrorist Attacks Upon the United States noted in one of its staff reports:

In a typical investigation, a financial institution received a grand jury subpoena or a National Security Letter (NSL) from a federal prosecutor or agent. The subpoena had a return date—the date by which the bank was required to produce the records requested. In a typical investigation, the bank searched its records and produced hard copies of the material requested. Banks and other financial institutions then needed substantial time to locate and produce records, even in response to a lawful subpoena. Financial institutions had been prohibited from giving law enforcement certain records absent compulsory legal process.⁶⁶

Investigative officials may also request information based on Suspicious Activity Reports (SARs). Financial institutions often file SARs on activities involving funds transfers. FinCEN's customers, including Federal, State and local law enforcement and regulatory agencies have direct access to certain SAR data through the existing BSA data systems. In addition, the filing financial institutions must produce any supporting documentation to FinCEN or the institution's federal functional regulator upon request, and may be required to provide that information to appropriate law enforcement officials upon request.⁶⁷

65 See, FATF-IX Report on Money Laundering Typologies, 12 February 1998, ¶ 28

66 Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States. p.59

67 See, e.g., 31 C.F.R. § 103.18(d), 103.19(e), (g), and 103.20(c)

To the extent that investigators can identify SARs that warrant further scrutiny, this provides one avenue for pursuing an investigation. Using link analysis, clustering, and other techniques, analysts and investigators with access to the BSA data (including cross-border funds transfer data) could more readily identify subjects and evaluate whether further investigation is warranted.

If a financial institution has filed a SAR, investigative officials with access to SARs can request, solely based on the SAR, that the financial institution provide underlying documents pertaining to the suspicious transaction. Supporting documentation may even include supplementary information resulting from the financial institution's own internal follow-up investigations with other parties to the transaction (e.g., information from their foreign correspondents).

In addition, some representatives from large-scale financial institutions, operating in the United States and often serving as correspondents in cross-border funds transfers, have indicated that correspondent financial institutions could make an effort to obtain certain customer specific information from foreign-based financial institutions.⁶⁸ A contributing factor in the receptiveness to such requests is the continuing global cooperation to counter terrorist financing and other criminal financial activity.

Along these lines, if investigative officials are able to identify⁶⁹ the foreign-based originator's or beneficiary's financial institutions that are involved in a given cross-border transaction, FinCEN may be able to help obtain additional information about the transaction. FinCEN, through its participation in the Egmont Group of financial intelligence units, and at the specific request of authorized officials, can contact those Egmont partners that may be able to retrieve relevant information.⁷⁰ If electronic funds transfer data were available through FinCEN the data could provide valuable leads in identifying foreign banks from which FinCEN may be able to obtain further information through its relationship with other FIU members of the Egmont group.

Section 314(a) of the USA PATRIOT Act of 2001 required the Secretary of the Treasury to adopt regulations to encourage regulatory authorities and law enforcement authorities to share with financial institutions information regarding individuals, entities, and organizations engaged in or reasonably suspected, based on credible evidence, of engaging in terrorist acts or money laundering activities. Pursuant to FinCEN's regulations, FinCEN developed a system that enables federal law enforcement agencies, through FinCEN, to reach

68 Indications received from some financial industry representatives are that these types of requests are increasingly common and that foreign institutions are increasingly receptive to such requests as global cooperation in anti-money laundering and counter terrorist financing efforts continues to improve.

69 E.g., through a domestic financial institution's records, funds transfer systems' message formats, or other independent means.

70 See appendix A for a description of the Egmont Group.

out to over 40,000 points of contact at more than 25,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering.

Another source, National Security Letters, are written investigative demands, somewhat analogous to administrative subpoenas that the Federal Bureau of Investigation may issue in counterintelligence and counterterrorism investigations to obtain the following:

- telephone and electronic communications records from telephone companies and Internet Service Providers (pursuant to the Electronic Communications Privacy Act, 18 U.S.C. § 2709);
- information from credit bureaus (pursuant to the Fair Credit Reporting Act, 15 U.S.C. § 1681u); and
- financial records⁷¹ from financial institutions⁷² (pursuant to the Right to Financial Privacy Act of 1978, 12 U.S.C. § 3401 *et seq.*).⁷³

Other federal government authorities may also issue National Security Letters to obtain financial records from financial institutions⁷⁴ for purposes of conducting foreign counter- or positive-intelligence activities,⁷⁵ certain protective functions,⁷⁶ or intelligence or counter-intelligence analyses related to international

71 Under the Right to Financial Privacy Act of 1978 (“RFPA”), “financial records” are defined as “an original of, a copy of, or information known to have been derived from, any record held by a financial institution pertaining to a customer’s relationship with the financial institution.” 12 U.S.C. § 3401 (2).

72 Section 374 of the Intelligence Authorization Act for Fiscal Year 2004 (Pub. Law 108-177 (Dec. 13, 2003) amended the definition of “financial institution” for purposes of the Right to Financial Privacy Act of 1978 (12 U.S.C. § 3414) to incorporate the definition of “financial institution” in the Bank Secrecy Act, 31 U.S.C. § 5312(a)(2) and (c)(1).

73 The USA PATRIOT Act changed the standard predicate for FBI RFPA National Security Letters to one requiring that the information being sought through the National Security Letter is “for foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment of the Constitution of the United States.” The USA PATRIOT Act also provided authority of the Director of the FBI to delegate signature authority for National Security Letters to Special Agents in Charge serving in designated field divisions.

74 In *Doe v. Ashcroft*, 334 F. Supp.2d 471 (S.D.N.Y. 2004), a federal district court held that 18 U.S.C. § 2709, which authorizes the issuance of national security letters to Internet service providers, is unconstitutional on account of its nondisclosure provisions and lack of judicial review. The Federal Bureau of Investigation appealed the decision and obtained a stay pending appeal, so it is continuing to issue national security letters under that statute. That decision did not adjudicate the constitutionality of the statute authorizing the issuance of national security letters to financial institutions, 12 U.S.C. § 3414.

75 Foreign counter- or positive-intelligence activities could include, for example, the audit of customer records of a financial institution related to the clandestine activities of an intelligence agency, pursuant to the RFPA, 12 U.S.C. § 3414(a)(1)(A). See, e.g., *Duncan v. Belcher*, 813 F.2d 1335, 1339 and 1339 n. 1 (4th Cir. 1987).

76 The RFPA, 12 U.S.C. § 3414(a)(1)(B), permits certain disclosures of financial records to the United States Secret Service for the purposes of conducting its protective functions.

terrorism.⁷⁷ National Security Letters are highly confidential investigative tools employed by the federal government. Financial institutions that receive National Security Letters must take appropriate measures to ensure the confidentiality of the letters. FinCEN encourages financial institutions to have procedures in place for processing and maintaining the confidentiality of National Security Letters.⁷⁸

Even with this kind of information available through these various established channels, the retrieval and analysis of such information can be difficult, and is usually time-consuming. Once an investigator identifies the information he or she wants, a subpoena or warrant must issue. Responding institutions must identify, extract, and prepare the relevant data for delivery to the investigator. Many institutions resist providing such information in electronic form, which results in the need for investigators or their support personnel to manually review the data and enter it into computers to aid in their analysis. This entire process can take weeks or even months to reach a point at which investigators and analysts can make use of the data. Another possible problem is that an investigator may be reluctant to turn to a particular financial institution at the outset of an investigation to inquire about the suspect's financial activities (i.e., suspected internal infiltration at the financial institution and concerns about possible intentional or inadvertent "tip-offs" to the suspect customer).

Some of the funds transfer systems can be potential sources for searching and retrieving funds transfer messages via subpoena. Law enforcement officials inform us that it can be difficult and time consuming to find funds transfer records after the fact in order to reconstruct the flow of money unless the investigators know the name or account number, the time and place of origin, or other specific characteristics of the transactions. Housing cross-border electronic funds transfer data at FinCEN could make such records available for efficient extraction of the needed information.

Below, we present information provided to us by representatives from other government agencies involved in efforts to detect, prevent, and prosecute illicit financial activity.

Federal Bureau of Investigation

As is typical among law enforcement, FBI agents begin with information developed in the course of an investigation and seek additional data through subpoenas to financial institutions and the message service providers, and National Security Letters. The information the FBI typically requests may

77 The RFP, 12 U.S.C. § 3414(a)(1)(C), permits certain disclosure of financial records pursuant to a request from a federal government agency authorized to conduct investigations or intelligence or counter-intelligence analyses related to international terrorism.

78 Pursuant to 12 U.S.C. § 3414(a)(3) and (5)(D), no financial institution, or officer, employee or agent of the institution, can disclose to any person that a government authority or the FBI has sought or obtained access to records through an RFP National Security Letter.

include “any and all documentation related to certain specified transactions” to include originator and beneficiary information, dates and amounts of transactions, any special instructions or notes included on the record, sender and recipient bank names, account numbers and ABA numbers and other internal codes. These records often arrive in paper format that then requires additional resources to input the information into analytical systems. Much of this information would reside in the proposed system, providing FBI and other law enforcement agencies ready access and thus saving considerable time and effort in the initial stages of a financial investigation. The identification of the overseas accounts used in cross-border transfers also facilitates the preparation of requests for information from foreign governments under Mutual Legal Assistance Treaties (MLAT) and via Letters Rogatory. The resulting records of which provide other leads and identify others connected to the subjects. The identification of overseas relationships in the data could also serve as a catalyst for the exchange of information between FinCEN and its international counterpart FIUs throughout the world.

The FBI currently has the ability to analyze large amounts of data from numerous sources. Under a Memorandum of Understanding between FinCEN and the FBI, FinCEN provides wholesale access to its archive of BSA reports. In turn, the FBI loads the data into its Investigative Data Warehouse (IDW) and finds the links between the data sets. The IDW is a centralized, web-enabled, closed system repository for intelligence and investigative data. This system allows appropriately trained and authorized personnel throughout the country to query for information of relevance to investigative and intelligence matters. In addition to the BSA data provided by FinCEN, IDW includes information contained in myriad other law enforcement and intelligence community databases. One of the many offices within FBI that makes use of the IDW is the FBI’s Terrorist Financing Operations Section (TFOS).

The FBI believes that TFOS allows for (1) consistency of financial investigations and the assurance that every major terrorism case will have a financial investigative component; (2) the establishment of effective working relationships with international banking, law enforcement, and intelligence communities; (3) the development of a real-time financial tracking capability, resting in large part on the FBI’s extensive relationships with the financial community, which has transformed financial investigations from the traditional, methodical, slow-paced analysis to a tool that can provide near real-time information in urgent situations; and (4) the formation of teams that can be sent to field offices to bolster document-intensive financial investigations and provide guidance and leadership on conducting financial investigations.⁷⁹

The benefits of IDW include the ability to efficiently and effectively access multiple databases in a single query. As a result of the development of this robust information technology, a review of data that might have previously

79 Monograph on Terrorist Financing, National Commission on Terrorist Attacks Upon the United States, p. 41-42

taken days or months now takes only minutes or seconds. According to the FBI, the BSA information has provided a tremendous lift to the FBI's investigative missions, particularly as they relate to terrorist financing. The cash reporting and suspicious activity reporting in particular are proving to be of significant value. FBI officials believe the potential benefits of the addition of cross border funds transfer information into this type of analysis are incalculable.

Financial information, lawfully acquired, significantly enhances the ability of U.S. law enforcement and intelligence community members to overcome defects in financial transparency as mentioned in the previous excerpt from the USA PATRIOT Act. Likewise, BSA data is of incalculable value in this important effort. When combined with other data collected by the law enforcement and the intelligence community, investigators are better able to "connect the dots."

More recently, BSA data has proven its utility relative to counterterrorism matters. For example, BSA data is used to obtain additional information about subject(s) under investigation and their methods of operation. Analysis of BSA data permits counterterrorism investigators to acquire biographical and descriptive information, to identify previously unknown subject associates and/or co-conspirators, and, in certain instances, to determine the location of subject(s) by time and place.⁸⁰

Drug Enforcement Administration

In a tactical or case-by-case context, DEA officials noted that each time DEA subpoenas records, the records provide leads that merit further subpoenas. However, this is an extremely time-consuming process. Given ready access to cross-border funds transfer data, DEA analysts could quickly track illicit funds through the financial system, greatly enhancing and streamlining their investigative capabilities. For example, this would potentially allow DEA investigators to penetrate the Black Market Peso Exchange (BMPE) process for laundering drug proceeds by tracing funds through the system from the U.S. exporter back to the source.

DEA officials stressed that every time they identify a financial target individual, business, or bank account, the cross-border funds transfer data would enable them to identify associated accounts, businesses, co-conspirators, nominees, the volumes of money involved, offshore partners, etc. Intelligence gleaned from cross-border funds transfer data could provide a basis for subpoenas to CHIPS, Fedwire, money transmitters, or other individual financial institutions.

DEA officials opined that a database such as this would allow them to attack the layering stage of the laundering process in ways that are currently unavailable. Investigators could tie together different investigations and identify shell/front companies, nominees, previously unidentified co-conspirators, etc. DEA representatives noted that because DEA is currently obtaining this information

80 Special Agent Michael Morehart, Section Chief, Terrorist Financing Operations Section, Federal Bureau of Investigation, before the U.S. House of Representatives Committee on Financial Services, May 26, 2005

on a case-by-case basis, they cannot easily identify “trends” per se. The analysis of a macro dataset of interbank transfer records could result in the identification of these trends. With the data, FinCEN could perform this kind of strategic trends-and-patterns analysis and provide the results to DEA and FinCEN’s other partners.

Intelligence-driven investigations and coordinated, strategic enforcement initiatives are essential components of the Organized Crime Drug Enforcement Task Force (OCDETF) Program. Each year OCDETF strives to focus on investigations of the highest priority regional, national, and international targets. OCDETF disseminates information generated from those investigations to law enforcement quickly and in a manner that allows for the maximum impact against drug trafficking and money laundering activity. To do this effectively, intelligence must drive enforcement efforts. OCDETF participants must have the ability to access, link, and interpret voluminous intelligence information from the OCDETF member agencies and from others in the drug law enforcement community. OCDETF provides a mechanism to disseminate and receive leads that will aid in the development of coordinated, multi-jurisdictional investigations targeting all related components of drug trafficking enterprises operating worldwide.

To enhance OCDETF’s overall capacity to engage in intelligence-driven enforcement, OCDETF created the OCDETF Fusion Center (OFC) – a comprehensive data center containing all drug and related financial intelligence information from six OCDETF-member investigative agencies, the National Drug Intelligence Center and FinCEN. The OFC is designed to:

- Conduct cross-agency integration and analysis of drug and related financial data,
- Create comprehensive intelligence pictures of targeted organizations, including those identified as Consolidated Priority Organization Targets (CPOTs) – the United States’ “most wanted” international drug and money laundering targets – and regional priority targets,
- Pass actionable leads through the multi-agency Special Operations Division (SOD) to OCDETF participants in the field, and,
- Develop and coordinate, multi-jurisdictional OCDETF investigations of the most significant drug trafficking and money laundering networks.

A primary objective of the OFC is to assist the OCDETF Program in focusing on the financial components of the most significant drug trafficking organizations influencing the U.S. drug supply. It is a requirement that every OCDETF investigation include a financial component within six months of receiving designation as an OCDETF investigation. The OFC will greatly increase

OCDETF's ability to disrupt and dismantle major organizations, including their financial components.

While in its infancy, the OFC has already assembled a team of senior agents and analysts from the OCDETF member agencies who are working to develop the protocols and procedures for OFC operations. The OFC expects to reach an initial operating capability in mid- 2006 when the technical infrastructure that supports the Center will be complete.

United States Secret Service

According to officials with the U.S. Secret Service (USSS), access to funds transfer data provides critical well-documented evidence of wire fraud, funding of digital and electronic currency accounts via MSBs and other electronic funds transfers, funds transfers associated with "account takeovers," telemarketing schemes, and other crimes within their jurisdiction. Accessing funds transfer data and tracking the data allows the USSS to determine whether money laundering is occurring and what suspects are involved, as well as providing documented evidence of criminal activity. However, this access has been extremely limited and has presented obstacles to investigators' efforts to gather evidence. Like the other law enforcement agencies, USSS points out that ready access to cross-border funds transfer data would significantly enhance the development of new investigative leads, increase and improve the validation of known investigative leads, allow proactive identification of suspects, locations and contraband, corroborate existing investigative leads, and generally add to the body of criminal intelligence information in support of the Secret Service investigative mission.

In the specific context of telemarketing schemes, USSS notes that schemes that originate from Canada and target U.S. victims often involve the movement of funds from the U.S. victim's accounts to the Canadian perpetrator's accounts. The transfers often flow from bank to bank or via MSBs. Organized criminal groups are also frequently using "the border" between two countries as a way of insulating themselves from investigators who normally will not investigate international cases. Typically, investigators will first pursue leads that they can quickly verify or dismiss. Pursuing leads related to cross-border activity are usually time consuming, involve extensive "red tape," and thus are assigned a lower priority. According to USSS officials, anything that can eliminate the bureaucracy and allow for quick resolution of leads would be useful. This additional information on the money laundering aspects of known criminal organizations could provide the extra information needed to decide if the organizations are large enough to warrant the necessary budget and labor allocation needed for a proper investigation.

USSS also notes that most, if not all, white collar and drug smuggling criminal organizations in Vancouver and western Canada primarily target the U.S. for criminal activity. The reasons for this are the close geographic proximity

between Vancouver and the U.S., the large population and financial base of the U.S. as compared to Canada, and differences in criminal penalties. In virtually every investigation of these groups, the movement of the proceeds of the criminal acts from the U.S. back to Canada, whether by movement of bulk cash, funds transfers, or stored value cards, has been significant. If FinCEN were to collect cross-border funds transfer reports, this kind of investigation would present a prime opportunity for FIU-to-FIU exchange of information between FINTRAC and FinCEN for example, expanding the analytical and investigative reach of the U.S. government in cross-border investigations

Department of Justice – Asset Forfeiture and Money Laundering Section

In addressing the current tools available to pursue investigation and analysis of funds transfers, Department of Justice officials echoed the same concerns raised above about the difficulty and time involved in obtaining electronic funds transfer data for investigations. Initially, a subpoena would issue requesting records of specific funds transfer activity (specific customers, specific amount thresholds) for a certain time period. The request should include all activity from named-originators or named-beneficiaries. Department of Justice officials noted that many financial institutions resist providing this information in electronic format.

The Department officials also noted that investigating crime is labor intensive and costly. In order to perform meaningful analysis of such data, investigators would need to have an open grand jury with subpoena power or have a search warrant issued by a magistrate judge. Once investigators receive bank statements based on a subpoena, the next challenge is to build a database of transactions. Details of originators and beneficiaries are essential. Each of these challenging phases of investigation is demanding and time consuming. Because delays are common, some investigative cases are shut down without adequate analytical support due to inadequate compliance by financial institutions.

Again, aggregating a collection of cross-border electronic funds transfer data in a central repository can mitigate, at least in part, the concerns highlighted by the Department of Justice. Access to this data by investigators can significantly reduce the time and labor involved in establishing a foundation for sophisticated financial investigations.

U.S. Department of Housing and Urban Development - OIG

The Department of Housing and Urban Development's Office of the Inspector General (HUD-OIG) investigates fraud against the programs administered by the Department. In this role, HUD-OIG sees numerous mortgage fraud and grant program frauds that involve the transmission of the proceeds outside the U.S. by funds transfer. HUD-OIG officials emphasize that they anticipate significant potential fraud against the programs designed to aid those impacted

by Hurricane Katrina. In the typical program fraud investigated by HUD-OIG, monies disbursed by HUD never fulfill their intended purposes, but rather, once deposited in the Management Agent's bank accounts, simply disappear. Investigations may reveal false invoicing and other schemes to cover the fraud, but HUD-OIG lacks ready access to, or the legal authority to obtain, relevant bank records to determine the disposition of the misappropriated funds. In a large number of their investigations, HUD-OIG uncovers allegations that perpetrators transferred the misappropriated funds overseas, but cannot obtain the evidence necessary to track the money any further. As an Inspector General's office, HUD-OIG must rely on other federal law enforcement agencies, which suffer their own resource allocation restraints, to obtain the legal process necessary to investigate further. Lacking more detailed evidence, HUD must often resort to open-ended orders for restitution in an often vain attempt to recover the losses.

HUD-OIG officials expressed the opinion that access to a database that included simple information such as the sender and recipient names, account numbers, institutions, and the dates and amounts of funds transfers out of the U.S. would provide HUD-OIG with prima facie evidence of the misuse of the funds. Such information would aid HUD-OIG in establishing the true extent of the losses suffered by HUD programs, recovering assets through asset forfeiture, and ensuring that these vital program funds reach those in need for whom they are intended.

U.S. Department of Agriculture - OIG

Officials of the U.S. Department of Agriculture's Office of Inspector General (USDA-OIG) expressed the opinion that they would benefit from cross-border funds transfer information, especially in investigations involving fraud in food stamp electronic benefits transfer (EBT), stolen infant formula, and export loans. For many years, USDA-OIG has seen large amounts of misappropriated program money transferred out of the country, usually overseas but sometimes to Canada and Mexico. Some stores accepting food stamps also serve as money services businesses to facilitate transferring these funds through money orders and funds transfers to banks or individuals in other parts of the country or overseas.

Funds transfers also appear in some cases to be replacing cross-border currency shipment. One recent search located many CMIRs involving the subjects/companies 5-10 years ago, but almost none recently, while several more recent SARs mentioned significant funds transfers by some of the parties to foreign banks.

USDA-OIG officials also echoed the opinion that traditional methods of obtaining information about electronic funds transfers are almost universally time- and labor-intensive, and in many cases ineffective. One USDA-OIG agent stated that, "It would be very useful for our agents to have direct access to cross-border funds transfer data to be better able to track where the funds are being sent and by whom and to more easily check if, indeed, this is occurring in their cases."

Internal Revenue Service – Criminal Investigation Division

The Internal Revenue Service Criminal Investigation Division (IRS-CI) has varied responsibilities and authorities under the BSA, including criminal enforcement of the tax laws, criminal enforcement of certain provisions of the BSA, and enforcement of federal money laundering statutes. IRS-CI accomplishes these tasks through a variety of programs such as its Suspicious Activity Report (SAR) Review Teams, its participation in the High Intensity Drug Trafficking Area (HIDTA) and High Intensity Money Laundering and Financial Crimes Area programs (HIFCA) and the IRS' fraud referral program. From fiscal year 2001 through fiscal year 2005, approximately 32% of IRS-CI's investigation time was devoted to money laundering-related investigations. IRS-CI's money laundering investigations involve a wide variety of predicate offenses including narcotics trafficking, health care fraud, gambling, and all manner of confidence and investment schemes.

The review and analysis of BSA data is a mandatory procedure in every IRS-CI criminal investigation. In fiscal year 2005 IRS-CI devoted approximately 15% of its investigative time to BSA related investigations. From fiscal year 2003 through fiscal year 2005 IRS-CI initiated in excess of 1,500 investigations from BSA data, BSA related projects and/or targeting BSA violations such as structuring and the operation of illegal MSBs.

As part of its compliance strategy, IRS-CI has designated Lead Development Centers (LDC) that focus on specific IRS-CI program areas. Investigative analysts in these LDCs access a variety of databases in the development of leads for criminal investigation. One of the programs within the LDC structure is BSA analysis. The LDCs provide support to IRS-CI and the Small Business/Self-Employed (SB/SE) BSA Compliance Examination program (see below) through identification of cases with trends, patterns and issues associated with income tax violations, money laundering and other financial crimes covered under the BSA.

Some of the objectives of the LDC program related to BSA include the following:

- Identification of income tax violations and money laundering violations for criminal or civil referral.
- Identification of newly emerging income tax violations, money laundering methodologies and trends through research and analysis.
- Identification of MSBs that are actively involved in or facilitate income tax violations and money laundering.

One key weapon in the LDC's arsenal is a powerful data mining tool. This system provides users with an enhanced capability to simultaneously access, analyze, and interpret large volumes of disparate data for the purpose of identifying and developing leads to criminal cases and asset forfeitures. This

program is unique in that it is linked to a variety of databases including its Currency and Banking Retrieval System (CBRS) and tax return information that is generally unavailable to other Federal, state and law enforcement agencies.⁸¹ This program also allows for the identification of connections in the information contained in different databases. Information such as that provided in cross border funds transfers could be combined with BSA data and tax return information in a program such as the IRS-CI's data mining tool. This information could further enhance the development of leads identified in these other databases.

IRS-CI officials inform us that it encounters funds transfers in many of its investigations in all program areas, including abusive trust schemes, money laundering, BSA, health care fraud, confidence and investment frauds, narcotics, and others.

Analytical Value – Canada

In contrast to FinCEN's operations, FINTRAC's analysis is entirely a proactive analysis. Canadian law enforcement and national security agencies cannot request that FINTRAC conduct specific analyses and do not have direct access to FINTRAC's databases. To develop its analysis and disseminate the results, FINTRAC's system applies business rules developed internally to assess its "Suspicious Transaction Reports" (STRs) and other intelligence information by correlating the STR data fields with data in the "Large Cash Transaction Report" (LCTR), Cross Border Currency, and "Electronic Funds Transfer" (EFT) databases. This process results in a score for each STR based on the links between that STR and other reports in the FINTRAC databases (i.e., same subject, account, etc.).

Every day, FINTRAC analysts review incoming STRs and other intelligence to determine whether to open a "case." Upon opening a case, analysts review the FINTRAC database information, and then conduct further research using all source information and link analysis, the results of which the analyst compiles into an Analytical Report and Disclosure Statement. A Senior Management Committee within FINTRAC must review and approve all Disclosure Statements before FINTRAC releases the report to law enforcement or national security agencies.

Each year, FINTRAC discloses approximately 140 analytical reports, approximately 30 of which are "Terrorist Financing" disclosures. FINTRAC officials informed us that, on average:

- Among money laundering disclosures, the majority are primarily domestic, while about one third contain international EFT data and could not be disclosed without that data;

⁸¹ But see 26 U.S.C. § 6103 (prescribing the circumstances under which specified persons and agencies may obtain federal tax returns or return information).

- Among Terrorist Financing disclosures, almost 80% contain international EFT data.

Analytical Value – Australia

AUSTRAC provides the Australian Taxation Office and specified law enforcement, security and revenue agencies with both general and specific access to the FTR information it collects. The general access, governed by memoranda of understanding, is by way of controlled on-line access to the data and, where appropriate, by extracts of parts of the data holdings. This allows AUSTRAC's partner agencies to add the financial intelligence to their own intelligence for a better understanding of the activity.

Officials from the Australian Federal Police (AFP), Australian Taxation Office (ATO), and the Australian Customs Service (ACS) all report that IFTI data available through AUSTRAC are integral to their investigative strategies, and both AFP and ATO have made the use of AUSTRAC data mandatory in the development of cases by their investigators. The Australian Federal Police, for example cite the data as the central piece in its attempts to not only identify, but to predict the movement of narcotics into and out of Australia. By analyzing patterns within the IFTI data and comparing it to other law enforcement information, including entry/exit data from the ports of entry, the AFP can identify recurring patterns of outgoing funds transfer activity based on historical cases and lay plans to interdict narcotics based upon patterns of funds transfer activity.

The ATO stated that IFTI data is an integral part of the ATO's overall strategy to deter the movement of money to offshore tax havens. The ATO has expended considerable effort in identifying jurisdictions, primarily tax havens that Australian taxpayers may use to avoid taxes. General trends and patterns analysis helps describe the overall flow of funds to and from Australia, and helps analysts develop a baseline profile of funds transfer activity. The very volume of the reporting enhances its value to ATO by providing a richer context for analysis. In turn, this enables analysts to identify and analyze apparent anomalies. Based on this information, ATO can concentrate on funds transfers to jurisdictions that raise concern.

One of the monitoring tools AUSTRAC utilizes highlights monthly variations in the flow of funds between Australia and other countries. AUSTRAC provides a monthly report to an ATO analyst who examines it for unusual transactions or trends (normally involving tax havens). In one case, an ATO analyst noted a sizeable increase in funds sent to Australia from a small tax haven country during a particular month. Further investigation identified that a particular individual had been receiving a large amount of these funds and had received around \$18 million (AUD) over the past 5 years.

Checks on tax records showed that the subject individual had not lodged returns for a number of years and ATO had to ascertain if the subject was an Australian resident and thereby establish if the \$18 million (AUD) was assessable income for Australian taxation purposes. Interviews with the subject established that he was a professional gambler who had developed a program to select winning horses for a business that operated from an offshore tax haven. Immigration checks on his international movements confirmed that the individual was not an Australian resident for Income Tax purposes. This research indicated a link between the subject and the United States.

ATO decided to provide the information they obtained during the course of the audit to the IRS. ATO provided the information under the Exchange of Information provisions of the Australia/United States Double Tax agreement.

On receipt of the information, the IRS conducted their own investigation and identified undeclared income of approximately \$32 million (USD) with uncollected tax and interest of \$9 million (USD). Three ATO officers received formal commendations from the IRS for their part in the investigation.

In addition, analysts are able to identify potential subjects based on volume, value, and geographic links. ATO has identified jurisdictions, including tax havens, and can monitor funds transfer activity between Australia and those jurisdictions for indicators of concern or suspicion. The information gleaned from such analysis helps ATO identify tax return information that warrants review. ATO updates its baseline analysis and outlier identification monthly. Among 21,000 ATO employees, 1,300 have direct access to the AUSTRAC data on their desktops, representing 48% of all AUSTRAC's external users. In FY '05, ATO made assessments for \$62 million (AUD) in back taxes and penalties in 499 cases developed from the AUSTRAC data. Over the past four fiscal years, ATO assessments have totaled over \$269 million (AUD). Of the assessments ATO makes based on AUSTRAC data, approximately 70% relate to IFTI data.

The ATO has been using AUSTRAC data to support its compliance activities since the early 1990s. The data provides an important source of financial intelligence for the ATO and has been used to:

- monitor money movements into and out of Australia;
- profile individuals, industries, occupations and geographical areas;
- identify potential high-risk transactions;
- identify and quantify compliance risks and develop compliance strategies;
- assist in the selection of compliance cases for further investigation;
- debt collection.

ATO relies on its analysis of AUSTRAC data in a number of ways to shape and direct its operational activities. ATO representatives explained to us that the agency uses AUSTRAC's IFTI reports for

- Case Selection -- ATO correlates AUSTRAC data (including IFTIs) with other information to determine whether a case is suitable for audit.
- Case Profiling -- ATO analyses AUSTRAC data (including IFTIs) to develop a financial profile of taxpayers already selected for audit.
- Debt Collection -- ATO queries AUSTRAC data (including IFTIs) to identify previously unknown bank accounts, undisclosed funds and new addresses or other information to help trace a taxpayer's whereabouts.

ATO also employs the IFTI data in its strategic analysis aimed at identifying and assessing potential revenue risks, such as tax havens. ATO analyses IFTI data to monitor money flows into and out of tax havens and highlights statistical anomalies for further investigation.

Representatives of the Australian Customs Service (ACS) emphasized that the IFTI data, standing alone, provides a useful starting point for identifying potential subjects. ACS uses IFTI data to develop a picture of the flow of funds into and out of Australia. By first identifying patterns and clusters of activity in the IFTI data, ACS can eliminate those patterns that are explicable on their face. By combining otherwise inexplicable patterns of activity with other law enforcement information such as immigration entry/exit data and trade data, ACS can prioritize its leads and identify patterns of activity that warrant further scrutiny. ACS has applied this methodology to investigations of narcotics trafficking, trade-based smuggling, and human trafficking with great success.

Benefits to Financial Industry Regulation and Compliance

In addition to its own analytical work and direct case support to law enforcement, FinCEN also provides analytical support to its regulatory partners. One example of FinCEN's support role is the conduct of targeted research of the reporting and compliance activity of identified institutions. Currently, FinCEN's Office of Regulatory Analysis can research the available BSA data related to a specific institution by extracting the reports filed by that institution. FinCEN analysts can then compare the data with other related reports submitted by other institutions. For example, analysts can review the SAR filings of an identified institution initially, and then extract SARs filed by other institutions related to transactions with the identified subject institution or its customers. Identification of transactions that other institutions identified as suspicious that the subject institution did not similarly report may provide some insight into possible compliance issues or weaknesses in the subject institution's anti-money laundering program. FinCEN can in turn provide the results of its analysis to the delegated regulators to aid in the conduct of examinations. The addition

of cross-border funds transfer data to the universe of BSA data would provide many of the same benefits in this application as it would in law enforcement-related analysis described above.

This type of analysis affords FinCEN many opportunities to enhance the use and utility of BSA data. First, it could provide FinCEN the opportunity, through the kinds of analysis described, to find indicators of compliance problems through proactive analysis. This capability would place FinCEN in a position to identify problems in the BSA reporting regime and the way financial institutions are implementing their AML programs. If this effort identifies the problems at an early stage, FinCEN, working with the functional regulators and the institution, can attempt to correct the problem. Combining electronic funds transfer data with BSA reporting and information gleaned from examinations by the functional regulators can theoretically enable the government and the financial services industry to address compliance and AML issues early. This would provide all involved the opportunity to correct AML compliance, and ensure the quality of overall BSA reporting, thus enhancing the transparency of the financial system. Effective use of the data in this way could aid in the overall efforts to combat illicit finance and potentially reduce the need for significant enforcement actions.

Internal Revenue Service – Small Business/Self-Employed

In general, under the BSA the IRS' Small Business/Self-Employed Division (SBSE) is responsible for examining non-bank financial institutions (NBFIs) not regulated by another federal agency for compliance with the BSA. These institutions include Money Services Businesses (MSBs), casinos, non-federally insured credit unions, dealers in precious metals stones or jewels, and insurance companies regulated under the BSA. In addition to compliance and examination responsibilities, IRS-SBSE is responsible for the identification of unregistered MSBs and educational outreach on NBFI BSA obligations. The difficulties in regulating and even in defining the money services business sector of the financial services industry are well known. While a substantial proportion of money transmitters are legitimate and law-abiding operations, IRS-SBSE and FinCEN face difficulty in identifying money transmitters that are neither registered as required nor in compliance with the BSA's anti-money laundering program requirements.

IRS-SBSE already makes effective use of CTR data in identifying businesses that make large cash deposits indicative of the operations of a money transmitter. However, that data, standing alone, has limitations. In an example posited by IRS-SBSE officials, a retail business that operates a money transmitting service as only part of its business, may be identified by its bank as a retail business but not as an MSB. As a result, a CTR related to transactions by that business identifies the account holder as a retail business. On its face, the CTR may not warrant further examination, because a retail business may

routinely take in large amounts of currency. However, the additional layer of understanding developed when combined with funds transfer data reflecting corresponding international funds transfers, may alert analysts or investigators to a problem. By combining the identifying information in the CTR and funds transfer data, with information available from IRS-SBSE's database of non-bank financial institutions for example, IRS could theoretically identify unregistered money transmitting businesses. Furthermore, employing geographical analysis techniques, IRS-SBSE, either independently or in cooperation with FinCEN could develop maps of financial activity that indicated suspicious or otherwise inexplicable geographic concentrations of the kinds of transactions that might indicate unregistered money transmitters.

As in other examples cited throughout this study, this kind of analysis has the potential of providing great benefits in conducting a "triage" of available leads, and in allocating analytical, investigative, and examination resources.

Benefits to State and Local Government Partners

Our conversations with representatives of state and local law enforcement and regulatory agencies reveal many of the same benefits that our Federal partners envision. However, the nature of the state and local agencies' work raises additional concerns that a cross-border electronic funds transfer database may mitigate. For example, while state and local authorities face many of the same difficulties in deriving useful information about funds transfer activity from subpoenas, they face additional difficulties related to their own geographic jurisdiction. The ease with which financial activity can cross international borders is mirrored in interstate commerce. Targets of a state or local investigation can easily conduct business with associates in other states or countries. State and local officials shared with us that they increasingly face resistance from financial institutions to subpoenas for records related to transactions involving out-of-state subjects that arise in their investigations. In addition to providing the same time and labor savings as at the Federal level, state and local authorities may enjoy the added benefit of avoiding protracted legal maneuvering sometimes required to obtain even the most basic investigative information.

State and local authorities also echoed the concerns of some federal investigators related to various types of fraud schemes. State and local authorities dedicate a significant amount of resources to investigating seemingly localized fraudulent financial schemes. Despite the local pool of victims, it is no more difficult for these criminals to employ the international financial system to spirit their proceeds out of reach of the state and local authorities. The investigators we spoke to noted, however, that the types of fraud schemes they investigate involve transactions that lend themselves to pattern analysis. A database of funds transfer data would provide a source for this kind of analysis in support of state

and local efforts to protect their citizens from fraud and would further enhance the Bank Secrecy Act data and other sources already available to them.

Benefits to Financial Services Industry

Another example of the utility of funds transfer reporting stems from recent efforts at FinCEN to establish information sharing agreements with the functional banking regulators. Under the program, the regulators provide FinCEN with the findings made during the conduct of examinations. The Office of Regulatory Analysis and the Office of Compliance review these reports and identify areas for further research. Based on the findings of the examiners, analysts can further research the BSA reporting by the subject institution for such items as application of the CTR filing exceptions, and can crosscheck all of the BSA reporting for consistency among the varying reports.

This kind of analysis in the context of regulatory and compliance programs and examination could, hypothetically, enable FinCEN analysts to identify general trends or vulnerabilities in the U.S. financial services industry that warrant the issuance of industry guidance. Through such guidance, FinCEN can theoretically aid U.S. financial institutions in compliance by casting light on kinds of activity that the institutions themselves might not be in a position to recognize. The addition of cross-border funds transfer data to the BSA reporting holds the potential of providing previously unavailable insights into illicit financial activity. As profiles of this activity emerge through analysis, FinCEN can describe to industry members the outline of such patterns and their significance. In this way, FinCEN can take a more direct role in assisting the industry in shaping its anti-money laundering efforts.

APPENDIX G – FINCEN INDUSTRY SURVEY AND RESPONSES

Federal Register / Vol. 71, No. 54 / Tuesday, March 21, 2006 / Notices

14289

DEPARTMENT OF THE TREASURY

Financial Crimes Enforcement Network; Proposed Collection; Comment Request; Cross-Border Electronic Transmittals of Funds Survey

AGENCY: Financial Crimes Enforcement Network, Treasury.

ACTION: Notice and request for comments.

SUMMARY: The Financial Crimes Enforcement Network requests comments on a survey that seeks input from trade groups representing members of the U.S. financial services industry on the feasibility of requiring reporting of cross-border electronic transmittals of funds, and the impact such reporting would have on the industry. The survey is part of a study of these issues required by section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004. This request for comments is being made pursuant to the Paperwork Reduction Act of 1995, Public Law 105–13, 44 U.S.C. 3506 (c)(2)(A).

DATES: Written comments should be received on or before May 5, 2006.

ADDRESSES: Written comments should be submitted to: Financial Crimes Enforcement Network, P.O. Box 39, Vienna, Virginia 22183, Attention: PRA Comments—Cross-Border Survey. Comments also may be submitted by electronic mail to the following Internet address: regcomments@fincen.gov, with a caption in the body of the text, "Attention: PRA Comments—Cross-Border Survey."

Inspection of comments. Comments may be inspected, between 10 a.m. and 4 p.m., in the FinCEN reading room in Washington, DC. Persons wishing to inspect the comments submitted must request an appointment by telephoning (202) 354–6400.

FOR FURTHER INFORMATION CONTACT: Requests for additional information or requests for copies of the questions for the new cross-border survey that is the subject of this notice should be directed to: Financial Crimes Enforcement Network, Regulatory Policy and Programs Division at (800) 949–2732.

SUPPLEMENTARY INFORMATION: On December 17, 2004, President Bush signed into law S. 2845, the Intelligence Reform and Terrorism Prevention Act of 2004 (Act).¹ Among other things, the Act requires that the Secretary of the Treasury study the feasibility of "requiring such financial institutions as

the Secretary determines to be appropriate to report to the Financial Crimes Enforcement Network certain cross-border electronic transmittals of funds, if the Secretary determines that reporting of such transmittals is reasonably necessary to conduct the efforts of the Secretary against money laundering and terrorist financing." The report must identify what cross-border information would be reasonably necessary to combat money laundering and terrorist financing; outline the criteria to be used in determining what situations will require reporting; outline the form, manner, and frequency of reporting; and identify the technology necessary for Financial Crimes Enforcement Network to keep, analyze, protect, and disseminate the data collected. This survey seeks input from trade groups representing members of the U.S. financial services industry on the feasibility of requiring reporting of cross-border electronic transmittals of funds, and the impact such reporting would have on the industry.

Title 31 CFR 103.33 (e)–(g) provides uniform recordkeeping and transmittal requirements for financial institutions and are intended to help law enforcement and regulatory authorities detect, investigate and prosecute money laundering and other financial crimes by preserving an information trail about persons sending and receiving funds through the funds transfer system. Although the requirements for banks and non-bank financial institutions are similar, their respective rules contain different terminology. For the purposes of this document, when terminology for banks is used, the intent is for it to apply to the broader universe of financial institutions.

Under current regulations, for each payment order that it receives, a financial institution must obtain and retain the following information on funds transfers of \$3,000 or more: (a) Name and address of the originator; (b) the amount of the funds transfer; (c) the date of the request; (d) any payment instructions received from the originator with the payment order; (e) the identity of the beneficiary's bank; (f) and as much information pertaining to the beneficiary as is received, such as name and address, account number, and any other identifying information. Intermediary and beneficiary banks receiving a payment order are required to keep an original or a copy of the payment order. An originator bank is required to verify the identity of the person placing a payment order if it is made in person and if the person is not already a customer. Similarly, if a beneficiary bank delivers the proceeds

to the beneficiary in person, the beneficiary bank is required to verify the identity of that person if not already a customer.

The feasibility study will examine the advisability of imposing the requirement that financial institutions report to the Financial Crimes Enforcement Network certain of the transactions of which it must currently maintain records under those regulations. The intent of this survey is to gather information from the banking and financial services industries to assist in determining the feasibility and impact of such a reporting requirement. If feasible, the Act requires the Secretary to promulgate rules imposing a reporting requirement by December 2007. An inadequate understanding of the impact could result in ineffective regulations that impose unreasonable regulatory burdens with little or no corresponding anti-money laundering benefits.

We would appreciate receiving comments on this survey on or before April 15, 2006.

You may submit comments or questions about this survey by e-mail to eric.kringel@fincen.gov or by U.S. Mail to: Financial Crimes Enforcement Network, Post Office, Box 39, Vienna, VA 22183, Attn: Eric Kringel, Senior Policy Advisor. Thank you for your assistance.

Solely for purposes of clarity and in aiding respondents in your comments to the questions below, we propose the following definition:

Cross-Border Electronic Transmittal of Funds. Cross-border electronic transmittal of funds means any wire transfer in which either the originator or the beneficiary of the transfer is located in the United States and the other is located outside the United States. This term also refers to any chain of wire transfer instructions that has at least one cross-border element, and encompasses any such transfer in which an institution is involved as originator's institution, beneficiary's institution, intermediary, or correspondent, whether that institution's involvement involves direct transmission to or from a foreign institution. The definition does not include any debit transmittals, point-of-sale (POS) systems, transaction conducted through an Automated Clearing House (ACH) process, or Automated Teller Machine (ATM).

To the extent your member financial institutions can provide the following information, we would like responses to the questions outlined below. We are seeking general or aggregated information (i.e., "45% of our membership * * *") rather than

¹ Pub. L. 108–458, 118 Stat. 3638 (2004).

specific responses about particular institutions.

Background Information

1. Please characterize the institutions your organization represents (i.e., banks, broker-dealers, currency dealers or exchangers, casinos, money services businesses, etc.).

2. How would you further describe the institutions your organization represents by the primary nature of your business (i.e., community banks, credit unions, money center banks, money transmitters, specialized business lanes, etc.).

3. What is the approximate volume of the overall funds transfer business (by total number and aggregate dollar amount) your member institutions conduct over a one-year period?

4. What is the approximate volume cross-border electronic transmittals of funds (by total number and aggregate dollar amount) your member institutions send and receive over a one-year period?

To the extent possible, please estimate the percentage of cross-border electronic transmittal of funds sent or received by your member financial institutions, in the following categories (if applicable):

a. On behalf of their own customers,
b. As an intermediary or correspondent for other institutions
c. As internal settlement with their own institution's foreign affiliates or branches.

d. As the U.S. financial institution that directly transmitted the payment order to or accepted the payment order from a financial institution located outside of the United States.

5. Do your member institutions send or receive cross-border electronic transmittal of funds in-house or through a correspondent?

a. What systems (e.g., SWIFT, Fedwire, CHIPS, proprietary system) are used to send or receive cross-border funds transfers?

b. What is the proportional usage of each system if more than one system is used?

c. Are there instances when the system used is dictated by the nature of the transaction or customer instruction? If possible, please exclude those situations where the decision is due to the fact that the receiving financial institution does not use a particular system.

Existing Record Maintenance and Compliance Process

6. How do your member institutions maintain the funds transfer records required by 31 CFR 103.33 (i.e., message system logs or backups, wire transfer

instruction database, account history files, etc.)?

a. If the data is stored electronically, can the storage systems export such data into a spreadsheet or database file for reporting?

7. Approximately how many times in a one-year period does the government subpoena or otherwise issue a legal demand requiring your member institutions to produce cross-border wire transfer information?

Note: We understand that many requests seek "any and all records" pertaining to an account or subject. Where possible, please distinguish those requests from more specific requests for cross-border electronic transmittals of funds.

8. Can you estimate the approximate total cost (e.g., person-hours or other costs) to your member institutions in time and expense responding to these legal demands? If you cannot estimate the costs incurred, please describe generally the resources involved in complying with such requests.

Foreign Transactions

9. Do your member institutions or any of their branches, subsidiaries, or affiliates transmit or receive cross-border electronic transmittals of funds from a location in either Australia or Canada?

a. If yes, please briefly describe the measures taken, including the general estimates of the costs in time and expense incurred, to ensure compliance with the cross-border funds transfer reporting requirements in those jurisdictions and the measures in place to monitor and maintain compliance.

10. If the Department of the Treasury required reports of cross-border electronic transmittals of funds involving amounts over \$3,000, what general steps would your member institutions need to take (and how burdensome would it be) to comply?

a. Would the answer differ if the value threshold were \$10,000?

b. Would the answer differ if there were no value threshold?

c. How would these different thresholds affect the volume of the reporting from your member institutions?

d. How would the answer differ with the type of required reporting (e.g., electronic file upload, Web-based form)?

e. How would the answer differ with the timing of required reporting (e.g., real-time, end-of-day, within 30 days)?

f. To the extent possible, please estimate any cost increase for cross-border electronic transmittals of funds that may result.

g. To the extent possible, please describe any effects that reporting

requirements may have on the volume or value of cross-border electronic transmittals of funds.

Potential Impact on Financial Institutions

11. If the Department of Treasury required reports of cross-border electronic transmittals of funds in a SWIFT, CHIPS or other file format specified by the Department, what steps would your member institutions need to take to extract such data from existing records to submit the information as required?

12. If the Department of Treasury required reports of cross-border electronic transmittals of funds but also provided exceptions for certain customers or types of transactions (i.e., internal settlement, identical originator and beneficiary, transfers to government entities, etc.), what exemptions would you suggest?

a. How difficult would it be for your member institutions to build such exceptions into the business process for creating the report?

b. Would the costs to implement the exceptions outweigh the benefits?

13. If the Department of the Treasury required reports of cross-border electronic transmittals of funds, should the requirement be limited to certain institutions (e.g., only the originating institution, only the beneficiary's institution, only the U.S. financial institution that directly transmits the payment order to or accepts the payment order from a financial institution located outside of the United States)? Please explain the rationale for your response.

14. Can your member financial institutions' automated systems distinguish between domestic funds transfer and a cross-border electronic transmittal of funds?

15. Among the following definitions of "cross-border electronic transmittal of funds" what potential advantages and disadvantages do you perceive? Do you have any suggestions for such a definition or can you highlight any particular issues that should be addressed in such a definition?

(Note: All of the following definitions would exclude check, debit transmittal, ATM, or ACH payments.)

a. Cross-border electronic transfer of funds means any wire transfer where the originator's and beneficiary's institutions are located in different countries and one of the institutions is located in the United States. This term also refers to any chain of wire transfers that has at least one cross-border element

b. Cross-border electronic transfers of funds include transactions where either (1) a foreign office of a financial institution instructs a U.S. office of a financial institution to effect payment in the U.S., directly or indirectly, or (2) where U.S. office of a financial institution instructs a foreign office of a financial institution to effect a payment abroad, directly or indirectly.

c. Cross-border electronic transmittal of funds means the transmission—through any electronic, magnetic or optical device, telephone instrument or computer—of instructions for the transfer of funds, other than the transfer of funds within the United States. In the case of SWIFT messages, only SWIFT MT 100 and SWIFT MT 103 messages are included.

d. Cross-border electronic transmittal of funds means an instruction for a transfer of funds that is transmitted into or out of the United States electronically or by telegraph, where the financial institution is acting on behalf of, or at the request of, another person who is not a financial institution.

Title: Cross-Border Electronic Transmittals of Funds Survey.

OMB Number: 1506-0048.

Abstract: Survey to be conducted with business owners and managers in the Cross-Border Electronic Transmittals of Funds industry. Survey asks respondents to report on cross-border financial services provided by their businesses.

Type of Review: New information collection.

Affected Public: Business or other for-profit institutions.

Frequency: One time.

Estimated Burden: Reporting average of 60 minutes per response.

Estimated Number of Respondents: 23,262.

Estimated Total Responses: 23,262.

Estimated Total Annual Burden

Hours: 23,262.

Request for Comments

Comments submitted in response to this notice will be summarized and/or included in the request for OMB approval. All comments will become a matter of public record. Comments are invited on: (a) Whether the collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility; (b) the accuracy of the agency's estimate of the burden of the collection of information; (c) ways to enhance the quality, utility, and clarity of the information to be collected; (d) ways to minimize the burden of the collection of information on respondents, including

through the use of automated collection techniques or other forms of information technology; and (e) estimates of capital or start-up costs and costs of operation, maintenance and purchase of services to provide information.

Dated: March 14, 2006.

Robert Werner,
Director, Financial Crimes Enforcement Network.

[FR Doc. E6-4073 Filed 3-20-06; 8:45 am]
BILLING CODE 4810-02-P

DEPARTMENT OF THE TREASURY

Request for Comments on Treasury's Report to Congress on International and Exchange Rate Policies

AGENCY: Office of the Under Secretary for International Affairs, Treasury.

ACTION: Request for comments.

SUMMARY: The Office of the Under Secretary for International Affairs of the U.S. Department of the Treasury invites all interested parties to comment on the methodology used in preparing its semi-annual report to Congress on International and Exchange Rate Policies and to submit views on the contents of its next report.

DATES: Written comments must be received on or before April 7, 2006.

ADDRESSES: Comments may be submitted by mail, facsimile or email. All comments should contain the following information in the heading: "Attn: Request for Public Comments on the Report to Congress on International and Exchange Rate Policies."

Mailing address: Office of the Under Secretary for International Affairs, Department of the Treasury, 1500 Pennsylvania Avenue, NW., Washington, DC 20220.

Facsimile: (202) 622-2009 (not a toll-free number).

Email: ashby.mccown@do.treas.gov.

For further information concerning the submission of comments, refer to the heading "Request for Comments" in the SUPPLEMENTARY INFORMATION portion of this notice.

FOR FURTHER INFORMATION CONTACT: John Weeks, Director, Global Economics Unit, Department of the Treasury, 1500 Pennsylvania Avenue, NW., Washington, DC 20220, (202) 622-9885 (not a toll-free number), john.weeks@do.treas.gov.

SUPPLEMENTARY INFORMATION:

Background

Section 3004 of Public Law 100-418 (22 U.S.C. 5304) requires, inter alia, that the Secretary of the Treasury analyze on

an annual basis the exchange rate policies of foreign countries, in consultation with the International Monetary Fund, and consider whether countries manipulate the rate of exchange between their currency and the United States dollar for purposes of preventing effective balance of payments adjustment or gaining unfair competitive advantage in international trade. Section 3004 further requires that: "If the Secretary considers that such manipulation is occurring with respect to countries that (1) have material global current account surpluses; and (2) have significant bilateral trade surpluses with the United States, the Secretary of the Treasury shall take action to initiate negotiations with such foreign countries on an expedited basis, in the International Monetary Fund or bilaterally, for the purpose of ensuring that such countries regularly and promptly adjust the rate of exchange between their currencies and the United States dollar to permit effective balance of payment adjustments and to eliminate the unfair advantage."

Section 3005 (22 U.S.C. 5305) requires, inter alia, the Secretary of the Treasury to provide each six months a report on international economic policy, including exchange rate policy. Among other matters, the reports are to contain the results of negotiations conducted pursuant to Section 3004. Each of these reports bears the title, Report to Congress on International Economic and Exchange Rate Policies, (the "Report").

Treasury is soliciting comments on the methods used by Treasury to analyze the economies and exchange rate policies of foreign countries in order to help improve the process of carrying out its responsibilities under Sections 3004 and 3005. The most recent Report can be found on the Web site of the Office of the Under Secretary for International Affairs, at <http://www.treas.gov/offices/international-affairs/economic-exchange-rates/>. Treasury is also soliciting views on approaches that might be fruitful in the upcoming spring 2006 Report.

Request for Comments

Comments must be submitted in writing by one of the methods specified in the ADDRESSES portion of this notice. All comments should contain the following information in the heading: "Attn: Request for Comments on the Report to Congress on International and Exchange Rate Policies." Comments must be received by April 7, 2006. Treasury requests that comments be no more than two pages in length.

The Office of the Under Secretary for International Affairs will not accept



1120 Connecticut Avenue, NW
Washington, DC 20036

1-800-BANKERS
www.aba.com

*World-Class Solutions,
Leadership & Advocacy
Since 1875*

Richard R. Riese
Director
Center for Regulatory
Compliance
Phone: 202-663-5051
Riese@aba.com

April 21, 2006

Via Email

Financial Crimes Enforcement Network
Post Office Box 39
Vienna, VA 22183

Re: Cross-Border Survey
71 *Federal Register* 14289; March 21, 2006

Ladies and Gentlemen:

Thank you for the opportunity to provide input to your survey of cross border electronic transmittal (CBET) activity and to comment on the feasibility of adopting a reporting system for such transfers. To develop responses to the survey, ABA conducted conference calls with member representatives from the AML compliance and wire transfer operations departments of their institutions. In addition, some members provided, on a non-attribution basis, proprietary information about their cross-border wire transfer activity. However, ABA did not conduct a survey that enabled it to make membership-wide statements about their experience. Accordingly, we offer answers to the survey in the form of discrete observations or experiences submitted to us by a small, but diverse subset of our membership that we believe represent a variety of views characteristic of those held by the banking industry in general.

Background Information and Summary of Position

The American Bankers Association, on behalf of the more than two million men and women who work in the nation's banks, brings together all categories of banking institutions to best represent the interests of this rapidly changing industry. Its membership--which includes community, regional and money center banks and holding companies, as well as savings associations, trust companies and savings banks--makes ABA the largest banking trade association in the country.

The US payment system is immensely complex, involving thousands of different institutions, operating across a wide variety of platforms, systems & payment methods. Daily volumes are massive and cannot in any way be compared with the experience in nations with existing CBET reporting requirements such as those in Australia & Canada. In most cases, the US payment system does not currently distinguish between domestic and cross-border transactions. Imposing a new requirement to include this type of information for all wire transfers would require substantial changes to US payment systems, as well as the internal systems of participating financial institutions.

ABA notes that US law enforcement agencies already have the ability to request relevant wire transfer data from financial institutions. However, in the banking industry's experience, this authority is not often used. In contrast to the current low level of law enforcement activity in this area, mandating a new reporting regime for CBET would impose substantial new compliance costs on financial institutions subject to the new rule far out of proportion with the law enforcement utility achieved. Combined with potential privacy concerns that the introduction of such a comprehensive cross border surveillance program would entail, these compliance burdens could provide an incentive to move business to offshore banks not subject to the reporting requirement.

ABA members remain unconvinced that FINCEN would be able to substantially benefit from the receipt of most of the reported information encompassed by a CBET reporting requirement. It is relevant to note in this regard that FINCEN already receives data from financial institutions on transactions of concern via the filings of SARs. As such, the ABA does not believe that the benefits to law enforcement associated with a virtually universal CBET reporting requirement would be worth the cost incurred by the American banking industry, nor the invasion of financial privacy suffered by US citizens and their businesses.

Responses to Survey Questions

Questions 3 & 4. ABA does not have a number that equates to a membership specific volume of funds transfer business activity conducted annually. However, our membership includes the industry's largest volume operations engaged in cross-border electronic transmittals (CBETs) and consequently accounts for the vast majority of transfers into and out of the United States every year.

A sample of the volume of overall funds activity reported by ABA members is quite diverse, and very impressive in terms of size. For instance, banks of less than \$10 billion in asset size reported low six figure transfers by number with a range of between 30 and 200 billion in dollar value. Larger institutions reported low seven figure transfers by number and between 2.5 and 15 trillion by dollar value—with the highest value reporter in this segment also being characterized as having several hundred billion dollars in assets under management. Finally, even those institutions generally considered among the nation's largest—but not necessarily leaders in CBETs—nonetheless reported tens of millions of wire transfers amounting to 50 to more than 150 trillion in dollar value annually.

Looking at CBETs alone, the larger institutions who are not among the banks usually identified as the industry's top leaders in CBETs, report in the range of 100 - 200 thousand cross border transfers a year valued at an even wider range of 8 billion to 2 trillion dollars. Several banks were not able to report numbers or volumes for all or parts of their international activity due to current system limitations. As a percentage of total fund transfer activity, CBETs represent somewhere between 5 and 50% of their total—but most were estimated at less than 20%.

Trying to apportion the volume of CBETs among those conducted on behalf of customers, as intermediaries, as internal settlements or as “last out, first in” institutions defies industry-wide conclusions. First some institutions do not have systems that allow them to make an accurate estimation of such a categorization of their activity. When an estimate can be ventured, the experience is diverse—but for most institutions the CBETs conducted for customers represents between 80 and 100% of their experience. Obviously leading institutions that hold themselves out as proficient in serving as correspondents for CBETs will estimate a larger volume of intermediary correspondent CBETs as well as transfers that qualify as “last out, first in.” An unscientific poll of bankers visiting ABA’s compliance web page revealed that only 1 in 4 respondents identified themselves as conducting “last out, first in” cross-border transfers.

Question 5. As suspected, many banks conduct their CBETs exclusively through a correspondent. Others conduct CBETs using both correspondents and in-house capabilities with varying percentage splits between the two. Fewer members conduct CBETs exclusively using in-house means.

This diversity of CBET experience is also reflected in the apportionment of transfers across systems used. Some members who transfer only through correspondents use exclusively Fedwire, whereas as others of this group report that they rely solely on SWIFT. Institutions that transfer using both in-house and correspondent accounts generally use both Fedwire and SWIFT—with many also using CHIPS and a few using a proprietary system. Some banks report that system choice is due to the fact that the receiving financial institution does not use a particular system, but this was not reported as a driver of their answers on the apportionment of use across systems.

Existing Record Maintenance and Compliance Process

Question 6. Responding to the question of funds transfer records systems illustrates another aspect of the diversity of the American banking industry—widely varied software solutions with differing capabilities. This variety of choice also represents differing degrees of investment and an election among record retention options. Many members reported having the capability of downloading CBETs to spreadsheets. Other institutions—including some of the largest—reported hurdles such as not being able to create reports for activity moved to their archive system or not being able to generate electronic reports from the system used for U.S dollar transfers.

Questions 7 & 8. Member experience with government subpoena of CBET information is generally characterized as rare. Most institutions reported fewer than 8 – 10 occasions a year on average. However, a report as high as 300 was also received. Costs attributed to these responses per institution varied with complexity of request and the member’s process for handling subpoenas generally. Members described research and retrieval effort, production staff time and supplies, compliance investigative unit involvement and legal office oversight. Given the infrequent occurrences, members did not translate this activity to cost figures of any confidence level. What is clear to all responding members is that a universal CBET

reporting regimen would be several orders of magnitude more expensive than the very limited subpoena process now applicable. It is also unlikely that CBET reporting requirement would eliminate subpoenas. Chances are that subpoenas would increase as reported CBETs are used to generate more investigative red flags that demand more in depth law enforcement inquiry to confirm or dismiss concerns.

Foreign transactions

Question 9. ABA members whose affiliates transmit or receive CBETs from locations in Australia or Canada have offered a few observations: Even with just two operating platforms, one bank stated that establishing the reporting process took over a year and considerable resources and coordination with existing IT partners as well as the purchase of additional third-party software. Because Canadian obligations require reporting aggregated CBETs within a 24 hour period totaling over \$10,000 for one originator, a bank will face more complicated IT logic to accomplish the aggregation function before reporting. Using a “last out, first in” reporting obligation leaves larger banks with the reporting burden, but for some it required less IT logic to be built into the reporting system. Banks with experience in Australia note that they are dealing with a couple thousand transfers a month versus millions a month coming out of the US market. This multiple orders of magnitude difference defies scalability between the Australian system and any prospective US reporting system.

Question 10. Generally, the steps each reporting institution would face to create a compliant reporting system would include evaluating the scope of the final reporting requirements and assessing gaps between new and old systems, having vendors modify their software, designing and creating new databases to keep data for reporting purposes, conducting significant training of staff, monitoring processes to assure compliance and engaging in audit reviews.

More specific member comments noted: a manual spreadsheet would have to be maintained for outgoing foreign wires, incoming wires from Fedwire are conducted as “straight through processing” and would need to be reviewed individually after receipt and a manual record be created—all requiring additional staff; some wire systems do not populate country code necessitating a vendor enhancement; a new program would be necessary to capture required data for reporting; existence of SWIFT messages is main method of separating domestic from cross-border transfers, but misses payments sent by Fedwire without SWIFT instructions, existing systems would need to be mapped to reporting format ultimately required by federal regulation.

Estimating the costs for these undertakings is very difficult, let alone trying to determine how they might vary depending on certain parameters. Real time and end of day reporting are not available from some existing systems. Thresholds—as long as there is no aggregation requirement—are not particularly complicating system wise—but distinctions can involve compliance monitoring challenges especially if the notion of structuring is applied to wire activity. Because system modifications compete for scheduling with core business demands and are budgeted over periods

of many quarters, a reporting regime cannot be implemented without long transition periods.

As for the cost impact on customers, some members believe that the expense of system changes and maintenance of reporting could affect transfer commissions. Some banks expressed the concern that U.S. dollar transactions could be impacted adversely if customers saw off-shore banks offering dollar transfers. For institutions with limited cross-border traffic that they handle directly, costs of reporting could drive some banks, that have insufficient market share to implement efficiencies or price transfers effectively, out of the business and promote consolidation of traffic in fewer direct providers.

Potential Impact on Financial Institutions

Question 12. If reporting were required in a SWIFT or CHIPS format banks would still need to develop a reporting capacity to append to their business systems just to aggregate and pass along the information in existing systems to the government.

Question 13. The value of exemptions/exceptions from reporting depends on their being simple, voluntary and not subject to a qualification process, compliance requirements, supervisory criticism or government enforcement. For instance, excluding internal settlements from reporting may eliminate converting specialized proprietary systems in some banks. Exempting transfers to or from government entities may enable some banks to segregate entire segments of their business activity in a cost effective manner; provided we can all agree on what constitutes a “government entity.” However, subjecting banks to supervisory criticism for failing to parse the qualifications for exemptions can quickly complicate matters and incur associated costs or regulatory risk that would outweigh any benefit from using the exemptions.

Question 14. An answer to the question of whether the reporting requirement should be limited to certain banks is ultimately dependent on how CBETs are defined. If one seeks to capture the actual funds payment, then you are going to be focused on a Fedwire or CHIPS transfer. In this situation a “last out, first in” reporting obligation would suffice to capture the cross border transfer of funds and whatever information is attached to that transmittal. Although this method shifts much of the reporting burden to a smaller number of generally larger banks, many of the possess sufficient capacity to perform the reporting with greater efficiency than would be the case if the obligation rested with all originating or beneficiary’s institutions.

Nevertheless, if CBETs were defined to encompass only SWIFT MT 103 messages, then the reporting obligation would most likely require the originators or recipient’s bank to report. This approach contains all travel information, but simplifies reporting by eliminating correspondent transfers of the money involved and excludes bank to bank settlement transfers.

Question 15. Our sampling of banks’ capabilities to distinguish between domestic and cross border transfers through their existing automated systems reveals mixed

results. Some banks have this capacity for all means of transmittal. Other banks can only distinguish cross border transfers as those associated with SWIFT messages and those that are not—hardly a fail safe method. Banks relying on Fedwire advise us that the best solution for distinguishing between domestic and cross-border transfers would be having the Federal Reserve develop a new message type for transaction through its system. Most banks report a need to reprogram their proprietary systems or their vendors' systems to make the distinction between domestic and cross-border transmittals.

Question 16. As noted in responding to question 14, how one defines CBETs will effect the ultimate reporting obligation. The FinCEN Survey suggests four variants that create differing operative terms and generate different categories of captured transmittals. This then leads to the idea of limiting the reporting obligation to “last out, first in.” Any all encompassing definition must deal with the variability of transmittal systems (e.g., Fedwire, CHIPS, SWIFT) that would be employed to achieve the conduct the transfer being captured. This in turn leads to a plethora of information systems, data formats, and compliance complications.

At this stage of evaluating the feasibility of instituting a cross-border wire reporting obligation, it is premature for ABA to recommend a single solution to the challenges faced. However, we suggest that implementing a comprehensive reporting program need not be the immediate objective. We should recognize that capturing only certain SWIFT messages, for instance, will generate terabytes of data not previously available to law enforcement—even if there would be information missed by selecting one channel to the exclusion of another. From a feasibility standpoint, ABA proposes for discussion whether piloting a single channel specific reporting requirement and then evaluating what has been achieved from a law enforcement perspective for what cost from an economic and privacy basis, isn't a preferred alternative to attempting to implement a comprehensive definition-and-exception driven cross-border, cross-system regime.

In organizing this discussion, we suggest that law enforcement evaluate the information available from a particular channel as it is currently available in its existing format and consider the additional utility that would be garnered without imposing any more requirements on banks to alter their present data systems. In other words, ABA urges law enforcement to exhaust information available from established data collection formats, before creating new information elements that are not driven by present business necessity. We believe this step is a fundamental part of addressing CBET reporting feasibility.

In evaluating the single channel approach, ABA wants to stress that even a reporting obligation based on existing transaction activity and message formats will still compel some system enhancements to enable tapes or other reports to be created and filed. Furthermore, regardless of the nature of any imagined reporting requirement, the financial services industry's responsibility should extend only to the simple transmittal of raw data, with FINCEN assuming full responsibility for the refinement and distillation of the data into a format useful to law enforcement agencies.

Conclusion

In summary, ABA contends that the prospect of mandating cross border electronic transmittal reporting will face substantial cost barriers for changing systems including the virtually prohibitive expenses in adding information elements to existing transaction information flows. In contrast to the current low level of law enforcement activity in this area, mandating a new reporting regime for CBET would impose substantial new compliance costs on financial institutions subject to the new rule far out of proportion with the law enforcement utility achieved and would incur unjustified government incursion into the financial privacy of U.S. citizens and their legitimate business conduct.

ABA and its members are available to participate in further discussions with regard to the prospects for cross border transfer reporting should there be future efforts to impose such an obligation.

Respectfully submitted,



Richard R. Riese
Director, Center for Regulatory Compliance



April 17, 2006

Mr. Eric Kringel
Senior Policy Advisor
Financial Crimes Enforcement Network
Post Office Box 39
Vienna, VA 22183

Re: Financial Institution Survey Regarding Cross-Border Electronic Transmittals of Funds

Dear Mr. Kringel:

America's Community Bankers (ACB)¹ is pleased to respond to the Financial Crimes Enforcement Network's (FinCEN) feasibility study regarding cross-border electronic transmittals of funds. FinCEN is evaluating whether it would be appropriate for financial institutions to report information about cross-border funds transmittals. It is also studying the impact that such a reporting requirement would have on the financial services industry. This study is required by the Intelligence Reform and Terrorist Prevention Act of 2004.

ACB requested members of three ACB committees to complete FinCEN's survey. The committees were:

- Regulation and Compliance Committee
- Retail Banking, Operations, Security & Technology Committee; and
- Electronic Banking and Payment Systems Committee.

The bankers that participate on these committees were the most appropriate persons within their institutions to review and complete the survey. Nevertheless, the response rate to the survey was very low. This may be attributable to a multiple factors, including:

- The length of the survey.
- The degree of internal research required to respond to the survey.

¹ America's Community Bankers is the member driven national trade association representing community banks that pursue progressive, entrepreneurial and service-oriented strategies to benefit their customers and communities. To learn more about ACB, visit www.AmericasCommunityBankers.com.

Financial Institution Survey Regarding Cross-Border Electronic Transmittals of Funds
April 17, 2006
Page 2

- The short time to respond to the survey.
- Limited staff time due to regulatory demands placed on community bank compliance and operations employees.

While the responses we received do not represent a statistically valid sample of ACB's membership, we were able to discern possible trends within the community banking industry and received pertinent comments from ACB members who engage in cross-border transactions. The following are some general comments regarding community bank involvement in cross-border transactions.

- The volume and dollar value of cross-border transactions originated by community banks varies significantly across the community banking industry.
- Most community banks that provide cross-border transfers provide this service only to their customers.
- Most community banks use a correspondent bank to provide cross-border transactions. As a result, most community banks do not deal directly with institutions located outside of the United States. Any reporting requirement should be limited to institutions that transmit funds directly to a foreign bank. The Department of the Treasury would still receive data about cross-border transfers originated by community banks, but that information would come from the correspondent. This approach would avoid placing additional regulatory burdens on community banks whose resources may also often be constrained.
- Community banks believe that the additional reporting requirements will add additional time to the processing of these transfers and that the requirements would be labor intensive.

FinCEN will weigh many factors as it analyzes the survey results and determines whether to impose additional reporting requirements on financial institutions. We specifically request FinCEN to consider the cumulative regulatory burden shouldered by the nation's community banks and to balance any new compliance requirements with the size and capacity of the depository institution.

Thank you for the opportunity to assist in collecting information regarding cross-border transfers. Should you have any questions, please contact the undersigned at 202-857-3187 or kshonk@acbankers.org.

Sincerely,



Krista J. Shonk
Regulatory Counsel



CUNA & Affiliates
A Member of the Credit Union System

Credit Union
National Association, Inc.

801 Pennsylvania Ave. NW, South Bldg.
Suite 600
Washington, D.C.
20004-2601

Telephone:
(202) 638-6777
Fax:
(202) 638-7734

Web Site:
www.cuna.org

April 14, 2006

Eric Kringel
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: PRA Comments – Cross Border Survey

Dear Mr. Kringel:

The Credit Union National Association (CUNA) appreciates the opportunity to provide feedback, on behalf of our credit union members, on the cross-border electronic transmittals of funds (transfers). By way of background, CUNA is the largest credit union trade association, representing 87% of our nation's 8,900 state and federal credit unions, which serve nearly 87 million members.

As mandated by Congress, the Treasury, through the Financial Crimes Enforcement Network (FinCEN), is seeking input from trade groups representing members of the U.S. financial services industry on the feasibility of requiring reporting of cross-border electronic transmittals of funds, and the impact such reporting would have on the financial services industry.

CUNA commends FinCEN for seeking input from credit unions and other financial institutions through trade groups on the feasibility of reporting certain information on cross-border transfers and support efforts to combat money laundering and terrorist financing.

However, mandating that financial institutions must segregate cross border transfers from domestic transfers may be problematic, especially for smaller institutions. Smaller credit unions typically send and receive wire transfers through a correspondent, which is generally a corporate credit union or larger financial institution. When a transfer is received by a correspondent, the domestic and cross border transfers are not distinguished. Credit unions would need to establish procedures that would differentiate cross border transfers from domestic transfers and maintain this information in a separate database for reporting purposes.

In addition to procedures to segregate cross border transfers, credit unions would need to establish additional recordkeeping procedures to implement any reporting requirements. Currently, some credit unions, typically those with

smaller assets, maintain records by filing wire information by account number in members' account histories, rather than by date. This enables credit unions to retrieve information on a particular account, including any electronic transfers as needed. This information is typically requested in response to government subpoenas, which tend to request specific account information and transaction histories rather than requesting cross border transfer information on particular dates. If cross border transfer information would be required to be reported, data processing systems would need to be upgraded to enable credit unions to retrieve the required information. This may be challenging for smaller credit unions, particularly those using a third party, such as a corresponding institution, to complete the transfer.

Thank you for the opportunity to comment on these important issues. Please contact me at 202-508-6733 or LThomas@cuna.coop if you have any questions or would like to discuss the impact cross border transfer reporting would have on credit unions.

Sincerely,

Lilly Thomas
Assistant General Counsel



TERRY J. JORISE
Chairman
JAMES P. GHIGLIERI, JR.
Chairman-Elect
CYNTHIA BLANKENSHIP
Vice Chairman
KEN PARSONS, SR.
Treasurer
ROBERT C. FRISCKE
Secretary
DAVID E. HAYES
Immediate Past Chairman
CAMDEN R. FINE
President and CEO

April 26, 2006

Mr. Eric Kringsel
Senior Policy Advisor
Financial Crimes Enforcement Network
P. O. Box 39
Vienna, Virginia 22183

Re: Cross-Border Electronic Transmittals of Funds Survey

Dear Eric:

The Independent Community Bankers of America (ICBA)¹ appreciates the opportunity to offer comments on the cross-border wire survey being conducted by the Financial Crimes Enforcement Network (FinCEN). The survey seeks comments from trade association representatives on the feasibility of requiring reporting of cross-border electronic transmittals of funds, as required by section 6302 of the Intelligence Reform and Terrorism Prevention Act of 2004.

General Comments

At the outset, ICBA believes several key points should be stressed. First, the impetus for the survey was reporting systems used in Australia and Canada. However, the banking system in the United States is substantially different and far more diverse than the banking systems in either of those countries, making it difficult – if not impossible – to draw parallels to their reporting mechanisms.

Second, even if the development of an automated system is possible, the costs and burdens for filing such reports are likely to far exceed the benefits. While banks are currently required by the Bank Secrecy Act to track the information, it is not likely to be

¹ The Independent Community Bankers of America represents the largest constituency of community banks of all sizes and charter types in the nation, and is dedicated exclusively to representing the interests of the community banking industry. ICBA aggregates the power of its members to provide a voice for community banking interests in Washington, resources to enhance community bank education and marketability, and profitability options to help community banks compete in an ever-changing marketplace.

With nearly 5,000 members, representing more than 18,000 locations nationwide and employing over 265,000 Americans, ICBA members hold more than \$876 billion in assets \$692 billion in deposits, and more than \$589 billion in loans to consumers, small businesses and the agricultural community. For more information, visit ICBA's website at www.icba.org.

INDEPENDENT COMMUNITY BANKERS of AMERICA *The Nation's Voice for Community Banks™*
One Thomas Circle, NW Suite 400 Washington, DC 20005 • (800)422-8439 • FAX: (202)659-1413 • Email: info@icba.org • Web site: www.icba.org

tabulated or organized in a format that lends itself to easy reporting. Therefore, any new reporting requirement would require substantial time and investment, detracting from other resources used for Bank Secrecy Act compliance. Community banks are already over-burdened by a vast array of regulatory requirements, especially smaller institutions. As new requirements are added, more community banks report seriously assessing whether to sell to larger institutions or otherwise cease independent operations because of the disproportionate impact of regulatory burdens on smaller institutions.

Third, even if the data is reported, FinCEN must be able to devote sufficient resources to collect, store and analyze the data. Without sufficient expenditures and resources to analyze the data, it will not provide useful information. Moreover, any database that FinCEN constructs must include resources devoted to incorporating sufficient protections to ensure access to the database is properly restricted and that the data is adequately safeguarded to avoid problems such as identity theft, misappropriation of information or other problems.

Finally, for a new data collection regime to be worthwhile, assuming the hurdles of collecting and analyzing the data can be overcome, the data must be demonstrably useful to law enforcement. Additional data that law enforcement cannot or does not use for investigations or prosecutions does little to further the goals of the BSA. Law enforcement should also explain why this new data collection will provide information that is not currently available from other sources.

Cross-Border Wire Survey

Background Information

To collect data to respond to FinCEN's survey, ICBA forwarded the survey to a number of bankers in a variety of community banks across the country. The bankers surveyed included banks of various sizes and in various communities. Perhaps due to the extent of the survey, the limited time to respond, and the subject matter, response levels were not statistically valid. However, several key points emerged that can be useful for the feasibility study.

Community banks that responded to the survey indicated overall wire activity ranging from 275 to 180,000 wires annually and aggregating anywhere between \$3 million and \$300 billion. Overall, only a small percentage of wire transactions was cross-border activity.² For the most part, cross-border wire services are restricted to established customers well-known to the bank. Cross-border wire activity ranged from virtually none to well over 1000 transfers annually (both incoming and outgoing) that aggregated up to \$20 million. Independent community banks did not offer correspondent cross-border wire services, but a number of bankers' banks³ offer cross-border wire

² It is important to recognize that community banks located along the Canadian and Mexican borders are more likely to engage in cross-border wire transfer activity.

³ Bankers' banks are correspondent banks that provide a variety of correspondent services for community banks.

services. None of the community banks that responded to the survey offered internal settlement services for their own foreign affiliates or branches.

Since most of the cross-border wire transfer activity conducted by community banks is done through correspondent banks, none of the banks that responded to the survey executed the actual transfer across the border. Most of the banks reported using either Fedwire or SWIFT for overall wire services, with Fedwire being the predominantly preferred wire service.⁴

Existing Record Maintenance and Compliance Process

Community banks report using a variety of mechanisms to comply with existing wire record retention requirements. Most use manual systems or Excel spreadsheets to track the information, although some use software to track the information. Most reported that the information could be transferred electronically for reporting. However, because many community banks maintain the information manually, a new reporting requirement would likely prove more burdensome for smaller institutions, causing some smaller community banks to cease offering wire transfer services if the reporting requirement is adopted.

Few community banks reported having been subpoenaed by the government to provide cross-border wire information, with the exception of one bankers' bank.

Foreign Transactions

As noted above, few of the community banks that responded to the survey reported conducting cross-border wires. However, those located in states near the Canadian border reported activity to and from Canada. Generally, the banks reported using OFAC compliance or other software for tracking and reporting, although the banks were unable to give accurate estimates of time and costs.⁵

If Treasury required reporting of cross-border wires, it would entail creation of new policies and procedures by community banks. This would be necessary no matter what threshold for reporting was adopted, although the general consensus is that it would be simpler to track and report cross-border wires as the threshold increased. However, any new reporting requirement would be costly and burdensome to implement, and a number of community banks indicated it would very likely require investment in new software to track the information.

Generally, the more time allowed for a community bank to report the information was preferable. Existing software would make real-time or end-of-day reporting difficult, and any requirement to furnish information real-time or end-of-day would likely entail expensive solutions. Moreover, because community banks report working through

⁴ Those that used SWIFT or Fedwire for cross-border transfers reported that between 78% and 97% was conducted over Fedwire.

⁵ Because cross-border wire activity for those few community banks that reported offering the service was part of their overall wire operations, the ability to segregate activity to one country or to segregate international and domestic wires was limited.

correspondent institutions for much of their wire activity, especially any cross-border wires, some information would not be readily available to the community bank.⁶

Potential Impact on Financial Institutions

If the reporting of cross-border wires were instituted, community banks would have to make arrangements with their correspondent banks to obtain some of the information. More detailed reporting requirements would entail commensurately more burden. And, to a certain extent, community banks would have to rely on software vendors to provide the appropriate tools to segregate and report the information in the formats required.⁷

Generally, community banks believe that the initial set-up to meet a new reporting requirement would be the most burdensome part of the process. For many of the community banks that responded to the survey, their current levels of cross-border wire activity would allow them to provide the information manually, but that could become more difficult if volume of cross-border wire activity increased. There seemed to be some preference for the originating institution as the most logical bank in the chain to report, since that bank would have the most information about the transaction. However, it is also important to recognize that community banks noted they would rely on correspondent banks to furnish additional information about the transaction to provide a full report. And, others firmly believe that the bank that actually sent the wire across the border (the last bank in the chain) would be the most logical reporting entity. Overall, though, community banks reported their existing systems allow them to distinguish between domestic and cross-border funds transfers.

Definition of "cross-border electronic transmittal of funds." There was no clear consensus among the community bankers who responded to the survey as to a particular definition for cross-border wire. However, there seemed a preference for the first definition⁸ as the most simple, most easily understood and easiest to apply.

Conclusion

ICBA firmly supports the federal government's efforts against money-laundering and terrorist financing. However, it is also critically important that the limited resources of financial institutions, government agencies and law enforcement be devoted to truly suspicious activities and not assessment of routine transactions. While additional data

⁶ The community banks indicated that, depending on the information required in the report, they would have to obtain the information from their correspondent bank before filing accurate reports.

⁷ If Treasury and FinCEN were to provide the software necessary to track and report the information, that would go a long way to addressing the burden of these requirements, but would not eliminate the burden.

⁸ "Cross-border electronic transfer of funds means any wire transfer where the originator's and beneficiary's institutions are located in different countries and one of the institutions is located in the United States. This term also refers to any chain of wire transfers that has at least one cross-border element."

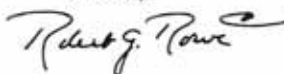
5

may be useful to law enforcement, the only way that data can be truly useful is if it can be processed and analyzed in a timely fashion. And, any database must include sufficient safeguards to ensure the information is properly protected.

Overall, ICBA questions whether the information contemplated in a cross-border wire transfer reporting system would provide benefits that would outweigh the burdens. The added costs to wire transfers could drive an increasing number of transactions underground where information about the transactions is much less readily transparent or available to law enforcement. And, the increased costs with a new reporting system could also drive legitimate community bank providers away from providing this service, leaving an increasingly fertile environment for underground providers. These are critical points to factor into any feasibility study of requiring a new reporting regime.

Thank you for the opportunity to comment. If you have any questions or need additional information, please feel free to contact me.

Sincerely,



Robert G. Rowe, III
Regulatory Counsel

INDEPENDENT COMMUNITY BANKERS of AMERICA *The Nation's Voice for Community Banks™*
One Thomas Circle, NW Suite 400 Washington, DC 20005 • (800)422-8439 • FAX: (202)659-1413 • Email: info@icba.org • Web site: www.icba.org

From: David Landsman [david@nmta.us]
Sent: Friday, May 05, 2006 11:55 PM
To: Comments, Regulation
Subject: Attention: PRA Comments-Cross-Border Survey
Attn: Mr. Eric Kringel
Senior Policy Advisor
Financial Crimes Enforcement Network
Alexandria, VA

By Email to: regcomments@fincen.gov

Dear Mr. Kringel:

The National Money Transmitters Association appreciates the opportunity to comment on the proposed collection of data on the cross-border electronic transmittals of funds conducted through our nation's financial institutions.

Our answers to the survey's numbered questions appear below. Below that, is a comprehensive list intended to illustrate the type of data fields our larger members' systems normally retain for all transactions, and are capable of reporting in digital form.

Comments were invited on the following issues:

- a) **Whether the collection of information is necessary or useful** – We believe the data may be useful for specifically-targeted retrospective financial investigations, as well as statistical surveys. We think, however, that FinCEN should plan and specify to the public, the way the data will be used, before embarking on the collection program.
- b) **The accuracy of the agency's estimate of the burden** – The agency correctly estimated the amount of time required to answer the survey itself, but the proposed data collection program requires close study as to the time and expense that will be required of all financial institutions, on an ongoing basis, should these requirements be adopted.
- c) **Ways to enhance the quality, clarity and utility of the information collected** – We recommend that FinCEN provide free money transfer software to smaller firms that have trouble affording it, standardize a common field structure for reports, and we urge the IRS to coordinate data collection efforts with the various state banking departments.
- d) **Ways to minimize the burden** – See response to (c)
- e) **Estimates of cost** – For those companies that already have advanced IT systems, the burden will be minimal. For those smaller institutions that may still be struggling, the cost of compliance will be prohibitive. For that reason, we recommend that free money transfer software be distributed, that will be capable of not only producing the cross-border reports, but have built-in anti-structuring and OFAC-checking features.

New requirements must be introduced slowly, as smaller entities may be incapable of complying and should not be criminalized as a result. On the other hand, fairness demands that all operators be made to play by the same rules, otherwise uneven costs will tilt the playing field.

It is for this reason that the NMTA believes that any new requirement must come with a commitment from FinCEN and the IRS to analyze the barriers to compliance, and assist money services businesses of all sizes to overcome those barriers in the most economical way. A pilot program with voluntary compliance may be useful in the beginning, in order to gain experience in these untested waters. The answers to the survey below are based on the assumption that we are referring to companies such as our larger members, who have already built sophisticated data systems.

Sincerely,

David Landsman
Executive Director
The National Money Transmitters Association, Inc.
12 Welwyn Road, Suite C
Great Neck, NY 11021
(917) 921-9529 cell
(516) 829-2742 office
(516) 706-0203 e-fax
david@nmta.us
www.nmta.us

Background Information

1. Please characterize the institutions your organization represents (i.e., banks, broker-dealers, currency dealers or exchangers, casinos, money services businesses, etc.).

Money services businesses.

2. How would you further describe the institutions your organization represents by the primary nature of your business (i.e., community banks, credit unions, money center banks, money transmitters, specialized business lanes, etc.).

Currently, 43 state-licensed money transmitters.

3. What is the approximate volume of the overall funds transfer business (by total number and aggregate dollar amount) your member institutions conduct over a one-year period?

\$16,165,634,193 in 68,039,457 transactions, for an average of \$237.59 per transaction

4. What is the approximate volume cross-border electronic transmittals of funds (by total number and aggregate dollar amount) your member institutions send and receive over a one-year period?

Same as above.

To the extent possible, please estimate the percentage of cross-border electronic transmittal of funds sent or received by your member financial institutions, in the following categories (if applicable):

- a. on behalf of their own customers,
- b. as an intermediary or correspondent for other institutions
- c. as internal settlement with their own institution's foreign affiliates or branches.
- d. as the U.S. financial institution that directly transmitted the payment order to or accepted the payment order from a financial institution located outside of the United States.

a. on behalf of their own customers: 100%

5. Do your member institutions send or receive cross-border electronic transmittal of funds in-house or through a correspondent?

Normally, foreign correspondents are used, i.e. either bank or non-bank financial institutions abroad

- a. What systems (e.g., SWIFT, Fedwire, CHIPS, proprietary system) are used to send or receive cross-border funds transfers?

N/A

- b. What is the proportional usage of each system if more than one system is used?

N/A

- c. Are there instances when the system used is dictated by the nature of the transaction or customer instruction? If possible, please exclude those situations where the decision is due to the fact that the receiving financial institution does not use a particular system.

N/A

Existing Record Maintenance and Compliance Process

6. How do your member institutions maintain the funds transfer records required by 31 C.F.R. § 103.33 (i.e., message system logs or backups, wire transfer instruction database, account history files, etc.)?

Electronically

- a. If the data is stored electronically, can the storage systems export such data into a spreadsheet or database file for reporting?

Yes

7. Approximately how many times in a one-year period does the government subpoena or otherwise issue a legal demand requiring your member institutions to produce cross-border wire transfer information?

Approximately 12 times per year, any and all records pertaining to a customer or agent

NOTE: We understand that many requests seek "any and all records" pertaining to an account or subject. Where possible, please distinguish those requests from more specific requests for cross-border electronic transmittals of funds.

8. Can you estimate the approximate total cost (e.g., person-hours or other costs) to your member institutions in time and expense responding to these legal demands? If you cannot estimate the costs incurred, please describe generally the resources involved in complying with such requests.

Transaction records in electronic form, agent or customer folders, correspondence, relevant BSA reports (CTRs, SARs, etc.), accounting records.

Foreign Transactions

9. Do your member institutions or any of their branches, subsidiaries, or affiliates transmit or receive cross-border electronic transmittals of funds from a location in either Australia or Canada?

Unknown

- a. If yes, please briefly describe the measures taken, including the general estimates of the costs in time and expense incurred, to ensure compliance with the cross-border funds transfer reporting requirements in those jurisdictions and the measures in place to monitor and maintain compliance.

N/A

10. If the Department of the Treasury required reports of cross-border electronic transmittals of funds involving amounts over \$3,000, what general steps would your member institutions need to take (and how burdensome would it be) to comply?

Establishing a query following the requested format, and producing a digital file for email once a month should not be a problem.

- a. Would the answer differ if the value threshold were \$10,000?

No

- b. Would the answer differ if there were no value threshold?

No

- c. How would these different thresholds affect the volume of the reporting from your member institutions?

Not at all

- d. How would the answer differ with the type of required reporting (e.g., electronic file upload, Web-based form)?

Electronic file upload would be more efficient

- e. How would the answer differ with the timing of required reporting (e.g., real-time, end-of-day, within 30 days)?

No more frequently than once a month, please, with 15 days' lead time.

- f. To the extent possible, please estimate any cost increase for cross-border electronic transmittals of funds that may result.

None

- g. To the extent possible, please describe any effects that reporting requirements may have on the volume or value of cross-border electronic transmittals of funds.

None

Potential Impact on Financial Institutions

11. If the Department of Treasury required reports of cross-border electronic transmittals of funds in a SWIFT, CHIPS or other file format specified by the Department, what steps would your member institutions need to take to extract such data from existing records to submit the information as required?

N/A

12. If the Department of Treasury required reports of cross-border electronic transmittals of funds but also provided exceptions for certain customers or types of transactions (i.e., internal settlement, identical originator and beneficiary, transfers to government entities, etc.), what exemptions would you suggest?

We would not suggest any exemptions, but be aware that some duplication will occur since much of our volume goes through banks.

- a. How difficult would it be for your member institutions to build such exceptions into the business process for creating the report?

Very

- b. Would the costs to implement the exceptions outweigh the benefits?

Yes

13. If the Department of the Treasury required reports of cross-border electronic transmittals of funds, should the requirement be limited to certain institutions (e.g., only the originating institution, only the beneficiary's institution, only the U.S. financial institution that directly transmits the payment order to or accepts the payment order from a financial institution located outside of the United States)? Please explain the rationale for your response.

Volume done in the role of intermediary financial institutions should be labeled as such, but not exempted.

14. Can your member financial institutions' automated systems distinguish between domestic funds transfer and a cross-border electronic transmittal of funds?

Yes

15. Among the following definitions of "cross-border electronic transmittal of funds" what potential advantages and disadvantages do you perceive? Do you have any suggestions for such a definition or can you highlight any particular issues that should be addressed in such a definition? (NOTE: All of the following definitions would exclude check, debit transmittal, ATM, or ACH payments.)

- a. Cross-border electronic transfer of funds means any wire transfer where the originator's and beneficiary's institutions are located in different countries and one of the institutions is located in the United States. This term also refers to any chain of wire transfers that has at least one cross-border element
- b. Cross-border electronic transfers of funds include transactions where either (1) a foreign office of a financial institution instructs a U.S. office of a financial institution to effect payment in the U.S., directly or indirectly, or (2) where U.S. office of a financial institution instructs a foreign office of a financial institution to effect a payment abroad, directly or indirectly.
- c. Cross-border electronic transmittal of funds means the transmission — through any electronic, magnetic or optical device, telephone instrument or computer — of instructions for the transfer of funds, other than the transfer of funds within the United States. In the case of SWIFT messages, only SWIFT MT 100 and SWIFT MT 103 messages are included
- d. Cross-border electronic transmittal of funds means an instruction for a transfer of funds that is transmitted into or out of the United States electronically or by telegraph, where the financial institution is acting on behalf of, or at the request of, another person who is not a financial institution

We prefer this last definition; simpler is usually better, but we suggest, instead of the exception for a person "who is not a financial institution,"

the phrase, “not in the role of intermediary financial institution, as already defined in the regulations.

Appendix: Illustrative list of fields that are routinely kept by licensed money transmitters.

Report Header Information:

- Reporting entity
- Entity type
- Date range
- Amount range
- Origin
- Order types

Invoice Fields:

- Invoice Number
- Invoice Date
- Invoice Time
- Any other ref #
- Internal Comments (e.g. memo fields related to investigations and complaints, messages from sender to receiver)
- Code Words

Status Fields:

- Open
- Paid (if paid, Date paid, ID shown)
- Pending
- Suspended (compliance hold, OFAC hold, OFAC block, credit hold, etc.)
- Void / Cancelled (by Agent, by Central Office, by Payer)
- Compliance Flag (if any)

Sender and Receiver Fields:

- (Possible additional 'on-behalf-of' sender, multiple senders, alternative beneficiaries.)
- FN, LN, MI, Full Name
- Address, City, State, Zip, Country, Phone
- ID Type, ID Number, ID Issuer, and expiration date
- Date of Birth
- Occupation

Amount Fields:

- US Net Transmission Amount, Foreign Equivalent Transmission Amount, Rate
- Settlement rates and amounts and distribution
- Total Due from Agent
- Commissions (%) and Fees (\$) broken down by distribution
- Total Fees and commissions charged to consumer (in USD)

Destination (Beneficiary's) Bank (if any):

- Bank Name
- Bank Address
- Branch Number
- Account #
- Account Type

Paying and Receiving Agent Data:

- Name and Full Address, sub-locations, location codes

Names and Approvals:

Agent Operator	HQ Operator
Agent Manager	HQ Approver

Please note: This listing does not discuss data validation rules or field structure issues.



May 5, 2006

Russell W. Schrader
Senior Vice President
Assistant General Counsel

By Electronic Delivery

Department of the Treasury
Financial Crimes Enforcement Network
P.O. Box 39
Vienna, VA 22183

Re: Attention: PRA Comments—Cross-Border Survey

Dear Sir or Madam:

This letter is submitted on behalf of Visa U.S.A. Inc. in response to the request for public comment (“Notice”) by the Financial Crimes Enforcement Network (“FinCEN”), published in the Federal Register on March 21, 2006.¹ The Notice seeks comment on a survey to obtain information from the banking and financial services industries to assist in determining the feasibility and impact of implementing a new reporting requirement for cross-border electronic transmittals of funds under the Bank Secrecy Act (“BSA”). Visa supports FinCEN’s decision to seek comment from individual banking institutions and financial services industry trade associations, and appreciates the opportunity to comment on this important matter.

The Visa Payment System, of which Visa U.S.A.² is a part, is the largest consumer payment system, and the leading consumer e-commerce payment system, in the world, with more volume than all other major payment cards combined. In calendar year 2005, Visa U.S.A. card purchases exceeded a trillion dollars, with over 510 million Visa cards in circulation. Visa plays a pivotal role in advancing new payment products and technologies, including technology initiatives for protecting personal information and preventing identity theft and other fraud, for the benefit of Visa’s member financial institutions and their hundreds of millions of cardholders.

EXEMPTION FOR CERTAIN TRANSACTIONS UNDER CURRENT RULES

The current rules under the BSA require covered financial institutions to create and retain records of specified transactions, including transmittals of funds. For example, if a “transmittal of funds,” as defined by the BSA rules,³ is in the amount of \$3,000 or more,

¹ Cross-Border Electronic Transmittals of Funds Survey, 71 Fed. Reg. 14,289 (Mar. 21, 2006).

² Visa U.S.A. is a membership organization comprised of U.S. financial institutions licensed to use the Visa service marks in connection with payment systems.

³ 31 C.F.R. § 103.11(jj). We refer to “transmittal of funds,” and the corresponding requirements that apply to non-bank financial institutions, solely for the sake of using terminology consistent with the Notice, even

Visa U.S.A. Inc.
P.O. Box 194607
San Francisco, CA 94119-4607
U.S.A.

t 415 932 2178
f 415 932 2525

Department of the Treasury
Financial Crimes Enforcement Network
May 5, 2006
Page 2

the financial institution that accepts the transmittal order must create a record containing particular items of information about the order, including the name and address of the transmitter, the amount of the transmittal order, and certain information to identify the recipient.⁴ In addition, both the financial institution acting for the transmitter and the receiving institution must retain records regarding the transmittal order in a form that satisfies established retrievability standards.⁵ The term “[t]ransmittal of funds” is broadly defined to include “[a] series of transactions beginning with the transmitter’s transmittal order, made for the purpose of making payment to the recipient of the order.”⁶ However, the existing BSA rules contain a specific exemption for any “[f]unds transfers governed by the Electronic Fund Transfer Act of 1978 [“EFTA”], as well as any other funds transfers that are made through an automated clearinghouse [“ACH”], an automated teller machine [“ATM”], or a point-of-sale [“POS”] system.”⁷

IMPORTANT TO RETAIN EXEMPTION FOR DEBIT, POS, ACH, AND ATM TRANSACTIONS

Visa believes that FinCEN has appropriately stated in the Notice that, for the purposes of facilitating comment on the survey, the term “cross-border electronic transmittal of funds” contains a broad exemption for “any debit transmittals, [POS] systems, transaction conducted through an [ACH] process, or [ATM].”⁸ Visa believes that the reporting requirements contemplated for cross-border transmittals should not extend to the categories of transactions described in the existing exemption, regardless of whether a transaction is conducted between individuals or business entities.

The Visa Payment System, which operates largely through POS and ATM systems, may conduct as many as 5,000 transactions *per second* in an ordinary business day. In addition, other electronic payments systems conduct huge volumes of transactions through POS and ATM systems on a daily basis. The vast majority of these transactions are related to legitimate transactions for the purchase of goods and services conducted between individuals and merchants that bear no relation to money laundering or terrorist financing activities. Even assuming, for the sake of this analysis, that a threshold amount per transaction is established at \$3,000 or a higher figure, requiring financial institutions to create and retain detailed records of information bearing on transactions governed by the EFTA or otherwise conducted through POS or ATM systems is simply not feasible given the enormous volume of transactions. Moreover, Visa respectfully submits that requiring records of transactions governed by the EFTA or otherwise conducted through POS or ATM systems would be inconsistent with the statutory mandate to establish reporting and recordkeeping requirements that are “reasonably necessary” to detect and take action against money laundering or terrorist financing.

though the substantively identical term “funds transfer” is used in the requirements that apply to banks.

31 C.F.R. § 103.11(q); 31 C.F.R. § 103.33(e).

⁴ 31 C.F.R. § 103.33(f).

⁵ 31 C.F.R. § 103.33(f)(4).

⁶ 31 C.F.R. § 103.11(jj).

⁷ *Id.*

⁸ 71 Fed. Reg. at 14,289.

Department of the Treasury
Financial Crimes Enforcement Network
May 5, 2006
Page 3

If FinCEN determines to move forward to propose reporting requirements for cross-border transmittals, Visa urges FinCEN to avoid creating any unwarranted inconsistency in the nature or scope of the funds transmittals subject to reporting requirements. In this regard, the language of the exemption should be clarified to cover any “funds transfer governed by the EFTA,” consistent with the language of the current recordkeeping requirements.⁹ Thus, regardless of the particular general definition of “cross-border electronic transmittal of funds,” Visa recommends adopting an exemption from that definition, as follows:

Funds transfers governed by the Electronic Fund Transfer Act of 1978 (“EFTA”) (Title XX, Pub. L. 95-630, 92 Stat. 3728, 15 U.S.C. § 1693, *et seq.*) and the rules promulgated under the EFTA, as well as any other funds transfers that are made by check, by debit transmittal, through an automated teller machine, or a point-of-sale system, are excluded from this definition.

Visa encourages FinCEN to continue to work with trade groups representing financial institutions to develop reasonable standards that will facilitate the efforts of law enforcement agencies to thwart money laundering and terrorist financing, without unduly impeding the legitimate operations of financial institutions.

We appreciate the opportunity to comment on this important matter. If you have any questions concerning these comments or if we may otherwise be of assistance in connection with this matter, please do not hesitate to contact me, at (415) 932-2178.

Sincerely,

Russell W. Schrader
Senior Vice President and
Assistant General Counsel

⁹ 31 C.F.R. § 103.11(q), (jj).

APPENDIX H – TECHNICAL ALTERNATIVES ANALYSIS

In developing our assessment of the technical feasibility of building and implementing a system to collect, process, store, secure, analyze, and disseminate cross-border funds transfer reports, we gathered information from published sources, issued a Request for Information from private sector information technology developers, and consulted with data systems experts from other government agencies. The study is also based on the lessons learned from a funds transfer proof-of-concept system developed in partnership with our colleagues at AUSTRAC. Other conclusions derive from discussions with technical experts from both the government and private sectors with experience in the design and construction of systems for the collection and analysis of extremely large volumes of data.

Assumptions About System Architecture

The underlying premise of the assumptions listed below is that the architecture of a system to collect, process, store, secure and disseminate cross-border funds transfer data must enable FinCEN to leverage existing infrastructure, interfaces, capabilities, and services; to benefit from the return on the investment in BSA E-Filing and other systems; and to integrate these under a common data architecture with shared application and data services.

FinCEN made the following assumptions when preparing this report:

- FinCEN plans to improve the level of constructive control it exerts over BSA data collection and management and to assume over time the full lifecycle BSA data management responsibilities.
- FinCEN plans to enhance the use and capabilities of its BSA E-Filing system as an integral component of the integrated BSA data center.
- FinCEN would provide direct, private, and secure communications between its collection system and reporting institutions' systems.
- Stability - The funds transfer system will meet all uptime and response time performance specifications as FinCEN's current and planned BSA data systems.
- Failover and disaster recovery processes and technologies should be in place.
- Risk – The architecture design should introduce minimal impact on the existing FinCEN technical environment.

- Flexibility – The chosen architecture must easily integrate existing and new technologies.
- Scalability – The architecture design should be easy to expand and scale. The target funds transfer system must scale to process 350-500 million transaction records per year, securely store 3-5 years of data available for online access, initially serve several hundred reporting financial institutions and several thousand data users, and provide 24/7/365 availability.

Data Warehouse Architecture Design Principles

A data warehousing architecture defines the technical framework needed to ensure that a variety of data warehousing components work together to provide the decision support capability expected by business users now and in the future. There are five main objectives of the architecture. 1) *Business Value*: Information systems are a means to an end, not an end unto themselves; 2) *Usability and Performance*: funds transfer data warehousing systems should be easy to use and provide useful business information within acceptable timeframes; 3) *Adaptability*: Data warehousing systems should accommodate changes in requirements and technologies in a cost effective manner; 4) *Interoperability*: A data warehouse should work well with the large number of operational and decision support systems in use at FinCEN; and 5) *Availability*: The data warehouse should incorporate redundancy sufficient for decision support and should meet the availability requirements typical of mission critical systems.

Service-Oriented Architecture

A Service-Oriented Architecture (SOA) provides the necessary components to facilitate the secure distribution and sharing of funds transfer data between FinCEN, financial institutions regulators, law enforcement agencies, and the intelligence community. In SOA, development is component-driven and based on reusable parts or services. SOA itself is not an application, but more of a methodology or architecture. One element of an SOA is the enterprise service bus (ESB). The role of an ESB is to provide the backbone on which you can build a SOA. SOA handles all of the service definitions, service creation, integration, and deployment and management. SOA enables the entire lifecycle of building, deploying, and managing multiple services while introducing minimum impact on the component parts. ESB simply acts like an application server. SOA permits a system owner to leverage the architecture design with existing technologies and systems, and to reuse the functionality of existing systems rather than building them from scratch. Eliminating overlapping point-to-point connections simplifies maintenance and integration. Developing the funds transfer system using the SOA design will provide FinCEN with a flexible integration approach based on dynamic (just-in-time integration), not hard-wired (point-to-point) integration.

Web Services

Most SOA implementations use Web services based on XML and HTTP.⁸² The Web services a standardized way of integrating web-based applications using XML, SOAP, WSDL and UDDI open standards over an internet protocol backbone.⁸³ XML is used to tag the data, SOAP is used to transfer the data, WSDL is used for describing the services available, and UDDI is used for listing what services are available. Web services allow organizations to communicate data without intimate knowledge of each other's IT systems. Web services also allow different applications from different sources to communicate with each other without time-consuming custom development or significant modification of existing systems, and because all communication is standards-based, web services are independent of a single operating system or programming language. Because web services are loosely coupled and granular, they provide a better infrastructure for protecting confidential data and securing business processes than traditional, application-centric security approaches.

Data Acquisition

The process of receiving and processing funds transfer data is similar to collecting other BSA data electronically. It involves interaction with a wide range of financial institutions. These financial institutions range in nature from relatively small organizations and money services businesses, to large organizations. This implies that the funds transfer system must address a wide range in both the volume of submissions, and in the technical sophistication of these entities.

Ideally, FinCEN could deploy a single solution to communicate with all the reporting financial institutions. However, industry best practices reveal that no single information technology solution, whether a proprietary (Secure FTP), virtual private network (VPN), secure web-based protocols (S-HTTP), or customized application, is appropriate for all financial institutions. Accordingly, FinCEN must combine solutions to allow myriad financial institutions to transmit data to FinCEN securely. The use of SSL and S-HTTP, in conjunction with Web forms hosted by FinCEN should adequately serve low-volume reporting institutions. Large volume reporting institutions can use the secure protocols implemented in BSA E-Filing to transfer the funds transfer data from their network into the FinCEN system securely.

82 HTTP - HyperText Transfer Protocol, the underlying protocol used by the World Wide Web. HTTP defines standards for the format of data presented, and prescribes what actions Web servers and browsers should take in response to various commands.

83 SOAP - Simple Object Access Protocol, an XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. SOAP messages are independent of any operating system or protocol and support a variety of Internet protocols. WSDL - Web Services Description Language, an XML-formatted language used to describe a Web service's capabilities as collections of communication endpoints capable of exchanging messages. WSDL is an integral part of UDDI, an XML-based worldwide business registry. WSDL is the language that UDDI uses. UDDI - Universal Description, Discovery, and Integration. A Web-based distributed directory that enables businesses to list themselves on the Internet and discover each other.

The BSA E-Filing system currently serves exactly this type of user community. The BSA E-Filing system uses InFlowSuite™ a commercial off the shelf (COTS) tool to manage the submission process. The system can ingest submissions in a variety of formats and using a variety of protocols, and control these submissions by placing them in protected storage. The system then queues submissions for subsequent processing. This allows the system to operate over a wide range of load conditions, queuing submissions received during periods of high stress for processing when submission volumes diminish. This gives the system an extremely wide “dynamic range” within which it can remain responsive to submitters’ needs.

Because the BSA E-Filing system employs service-oriented architecture design and web services, the integration of funds transfer data into BSA E-Filing becomes possible. The BSA e-Filing system is stable, and adheres to a 99.999% availability standard. Usage is growing and FinCEN currently receives 47% of its total BSA filings using the system. To date reporting institutions have filed over 9 million reports electronically and with the recent inclusion of larger banks, FinCEN is processing 350,000 to 380,000 reports through the system per month (as compared to an anticipated 30-40 million funds transfer reports per month). Over 300 of the 650 identified top filers are using the system.

To accommodate the concerns of filing institutions about data security, the BSA E-Filing system implements a solution that combines SSL (Secure Sockets Layer), S-HTTP (secure HTTP) and web-based forms. SSL and HTTPS are mature open standards-based communication protocols that enjoy wide adoption and that all World Wide Web browsers implement. For the end user, the use of browser technology eliminates the need to purchase and deploy specialized software and lowers maintenance and support costs. Both Canada and Australia have adopted this approach in their reporting systems. For example, a medium-volume reporting institution could prepare a file containing all of the required reports and by logging into a secure web portal hosted by FinCEN, manually upload the file to the FinCEN system. In addition, FinCEN could provide a secure web-based form by which small-volume reporting institutions could file reports regarding single transactions.

FinCEN’s BSA E-Filing system relies upon Sterling Commerce's Connect:Direct software to provide reporting institutions with a secure communications tunnel between their network and FinCEN’s. Large-volume reporting institutions can employ FinCEN’s BSA E-Filing system by using the Connect:Direct FTP protocol over SSL to secure the control and data connections over the internet. This has proved to be an effective method for hundreds of financial institutions to send their reports to FinCEN. The benefits of extending this tool include having a highly secured and homogeneous environment, which reduces the need to support multiple communication standards. This solution does require reporting institutions to obtain and implement compatible communications software.

Data Transformation, Enhancement, and Loading

Data Quality

Data quality assessment is an integral part of data warehouse development. The objective in implementing a data warehouse is to enable the users to produce better analysis and make better decisions by making available accurate, correct, and high quality data. If the data does not satisfy high quality standards, the value of the data is lost.

There are a number of data quality problems that a data warehouse architecture must address:

- Data Validity - Non-conformance of the submitted data to permitted values.
- Data Decay - Values are correct at one point in time but the values change and the data is not automatically updated to reflect the change.
- Synchronization - Values of core data stored in multiple places are not maintained in consistent ways.
- Business Rules - Values that have rules associated with them are not programmatically enforced.

Without consistently high quality data, users may miss opportunities of detecting potentially important information in the data. For example, a recent search of FinCEN's BSA reports revealed 144 variations in a single street address. Because FinCEN does not have direct quality control over the data collection process, in order to make it useful and sensible, data must be enhanced and improved before analysts and investigators can make use of it.

If data quality is suspect, analysts cannot effectively use the information or share it properly. The challenges FinCEN may face while trying to integrate the cross border funds transfer data with BSA data include:

- Finding authoritative information sources (master data stores)
- Knowing the underlying location, structure, context, quality and use of information
- Determining how to resolve differences in meaning (semantic reconciliation)
- Understanding how to profile and ensure data quality
- Applying methods to connect to data sources (choosing among several data integration technologies)

- Knowing how to encapsulate information models to support business service composition

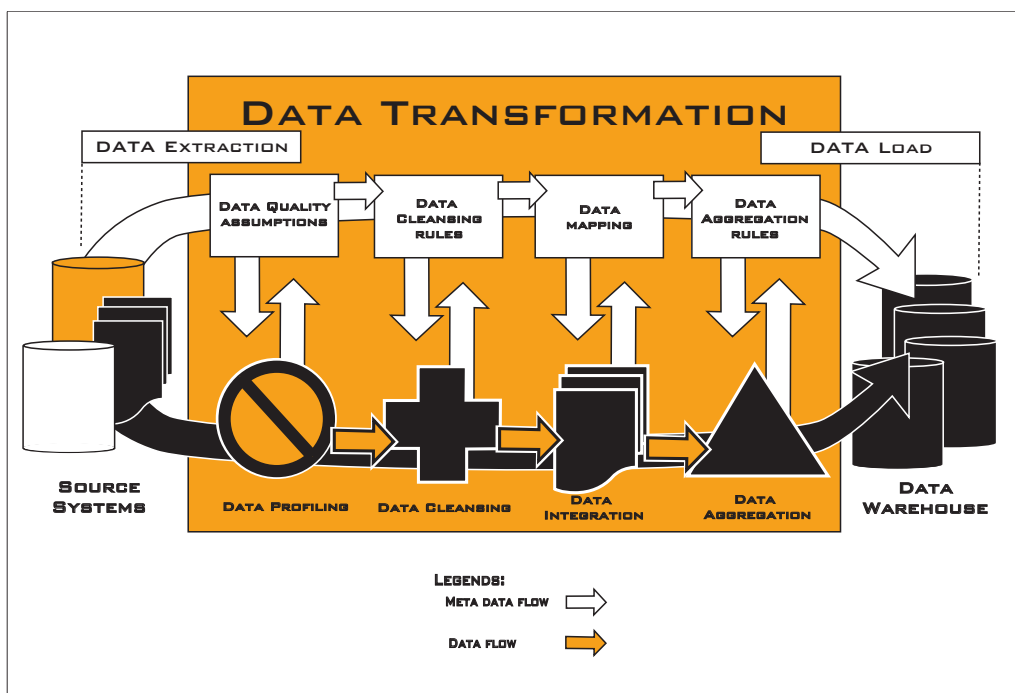
High quality data is a prerequisite for a successful data warehouse and for effective data mining and other quantitative analysis. Managing data quality requires system developers to view data quality as a business issue and to approach it in a structured manner. The methodology for data quality management must focus on three critical components:⁸⁴

- People and skills: Cultural and organizational change to build awareness, understanding, ownership and engagement of key stakeholders
- Processes: Establishing standard and repeatable workflows for addressing data quality, including metrics, a focus on data quality trends and iterative tuning of data quality rules
- Technology: Implementing data quality analysis, monitoring, controls and enhancement functionality

Data transformation is computationally intense, and requires sufficiently powerful systems to accomplish the task within acceptable periods. For example, determining whether two different funds transfers originated from the same individual is not easy. Funds transfer instructions rarely contain unique indicators such as a Social Security number; small variations in format and spelling can defeat simple word matching; addresses are not always provided and money launderers can use multiple, shifting account numbers.

Simply put, a data warehouse system must establish a standard for data quality and upon receipt, the system must examine the submitted data, identify and correct errors, convert it into a form suitable for analysis, and load the data into the data warehouse. In terms of technical feasibility, a funds transfer reporting system must incorporate adequate processes and technology to manage the data quality. These steps in this “enhancement-transformation-and-load” (ETL) process are data profiling, data enhancement, and data load.

⁸⁴ Data Quality Methodologies: Blueprints for Data Quality Success, Ted Friedman, July 26, 2005



Data Profiling

To ensure that a data warehouse system can handle all these problems and establish links to other data, the system must incorporate a data profile. In general, data profiling is a process of discovering the characteristics of a target set of data. Data profiling is a critical diagnostic process that provides information about the quality of the collected data.

Data profiling generally includes data consistency discovery, data business rules validation, and data relationships verification. Data consistency discovery checks whether the patterns within the submitted data adhere to expected patterns or formats. Data business rules validation typically focuses on analyzing and determining if the data values are accurate (i.e., identify ZIP codes that contain only four digits), complete, and compliant with the business rules (i.e., text appearing in the “amount” field). Data relationships verification encompasses not only the identifying data redundancy and potential key inter-data relationships but also optimizing the relationships between data elements, and data tables. In simpler terms, it looks for repetitive use of the same information in multiple places in a data record and begins to identify common elements between different data records (i.e., an account number may appear in both a funds transfer report and a Currency Transaction Report – the data profile will reflect this common element).

To develop meaningful business rules, identify the relationships between funds transfer reports and other BSA data, and to handle the errors or rejected records, will require extensive requirements development. Commercial off-the-shelf (COTS) data profiling tools exist that can analyze a given set of data and proffer appropriate business rules to apply to the data. These products usually include common business rules that apply to any organization. During the development of a funds transfer reporting system, it will be vital to apply data profiling analysis and tools to sample data.

Data Enhancement

Data enhancement is the process of applying the business rules that arise from the data profiling process, to “improve” the data. The enhancement of the data can include “data cleansing” - the alteration of certain data elements to ensure consistency (i.e., 5-digit zip codes expanded to ZIP+4 format) or the addition of data elements to enhance the usefulness of the data (i.e., addition of “county” information based on address and ZIP code); “data integration” – the conversion of multiple data structures (i.e., SWIFT and non-SWIFT funds transfer messages) into a single consistent format and the conversion of certain data elements into human readable form (i.e., “bank identifier codes” into the full name of a financial institution); and “data aggregation” - the summarization of certain elements of the data to enhance accessibility. The data enhancement process ensures that data is consistently structured into correct and appropriate fields, formatted (e.g., abbreviations are expanded into full words), and is grouped into appropriate collections.

Metadata Management

After the system enhances the data and structures it consistently, the next step is to integrate and aggregate the data. Depending on the source of data, data integration can be very complicated. The result of data integration usually generates new data entities or attributes, which are easy for end users to access and understand. Data aggregation is a key data warehouse requirement that facilitates the presentation of data in the form of business reports. Systems also generally implement data aggregation to improve query performance.

Overall, the ETL process results in the creation of “metadata” or “data about the data.” Metadata is information about the data such as data source, data type, extraction and transformation rules, and any other information needed to support and manage the operation of the data warehouse.

There are three types of metadata that are associated with data warehousing, including technical metadata, operational metadata and business metadata. Technical metadata describe the data and explain what has been done to cleanse, enhance, and standardize the data. The operational metadata created during the ETL process includes records of the job executed, the date and time when the job executed, the job status (successful/failed), a system generated

Batch_ID and the number of records extracted and loaded. The metadata adds a layer of context to the data by providing consistent views of, for example, abbreviations, acronyms, and other codes in the data.

As a result, the “size” of a data set increases dramatically through the enhancement process. The addition of new elements and the transformation of others have a significant impact on storage requirements. All these operational metadata are available to the user in support of analysis and reporting activities.

Designing an appropriate ETL process requires both familiarity with the specific types of data and general database skills. Therefore, both skilled database administrators and end users should be involved in this task. Because familiarity with funds transfer message data will be central to the design of the system, FinCEN will need to rely heavily upon the expertise of U.S. financial institutions throughout the development process.

Data Load

Once the transformation process is complete, the system must load the enhanced data into the data warehouse. The data load process depends primarily on the kinds of query operations the users will perform and the volume of data that must be available on the system. These factors will determine the structure of the data warehouse itself, and in turn, the process for loading the data.

Data Warehouse Architecture Alternatives – Centralized or Federated

The three most common data warehouse architectures are: (1) hub and spoke architecture (i.e., centralized data warehouse with dependent data marts), (2) centralized data warehouse (with no dependent data marts), and (3) federated data warehouse (independent data marts with common elements). The first two are centralized approaches and the third is a non-centralized approach.

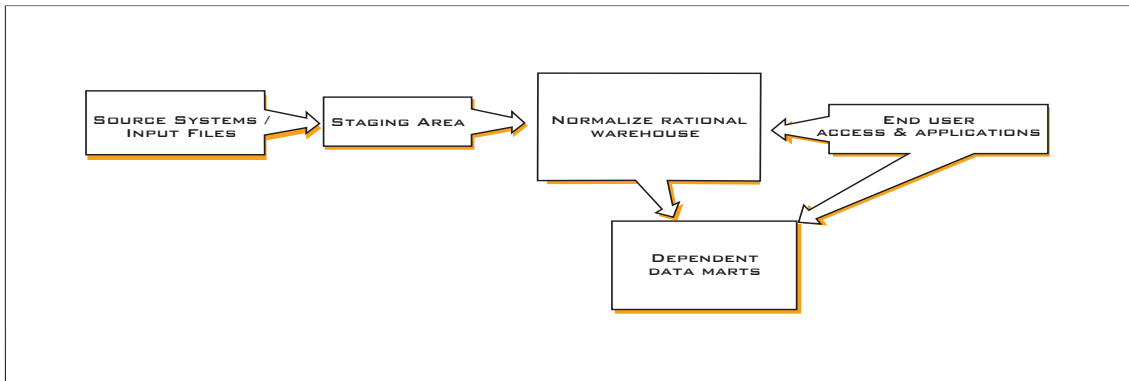
Eight factors potentially affect the selection of the data warehouse architecture.

- Information Interdependence -- There is a high level of information interdependence where one or more funds transfers relate to one or more large cash transactions recorded in the CTR data, for example. In this situation, the ability to share and integrate divergent information sources is important.
- Urgency of Need -- Some architectures are more quickly implemented than others, which can impact the architecture selected.
- Nature of End User Tasks -- Some users perform more complex tasks than others do. Detailed requirements analysis in close partnership with FinCEN's law enforcement and regulatory partners would be a prerequisite for defining the appropriate architecture.

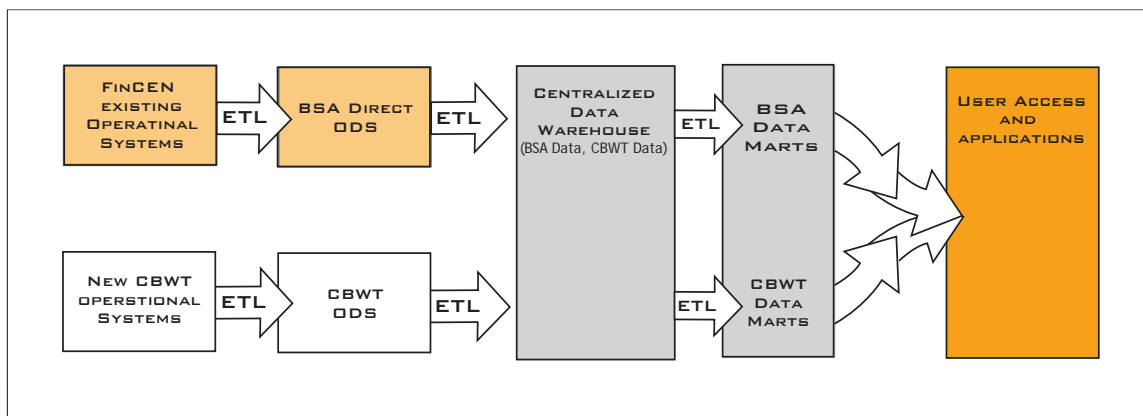
- **Constraints on Resources** -- Some data warehouse architectures require more resources than others do. As a result, the availability of IT personnel, business unit personnel, and monetary resources can influence the selection of the architecture.
- **Strategic View** -- Based on current FinCEN's strategic view of the warehouse, integration of multiple different information sources is necessary.
- **Compatibility with Existing Systems** -- There are many benefits to implementing solutions that are compatible with existing systems. The cost and time benefits of implementing a funds transfer data warehouse that is compatible with existing systems are substantial.
- **Perceived Ability of Developers** -- It will be essential that FinCEN dedicate sufficient and appropriately skilled project management resources to the management of the acquisition and development of such a system.
- **Technical Issues** -- A variety of technical considerations affect the choice of architecture – the ability to integrate metadata; scalability in terms of the number of users, volume of data, query performance; the ability to maintain historical data; and the ability to leverage existing infrastructure.

Hub and Spoke Architecture

A hub-and-spoke architecture builds upon an enterprise-level analysis of the system users' data requirements. A hub-and-spoke architecture is a scalable and maintainable infrastructure. The architecture is developed in an iterative manner, subject area by subject area. That is to say that initially, all data is combined into a single data repository, and other specialized "data marts" are created by extracting subsets of that data based on frequently used queries. These data marts enhance certain queries by organizing the data according to pre-defined needs of certain users. For example, a centralized data warehouse might contain a complete collection of all BSA reports, while separate data marts contain SARs, CTRs, CMIRs, funds transfer reports, and so on.

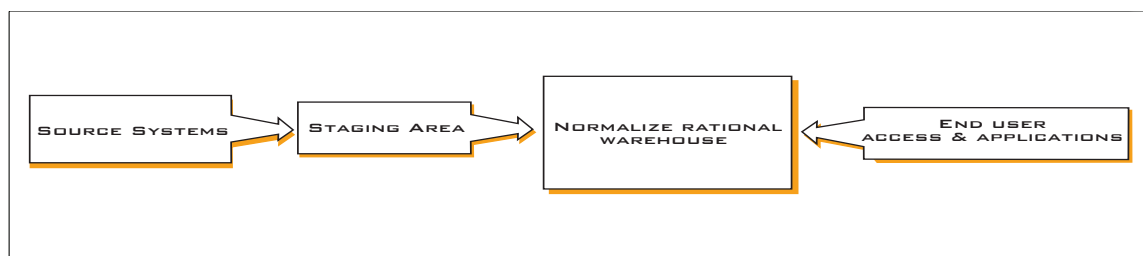


The figure below represents a hub-and-spoke approach to a funds transfer data system. Under this scenario, FinCEN would consolidate data from both the funds transfer and the BSA data systems into a single, centralized data warehouse. During the data transformation process, the existing reference data and business rules can be reused to cleanse the funds transfer data before it is loaded into the data warehouse. Depending on the business requirements, the system could extract a subset of data from the data warehouse to create data marts for answering specific questions.



Centralized Data Warehouse

A centralized data warehouse is similar to the hub and spoke architecture except that there are no dependent data marts. The data warehouse contains atomic level data, some summarized data and logical dimensional views of the data. Users perform queries directly on the centralized store of data. The following figure illustrates this architecture.

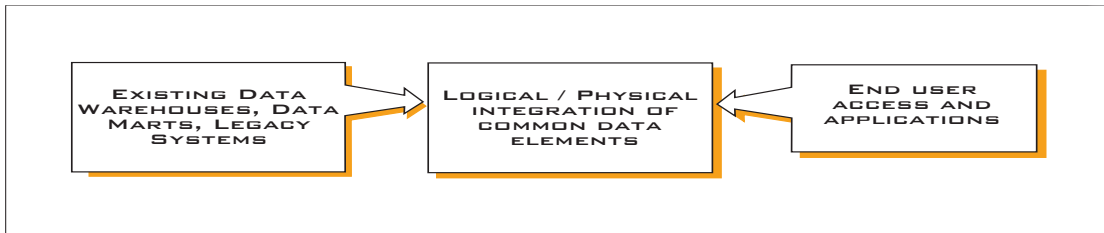


Implementation of a centralized data warehouse requires that FinCEN would implement an entirely new system for the collection of all BSA reporting, including funds transfer information. The proof-of-concept system developed by FinCEN and AUSTRAC implements a centralized architecture.

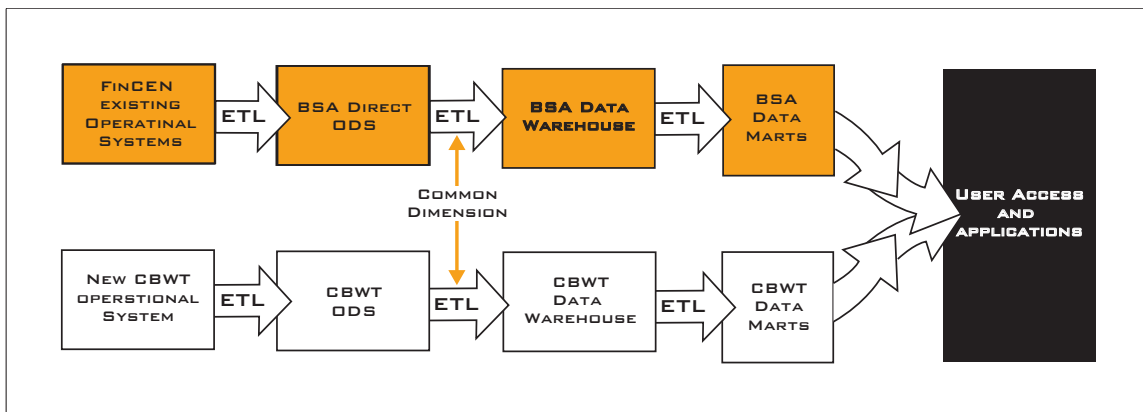
Whether the funds transfer data system includes dependent data marts or not, a centralized data warehouse architecture will entail more up-front investment in time and money. FinCEN will need to be able to identify the common data elements between the existing BSA data and funds transfer data in order to establish the linkage between the two systems so that an integrated and consistent view of the data is available to the users. FinCEN must create a new data model to represent both BSA and funds transfer data simultaneously. The new integrated data model also would require structural changes to the existing BSA databases. Depending on the complexity of the changes, it may require significant effort to implement. FinCEN would also need to modify and enhance the current ETL procedures and reports. Further, FinCEN would need to create new business rules to replace the ones currently used or significantly modify existing business rules to accommodate the new data.

Federated Data Warehouse

A federated architecture extends the existing operational systems, data marts, and data warehouses that are already in place. A federated architecture introduces a “services layer” between the user and the multiple data sources available (i.e., current BSA data and cross-border funds transfer data). Based on users’ varying business requirements, the system manages the distribution of the users’ queries across the multiple data sources, aggregates the results, and presents a single result to the user. From the users’ perspectives, there is a single data source and the technical management of the query is invisible to the user. This process integrates multiple sets of data either logically or physically using these common or shared elements, global metadata, distributed queries, or other methods. As a result, users conduct queries on the integrated data elements, reducing the computational load on the respective systems that house the data, and increasing the response time of the system. The separate data sets remain available as well for more detailed query and analysis. A federated architecture provides a solution for environments that already have a complex, existing decision support environment or multiple data sets and do not want to create an entirely new environment.



The figure below depicts a federated database for the funds transfer system. With this design, FinCEN would create a new funds transfer data warehouse. In this example, the current BSA data continues to reside within a separate BSA data warehouse. Each system will maintain its own ETL procedures, implementation schedules and data warehouse. However, the working ETL procedure logic and tools will apply effectively to the funds transfer system. Both systems would apply the same reference data to cleanse the funds transfer data to make it consist with the BSA data. Minimum design changes will be required for the existing BSA data systems. The implementation schedule of this kind of funds transfer system can be flexible and will not impact significantly on the existing production systems. The federated environment also provides funds transfer system with more choices of the infrastructure selection that allows FinCEN to choose the latest and best technology.



A federated architecture also provides a strong foundation for distributing the computing load and adapting the system to the various needs of different user communities. With a federated architecture, FinCEN would be able to deploy customized portals designed to serve the needs of different external user groups (i.e., regulatory, law enforcement, internal FinCEN users) without the need to redesign the system, limit system capabilities to a “lowest common denominator” of features, or build a system that is all things to all users. By avoiding “one size fits all” architecture, FinCEN will be better able to focus on the particular needs

of different user communities. Such an approach also permits more control over system changes and facilitates an incremental investment in the system development. The initial investment will focus on the data collection and storage system, while hardware, bandwidth, and other infrastructure costs that arise as user needs develop can be distributed over time.

The keys to the success of a federated architecture lie in the development and adherence to a consistent data standard, the use of standardized extracts, a robust metadata repository, and toolset to maintain and translate multiple sets of data definitions. It is also critical that a common business model be defined which will provide the basis for common dimensions. The common dimensions represent the dimensions having identical business meaning, structure, and data. For example, the “currency” of the data (i.e., its age) is a common dimension for both traditional BSA data and funds transfer reports. However, the currency of the BSA data is very different from the funds transfer data. The funds transfer data may be as little as twenty-four hours old if filed daily, but the other BSA data may be as much as two months old when it is first available to analysts because the BSA allows filers to submit the data up to 60 days after the transactions occurred. The volume of the funds transfer data is many times larger than the BSA data. To maintain an acceptable performance level, the system might only make three years worth of funds transfer data available to users while it offers more than ten years worth of BSA data. FinCEN will need a very robust services layer that can query two very large volumes of data warehouses and integrate the information on the fly to provide users with a consistent view. The system hardware that supports both data sets must be substantial so that the response time is acceptable.

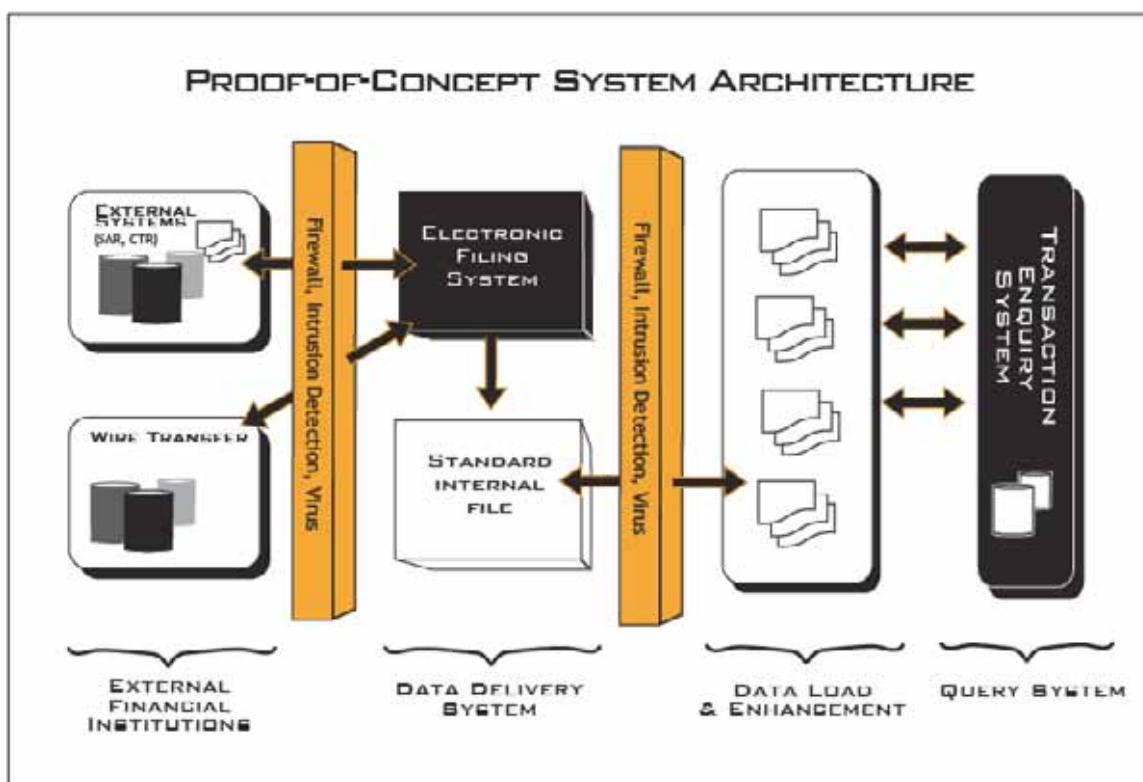
Fortunately, technology continues to evolve. For example, grid computing enables the virtualization of distributed computing and data resources such as processing, network bandwidth and storage capacity to create a single system image, granting users and applications seamless access to vast IT capabilities. Grid computing relies upon an open set of standards and protocols — e.g., Open Grid Services Architecture (OGSA) — that enable communication across heterogeneous, geographically dispersed environments. With grid computing, organizations can optimize computing and data resources, pool them for large capacity workloads, share them across networks, and enable collaboration.

Many financial services businesses have implemented grid computing technology and realized increasing productivity and flexibility in sharing data and computing resources. Grid computing technology provides a means to leverage FinCEN’s existing investments and infrastructure and to optimize the utilization of computing capabilities.

Lessons Learned Technical Issues – Proof-of-Concept

Beginning in March 2006, FinCEN constructed a proof-of-concept system based on an architecture and software employed by AUSTRAC for managing the

receipt, storage, analysis, and dissemination of its IFTI reports. The proof-of-concept system was, necessarily, a very small-scale version of the system, designed to permit FinCEN to test AUSTAC's architecture and to determine whether a similar approach might fill the needs of FinCEN in the event it requires such reporting under the BSA. As noted above, AUSTAC's system implements a centralized data architecture for the management of IFTI reports and the other reporting AUSTAC collects. AUSTAC and FinCEN personnel modified the system to accommodate SARs, CTRs, and funds transfer data from U.S. institutions. The figure below illustrates, at a high level, the general architecture of the proof-of-concept system.



Through this experiment, FinCEN was able to draw the following general conclusions about handling cross-border funds transfer data in the U.S. First, a cross-border funds transfer data warehouse should make available to the user only those data elements that their partner agencies find useful to analysis. The data warehouse should separately preserve the entire funds transfer report for auditing and advanced analytical purposes. To make the entire funds transfer message available to all users will dramatically increase the data load and dramatically increase storage requirements. Second, the system should distribute data sources for special analytical requirements. In other words, depending on the requirements, the system should replicate and store the data in a separate environment for particular purposes such as data mining, link analysis, or other advanced analysis by specific subsets of users. Third, based

on a robust user requirements analysis, the system should integrate multiple commercial off-the-shelf (COTS) tools to satisfy users' needs. The system design must reflect that one size does not fit all and therefore should implement appropriate tools at the services layer. Fourth, the proposed system should integrate COTS products as much as possible. AUSTRAC's system contains mainly custom software developed by in-house IT staff. This solution is viable for AUSTRAC because it employs such staff. FinCEN employs a much smaller number of in-house technical experts and therefore should consider COTS products for ease of maintenance. Last, FinCEN must pay special attention to the development of a data load process tailored to high volume reporting. The data load method adopted in the AUSTRAC system is not optimized for loading the much larger volume that FinCEN anticipates.

APPENDIX I – BSA E-FILING FACT SHEET

What is the BSA E-Filing System?

BSA E-Filing (BSA E-Filing) is the system that supports electronic filing of Bank Secrecy Act (BSA) forms (either singly or in batches) by a filing institution to the BSA database through a FinCEN secure network. It also allows members of filing organizations to send secure messages to FinCEN (and receive responses when appropriate). In addition, FinCEN can use BSA E-Filing to issue advisories and BSA E-Filing system updates to the BSA E-Filing user community.

BSA E-Filing was originally called PACS (PATRIOT Act Communications System), because the system was mandated by Section 362 of the USA PATRIOT Act. The system was renamed in February 2005.

How does BSA E-Filing Work?

The BSA E-Filing system is hosted on a secure website accessible on the Internet. Institutions that file BSA forms with FinCEN use digital certificates to access the BSA E-Filing system securely. Designated personnel from a filing institution can access BSA E-Filing after they have applied for and received a digital certificate from a government-approved certificate authority.

More information about the enrolling in and using BSA E-Filing is available at ["Should I Use BSA E-Filing?"](#) on the [BSA E-Filing website](#). Step by step instructions for enrolling are provided online at [Getting Started](#).

What BSA forms can be filed using BSA E-Filing?

Currently, the forms that can be E-Filed are:

- CTR (Currency Transaction Report)
- CTRC (Currency Transaction Report by Casinos)
- SAR (Suspicious Activity Report by Depository Institutions)
- SARC (Suspicious Activity Report by Casinos and Card Clubs)
- SAR MSB (Suspicious Activity Report by Money Services Businesses)
- SAR SF (Suspicious Activity Report by the Securities and Futures Industries)
- DEP (Designation of Exempt Person)
- The Money Services Business Registration and other forms will be added as they become available.

What are the advantages of using BSA E-Filing?

BSA E-Filing is cheaper, faster, more accurate, and more secure than paper or magnetic media filing. A recent Treasury Inspector General report found BSA E-Filing to be an effective mechanism for filing BSA reports. The same report concluded that institutions using BSA E-Filing to file reports generally found the system easy to use.

Who uses BSA E-Filing?

More than 2,300 users representing 700 institutions actively use the system to file BSA forms with FinCEN. Since its implementation in October 2002, more than nine million forms have been successfully E-Filed and the numbers continue to grow. In fact, institutions file 350,000 to 380,000 forms through BSA E-Filing in March 2005.

As of March 2006, approximately 47% of all BSA filings and nearly 40% of the critical Suspicious Activity Reports - are now E-Filed.

APPENDIX J – PRELIMINARY WORK BREAKDOWN SCHEDULE

Task	Duration	Start Date	Finish Date	Predecessors
1 Acquisition Strategy and Planning	200 days?	October 2, 2006	July 6, 2007	
2 Acquisition Planning	15 days	October 2, 2006	October 20, 2006	
3 Develop Concept and high-level Requirement definitions	15 days	October 23, 2006	November 10, 2006	2
4 Develop performance Requirements and Measures	15 days	October 23, 2006	November 10, 2006	2
5 Design and develop evaluation criteria	15 days	November 13, 2006	December 1, 2006	3,4
6 Develop RFP (SOW)	40 days	November 13, 2006	January 5, 2007	3,4
7 Issue RFP	1 day?	January 8, 2007	January 8, 2007	6
8 Source Selection	79 days	January 9, 2007	April 27, 2007	7
9 Form Source Selection Team	5 days	January 9, 2007	January 15, 2007	
10 Evaluate Proposals	45 days	February 26, 2007	April 27, 2007	9
11 Final Selection	25 days	April 30, 2007	June 1, 2007	8
12 Award	25 days	June 4, 2007	July 6, 2007	11
13 Project kickoff	1 day?	July 9, 2007	July 9, 2007	12
14 Project Management	710 days?	July 10, 2007	March 29, 2010	13
15 Project Planning, integration and Control	650 days?	October 2, 2007	March 29, 2010	
16 Configuration Management	649 days?	October 2, 2007	March 26, 2010	
17 Quality Assurance	649 days?	October 2, 2007	March 26, 2010	
18 Risk Management	586 days?	December 28, 2007	March 26, 2010	
19 Security Management	649 days?	October 2, 2007	March 26, 2010	
20 Strategy and Architecture	199 days	July 10, 2007	April 11, 2008	
21 System Development Methodology	10 days	July 10, 2007	July 23, 2007	
22 Architecture	199 days	July 10, 2007	April 11, 2008	
23 Phase one	45 days	July 10, 2007	September 10, 2007	
24 Phase two	30 days	March 3, 2008	April 11, 2008	
25 Infrastructure Implementation	289 days?	July 10, 2007	August 15, 2008	
26 Planning	30 days?	July 10, 2007	August 20, 2007	
27 Acquisition	45 days	July 24, 2007	September 24, 2007	
28 Build	289 days?	July 10, 2007	August 15, 2008	
29 Development, Test, model office	10 days	July 10, 2007	July 23, 2007	
30 Primary site - HW/SW	100 days?	July 10, 2007	November 26, 2007	
31 Secondary site- SW/HW	75 days?	May 5, 2008	August 15, 2008	
32 Phase one - SWIFT message submission	320 days?	July 10, 2007	September 29, 2008	13
33 Data Warehouse	230 days?	July 10, 2007	May 26, 2008	
34 Planning	35 days	July 10, 2007	August 27, 2007	
35 Requirement Analysis	45 days	August 28, 2007	October 29, 2007	34
36 System Design and Development	120 days?	October 30, 2007	April 14, 2008	
37 CBWT Data Warehouse	120 days?	October 30, 2007	April 14, 2008	35
38 Query and Reporting	120 days	October 30, 2007	April 14, 2008	35
39 Unit Testing	30 days	April 15, 2008	May 26, 2008	38
40 CBWT Application	200 days	July 10, 2007	April 14, 2008	
41 Planning	30 days	July 10, 2007	August 20, 2007	
42 Requirement Analysis	45 days	August 21, 2007	October 22, 2007	41
43 System Design and Development	100 days	October 23, 2007	March 10, 2008	42
44 Unit Testing	25 days	March 11, 2008	April 14, 2008	43
45 System Test and Integration	70 days	April 15, 2008	July 21, 2008	
46 Integrate DBWT DW with CBWT application	30 days	May 27, 2008	July 7, 2008	39,44
47 Integrate CBWT DW with BSADW	40 days	May 27, 2008	July 21, 2008	39
48 Integrate CBWT with Secure Outreach	40 days	May 27, 2008	July 21, 2008	39,44
49 Integrate CBWT with BSA E-Filing	45 days	April 15, 2008	June 16, 2008	44
50 Roll out and Deploy pilot	30 days	July 22, 2008	September 1, 2008	45
51 Evaluate Pilot	20 days	September 2, 2008	September 29, 2008	50
52 Phase two - non-SWIFT message submission	541 days?	March 3, 2008	March 29, 2010	
53 Data Warehouse	275 days?	March 3, 2008	March 20, 2009	
54 Planning	30 days	March 3, 2008	April 11, 2008	
55 Requirement Analysis	75 days	April 14, 2008	July 25, 2008	54
56 Design and Development	120 days?	July 28, 2008	January 9, 2009	
57 CBWT Data Warehouse	120 days?	July 28, 2008	January 9, 2009	55
58 Query and Reporting	120 days	July 28, 2008	January 9, 2009	55
59 Portal Design and Developemnt	120 days	July 28, 2008	January 9, 2009	55
60 Unit Testing	50 days	January 12, 2009	March 20, 2009	59
61 CBWT Application	260 days	March 3, 2008	February 27, 2009	
62 Planning	30 days	March 3, 2008	April 11, 2008	
63 Requirement Analysis	60 days	April 14, 2008	July 4, 2008	62
64 Design and Development	120 days	July 7, 2008	December 19, 2008	63
65 Unit Testing	50 days	December 22, 2008	February 27, 2009	64
66 System Test and Integration	75 days	March 2, 2009	June 12, 2009	
67 Integrate CBWT DW with CBWT application	60 days	March 23, 2009	June 12, 2009	60,65
68 Integrate CBWT DW with BSADW	60 days	March 23, 2009	June 12, 2009	60
69 Integrate CBWT with Secure Outreach	60 days	March 23, 2009	June 12, 2009	60
70 Integrate CBWT with BSA E-Filing	75 days	March 2, 2009	June 12, 2009	65
71 User Acceptance Test	60 days?	June 15, 2009	September 4, 2009	66
72 Production Readiness Test	60 days	September 7, 2009	November 27, 2009	71
73 Roll-out and Deployment	271 days	March 16, 2009	March 29, 2010	
74 Training	120 days	March 16, 2009	August 28, 2009	
75 Help Desk	206 days	June 15, 2009	March 29, 2010	66
76 Roll-Out	86 days	November 30, 2009	March 29, 2010	72
77 C & A	111 days	June 1, 2009	November 2, 2009	
78 Initiation Phase	25 days	June 1, 2009	July 3, 2009	
79 Preparation	5 days	June 1, 2009	June 5, 2009	
80 Notification and Resource Identification	5 days	June 8, 2009	June 12, 2009	79
81 System Security Plan Analysis, Update and Acceptance	20 days	June 8, 2009	July 3, 2009	79
82 Security Certification Phase	60 days	July 6, 2009	September 25, 2009	78
83 ST & E Testing	15 days	July 6, 2009	July 24, 2009	
84 ST & E Report Document	15 days	July 27, 2009	August 14, 2009	83
85 Security Certification Documentation	30 days	August 17, 2009	September 25, 2009	84
86 Risk and Security Assessment Document	15 days	August 17, 2009	September 4, 2009	
87 Configuration Management Plan (CMP) Document	15 days	September 7, 2009	September 25, 2009	86
88 Contingency Plan Document	15 days	September 7, 2009	September 25, 2009	86
89 Incident Response Plan (IRP) Document	15 days	September 7, 2009	September 25, 2009	86
90 Security Awareness and Training Plan Document	15 days	September 7, 2009	September 25, 2009	86
91 Security Accreditation Phase	25 days	September 28, 2009	October 30, 2009	82
92 C & A results briefing	10 days	September 28, 2009	October 9, 2009	
93 Security Accreditation Package	15 days	October 12, 2009	October 30, 2009	92
94 Compete C & A	1 day	November 2, 2009	November 2, 2009	93

APPENDIX K – ROUGH ORDER OF MAGNITUDE COST ESTIMATES

Summary

	Acquisition	Phase One	Phase Two	Sub-Totals
Acquisition Cost				
FTE Cost	\$347,710			\$347,710
Contract Support	\$770,000			\$770,000
SubTotal	\$1,117,710			\$1,117,710
Hardware				
Server Hardware		\$1,466,397	\$1,274,397	\$2,740,794
Development Hardware		\$113,995		\$113,995
Security		\$50,000	\$50,000	\$100,000
SubTotal		\$1,630,392	\$1,324,397	\$2,954,789
Software & COTS				
Development Software		\$5,427		\$5,427
RDBMS		\$582,146	\$575,720	\$1,157,866
ETL		\$458,314		\$458,314
OLAP, Reporting		\$450,000	\$450,000	\$900,000
CM, QA, Test Manager		\$76,950		\$76,950
Firewall		\$76,928	\$76,928	\$153,856
SAN Software		\$25,250	\$25,250	\$50,500
Reference Data		\$400,000		\$400,000
Entity Extraction Tool		\$1,000,000		\$1,000,000
Others		\$100,000	\$100,000	\$200,000
SubTotal		\$3,175,015	\$1,227,898	\$4,402,913
Maintenance				
Hardware		\$67,786	\$135,572	\$203,358
Software & COTS		\$622,583	\$632,333	\$1,254,916
SubTotal		\$690,369	\$767,905	\$1,458,274
Vendor Support				
Hardware, Servers		\$100,000	\$100,000	\$200,000
Software, Tools		\$300,000	\$300,000	\$600,000
SubTotal		\$400,000	\$400,000	\$800,000
Contract Service & Support		\$5,374,797	\$12,012,392	\$17,387,189
IV & V		\$500,000	\$800,000	\$1,300,000
C & A Contract Support			\$300,000	\$300,000
FinCEN FTE		\$754,110	\$933,660	\$1,687,770
Web Hosting			\$1,200,000	\$1,200,000
Grand Totals	\$1,117,710	\$12,524,683	\$18,966,252	\$32,608,645

Labor Cost by Phase

Job Title	Phase One ¹		Phase Two ²		Total	
	Labor	Cost	Labor	Cost	Labor	Cost
Program	560	\$105,752	920	\$182,422	1,480	\$288,174
Project	2,520	\$430,398	3,120	\$559,518	5,640	\$989,916
Lead	2,520	\$740,880	2,940	\$907,578	5,460	\$1,648,458
DBA/Data	2,520	\$463,050	2,840	\$547,943	5,360	\$1,010,993
Systems	2,300	\$188,612	3,340	\$287,592	5,640	\$476,203
Lead	2,200	\$308,085	3,260	\$479,352	5,460	\$787,436
Data	2,200	\$404,250	2,960	\$571,095	5,160	\$975,345
Web	900	\$127,877	3,960	\$590,794	4,860	\$718,671
Web	900	\$96,239	3,580	\$401,957	4,480	\$498,196
Web	900	\$96,239	3,580	\$401,957	4,480	\$498,196
EAV/ETL	1,200	\$186,732	3,960	\$647,026	5,160	\$833,758
EAV/ETL	1,200	\$139,847	3,580	\$438,072	4,780	\$577,919
EAV/ETL	1,200	\$110,111	3,580	\$344,924	4,780	\$455,035
EAV/ETL	1,200	\$110,111	3,580	\$344,924	4,780	\$455,035
Business	900	\$118,125	3,980	\$548,494	4,880	\$666,619
Business	900	\$91,429	3,880	\$413,867	4,780	\$505,296
Business	900	\$87,394	3,880	\$395,602	4,780	\$482,995
Software	2,520	\$226,630	2,840	\$268,179	5,360	\$494,809
Report	1,200	\$125,118	3,910	\$428,060	5,110	\$553,178
Report	1,200	\$93,051	3,710	\$302,067	4,910	\$395,118
Usability	0	\$0	160	\$13,027	160	\$13,027
Operations	1,600	\$143,892	3,280	\$309,728	4,880	\$453,620
Operations	1,600	\$142,850	3,280	\$307,485	4,880	\$450,336
Test	900	\$68,446	3,000	\$239,562	3,900	\$308,009
Tester 1	900	\$66,443	2,800	\$217,047	3,700	\$283,490
Tester 2	900	\$66,443	2,500	\$193,792	3,400	\$260,235
Tester 3	900	\$66,443	2,500	\$193,792	3,400	\$260,235
Network	1,800	\$123,587	3,260	\$235,021	5,060	\$358,609
CM Lead	1,400	\$132,315	2,600	\$258,014	4,000	\$390,328
SQA Lead	1,400	\$132,315	2,600	\$258,014	4,000	\$390,328
Security	200	\$20,595	1,200	\$129,747	1,400	\$150,341
Help Desk	400	\$31,109	1,680	\$137,192	2,080	\$168,302
Help Desk	400	\$25,154	1,680	\$110,928	2,080	\$136,082
Tech Writer	600	\$59,352	1,780	\$184,882	2,380	\$244,235
Training	400	\$22,961	1,350	\$81,369	1,750	\$104,331
Training	400	\$22,961	1,350	\$81,369	1,750	\$104,331
Totals	43,740	\$5,374,797	102,420	\$12,012,392	146,160	\$17,387,189

Labor Cost by Fiscal Year

Job Title	Unit Price	Fiscal Year One		Fiscal Year Two		Fiscal Year Three		Fiscal Year Four		Total	
		Hours	Cost	Hours	Cost	Hours	Cost	Hours	Cost	Hours	Cost
Program	\$179.85	120	\$21,582	480	\$90,644	480	\$95,177	400	\$83,280	1,480	\$290,583
Project	\$162.66	480	\$78,077	2,080	\$355,249	2,080	\$373,012	1,000	\$188,299	5,640	\$994,637
Lead	\$280.00	480	\$134,400	2,080	\$611,520	2,080	\$642,096	820	\$265,791	5,460	\$1,653,807
DBA/Data	\$175.00	432	\$75,600	2,080	\$382,200	2,080	\$401,310	768	\$155,585	5,360	\$1,014,695
Systems	\$78.10	480	\$37,488	2,080	\$170,570	2,080	\$179,099	1,000	\$90,411	5,640	\$477,568
Lead	\$133.37	480	\$64,018	2,080	\$291,280	2,080	\$305,844	820	\$126,602	5,460	\$787,744
Data	\$175.00	480	\$84,000	2,080	\$382,200	2,080	\$401,310	520	\$105,344	5,160	\$972,854
Web	\$135.32	288	\$38,972	2,080	\$295,539	2,080	\$310,316	412	\$64,540	4,860	\$709,367
Web	\$101.84	288	\$29,330	2,080	\$222,419	1,800	\$202,101	312	\$36,782	4,480	\$490,632
Web	\$101.84	288	\$29,330	2,080	\$222,419	1,800	\$202,101	312	\$36,782	4,480	\$490,632
EA/VE/TL	\$148.20	384	\$56,909	2,080	\$323,669	2,080	\$339,852	616	\$105,681	5,160	\$826,111
EA/VE/TL	\$110.99	384	\$42,620	2,080	\$242,402	1,900	\$232,496	416	\$53,450	4,780	\$570,968
EA/VE/TL	\$87.39	384	\$33,558	2,080	\$190,860	1,900	\$183,060	416	\$42,085	4,780	\$449,562
EA/VE/TL	\$87.39	384	\$33,558	2,080	\$190,860	1,900	\$183,060	416	\$42,085	4,780	\$449,562
Business	\$125.00	384	\$48,000	2,080	\$273,000	1,900	\$261,844	516	\$74,667	4,880	\$657,511
Business	\$96.75	384	\$37,152	2,080	\$211,302	1,900	\$202,667	516	\$57,792	4,880	\$508,913
Business	\$92.48	384	\$35,512	2,080	\$201,976	1,900	\$193,722	416	\$44,536	4,780	\$475,747
Software	\$85.65	480	\$41,112	2,080	\$187,060	2,080	\$196,413	720	\$71,388	5,360	\$495,973
Report	\$99.30	360	\$35,748	2,080	\$216,871	2,080	\$227,715	590	\$67,822	5,110	\$548,156
Report	\$73.85	360	\$26,586	2,080	\$161,288	2,080	\$169,353	390	\$33,341	4,910	\$390,569
Usability	\$73.85	0	\$0	80	\$6,203	80	\$6,514	0	\$0	160	\$12,717
Operations	\$85.65	350	\$29,978	1,600	\$143,892	2,080	\$196,413	850	\$84,278	4,880	\$454,560
Operations	\$85.03	350	\$29,761	1,600	\$142,850	2,080	\$194,991	850	\$83,668	4,880	\$451,270
Test	\$72.43	96	\$6,953	1,600	\$121,682	2,000	\$159,708	204	\$17,105	3,900	\$305,449
Tester 1	\$70.31	0	\$0	1,600	\$118,121	1,800	\$139,530	300	\$24,418	3,700	\$282,069
Tester 2	\$70.31	0	\$0	1,600	\$118,121	1,800	\$139,530	0	\$0	3,400	\$257,651
Tester 3	\$70.31	0	\$0	1,600	\$118,121	1,800	\$139,530	0	\$0	3,400	\$257,651
Network	\$65.39	336	\$21,971	1,800	\$123,587	2,080	\$149,952	844	\$63,888	5,060	\$359,399
CM Lead	\$90.01	336	\$30,243	1,600	\$151,217	1,600	\$158,778	464	\$48,348	4,000	\$388,586
SQA Lead	\$90.01	336	\$30,243	1,600	\$151,217	1,600	\$158,778	464	\$48,348	4,000	\$388,586
Security	\$98.07	48	\$4,707	400	\$41,199	800	\$86,498	152	\$17,256	1,400	\$149,651
Help Desk	\$74.07	0	\$0	444	\$34,531	800	\$65,330	480	\$41,158	1,724	\$141,019
Help Desk	\$59.89	0	\$0	800	\$50,308	800	\$52,823	480	\$33,278	2,080	\$136,409
Tech Writer	\$94.21	144	\$13,566	1,000	\$98,921	1,000	\$103,867	236	\$25,738	2,380	\$242,091
Training	\$54.67	0	\$0	550	\$31,572	1,000	\$60,274	200	\$12,657	1,750	\$104,503
Training	\$54.67	0	\$0	550	\$31,572	1,000	\$60,274	200	\$12,657	1,750	\$104,503
Totals		9,700	\$1,150,974	58,424	\$6,706,432	60,680	\$7,175,336	17,100	\$2,259,059	145,904	\$17,291,802

Labor Cost by Calendar Year

Unit Price	Year One ¹		Year Two ²		Year Three ³		Year Four ⁴		Total	
	Hours	Cost	Hours	Cost	Hours	Cost	Hours	Cost	Hours	Cost
\$179.85	300	\$53,955	480	\$90,644	480	\$95,177	220	\$45,804	1,480	\$285,580
\$162.66	1,000	\$162,660	2,080	\$355,249	2,080	\$373,012	480	\$90,384	5,640	\$981,305
\$280.00	1,000	\$280,000	2,080	\$611,520	2,080	\$642,096	300	\$97,241	5,460	\$1,630,857
\$175.00	900	\$157,500	2,080	\$382,200	2,080	\$401,310	300	\$60,775	5,360	\$1,001,785
\$78.10	1,000	\$78,100	2,080	\$170,570	2,080	\$179,099	480	\$43,397	5,640	\$471,166
\$133.37	1,000	\$133,370	2,080	\$291,280	2,080	\$305,844	300	\$46,318	5,460	\$776,812
\$175.00	1,000	\$175,000	2,080	\$382,200	2,080	\$401,310	0	\$0	5,160	\$958,510
\$135.32	600	\$81,192	2,080	\$295,539	2,080	\$310,316	100	\$15,665	4,860	\$702,712
\$101.84	600	\$61,104	2,080	\$222,419	1,800	\$202,101	0	\$0	4,480	\$485,624
\$101.84	600	\$61,104	2,080	\$222,419	1,800	\$202,101	0	\$0	4,480	\$485,624
\$148.20	800	\$118,560	2,080	\$323,669	2,080	\$339,852	200	\$34,312	5,160	\$816,393
\$110.99	800	\$88,792	2,080	\$242,402	1,900	\$232,496	0	\$0	4,780	\$563,690
\$87.39	800	\$69,912	2,080	\$190,860	1,900	\$183,060	0	\$0	4,780	\$443,832
\$87.39	800	\$69,912	2,080	\$190,860	1,900	\$183,060	0	\$0	4,780	\$443,832
\$125.00	800	\$100,000	2,080	\$273,000	1,900	\$261,844	100	\$14,470	4,880	\$649,314
\$96.75	800	\$77,400	2,080	\$211,302	1,900	\$202,667	100	\$11,200	4,880	\$502,569
\$92.48	800	\$73,984	2,080	\$201,976	1,900	\$193,722	0	\$0	4,780	\$469,683
\$85.65	1,000	\$85,650	2,080	\$187,060	2,080	\$196,413	200	\$19,830	5,360	\$488,952
\$99.30	750	\$74,475	2,080	\$216,871	2,080	\$227,715	200	\$22,990	5,110	\$542,051
\$73.85	750	\$55,388	2,080	\$161,288	2,080	\$169,353	0	\$0	4,910	\$386,029
\$73.85	0	\$0	80	\$6,203	80	\$6,514	0	\$0	160	\$12,717
\$85.65	720	\$61,668	1,600	\$143,892	2,080	\$196,413	480	\$47,592	4,880	\$449,565
\$85.03	720	\$61,222	1,600	\$142,850	2,080	\$194,991	480	\$47,248	4,880	\$446,311
\$72.43	200	\$14,486	1,400	\$106,472	2,000	\$159,708	300	\$25,154	3,900	\$305,820
\$70.31	200	\$14,062	1,400	\$103,356	1,800	\$139,530	300	\$24,418	3,700	\$281,366
\$70.31	200	\$14,062	1,400	\$103,356	1,800	\$139,530	0	\$0	3,400	\$256,948
\$70.31	200	\$14,062	1,400	\$103,356	1,800	\$139,530	0	\$0	3,400	\$256,948
\$65.39	700	\$45,773	1,800	\$123,587	2,080	\$149,952	480	\$36,335	5,060	\$355,647
\$90.01	700	\$63,007	1,600	\$151,217	1,600	\$158,778	100	\$10,420	4,000	\$383,421
\$90.01	700	\$63,007	1,600	\$151,217	1,600	\$158,778	100	\$10,420	4,000	\$383,421
\$98.07	100	\$9,807	400	\$41,189	800	\$86,498	100	\$11,353	1,400	\$148,847
\$74.07	0	\$0	800	\$62,219	800	\$65,330	480	\$41,158	2,080	\$168,706
\$59.89	0	\$0	800	\$50,308	800	\$52,823	480	\$33,278	2,080	\$136,409
\$94.21	300	\$28,263	1,000	\$98,921	1,000	\$103,867	80	\$8,725	2,380	\$239,775
\$54.67	150	\$8,201	400	\$22,961	1,000	\$60,274	200	\$12,657	1,750	\$104,093
\$54.67	150	\$8,201	400	\$22,961	1,000	\$60,274	200	\$12,657	1,750	\$104,093
	21,140	\$2,463,877	57,680	\$6,657,393	60,680	\$7,175,336	6,760	\$823,801	146,260	\$17,120,407

Acquisition Costs

Salary				Hourly Costs		
	Base		Fully Loaded	Work Hours	Fully Loaded	Base
Full Loaded GS-14 Daily Rate:	\$91,407	32.00%	\$179,942.00		\$95.71	\$57.81
Hours	2,087			1,880		
Full Loaded GS-15 Daily Rate:	\$107,521		\$202,767.00		\$107.85	\$68.01
Acquisition Planning		Hours	FTE Cost	Contract Administration	Grand Totals	
GS-15		160	\$17,257		\$17,257	
GS-14	2	80	\$15,314		\$15,314	
SubTotal			\$32,571		\$32,571	
Develop SOW						
GS-15		320	\$34,514		\$34,514	
GS-14	2	320	\$61,257		\$61,257	
Contract Support				\$425,000	\$425,000	
SubTotal			\$95,770	\$425,000	\$520,770	
Source Selection						
GS-15	3	320	\$103,541		\$103,541	
GS-14	3	320	\$91,885		\$91,885	
Contract Support				\$230,000	\$230,000	
SubTotal			\$195,426	\$230,000	\$425,426	
Award						
GS-15		80	\$8,628		\$8,628	
GS-14	2	80	\$15,314		\$15,314	
Contract Support				\$115,000	\$115,000	
SubTotal			\$23,943	\$115,000	\$138,943	
Totals			\$347,710	\$770,000	\$1,117,710	

Hardware Costs

Function	Vendor	Unit Cost	Develop & Test		Phase One	
			Quantity	Cost	Quantity	Cost
Load Balancer	F5 BIG IP	\$11,585			2	\$23,170
Web Server	Sun V490	\$40,995			2	\$81,990
Application Server	Sun V490	\$40,995			2	\$81,990
Database Server	Sun V490	\$40,995			2	\$81,990
Portal Server	SUN V490	\$40,995			1	\$40,995
OLAP Server	SUN V490	\$40,995			2	\$81,990
CoronetDirect Server	Sun V490	\$40,995			2	\$81,990
Dell Server - Site 1						\$56,000
Dell Server - Site 2						
Firewall	Cisco PIX	\$7,000			4	\$28,000
Admin Server	SUN V240	\$4,250			2	\$8,500
SAN Device	Sun 6920	\$287,200			1	\$287,200
Backup & Restore (BAR)		\$203,200			1	\$203,200
Cisco 6503 Switches		\$29,691			2	\$59,382
SUN Shared SAN						\$150,000
Miscellaneous						\$200,000
SubTotal						\$1,466,397
Maintenance						
Sun Servers	4%					\$29,866
Dell Servers	30%					\$16,800
Firewall						\$1,120
Miscellaneous	10%					\$20,000
SubTotal						\$67,786
Development environment						
RDBMS Server	Sun V490	\$40,995	1	\$40,995		
Portal Server	SUN V240	\$4,250	1	\$4,250		
Web Server	SUN V240	\$4,250	1	\$4,250		
Application Server	SUN V240	\$4,250	1	\$4,250		
OLAP Server	SUN V240	\$4,250	1	\$4,250		
CM Server	Dell	\$11,500	1	\$11,500		
QA Server	Dell	\$11,500	1	\$11,500		
Test Manager Server	Dell	\$11,500	1	\$11,500		
Network Server	Dell	\$11,500	1	\$11,500		
Miscellaneous				\$10,000		
SubTotal				\$113,995		
Maintenance						
Sun Servers	4%					
Dell Servers	30%					
Other	10%					
SubTotal						
Software						
Oracle - 16 CPU						\$575,720
Oracle - 10 Licenses		\$543	10	\$5,427		
ETL						\$458,314
OLAP, Reporting Tool						\$450,000
MS 2003 Server						\$14,200
Rational Suite(CM, RM, Test)		\$7,695			10	\$76,950
Firewall Unlimited License		\$19,232			4	\$76,928
MS Project						
SAN Software						\$25,250
Entity Extraction Tool						\$1,000,000
Reference Data						\$400,000
SubTotal				\$5,427		\$3,077,362
Maintenance						
SAN Software Maintenance						
RDBMS	15%					\$86,358
ETL	20%					\$87,172
OLAP, Reporting Tool						\$91,663
Rational Suite (CM, RM, Test)						\$90,000
Firewall Unlimited License						\$15,390
Reference Data	18%					\$72,000
Entity Extraction Tool						\$180,000
SubTotal						\$622,583
IV & V cost						\$500,000
Vendor Support						\$300,000
Web Hosting						
Government FTE						
PM & CQTR	GS-15	\$58			2,520	\$171,385
Requirement	GS-14	\$58			2,520	\$145,681
ISSO	GS-14	\$58			2,520	\$145,681
System Integrator	GS-14	\$58			2,520	\$145,681
Project Administrator	GS-14	\$58			2,520	\$145,681
SubTotal					12,600	\$754,110
Total				\$119,422		\$6,788,238

APPENDIX L – PROJECT MANAGEMENT AND INFORMATION TECHNOLOGY PROCESSES

FinCEN is an agency whose mission is dependent on the effective collection, dissemination, and meaningful analysis of large quantities of data. As such, FinCEN must manage its information technology effectively in order to ensure the most effective use of the data. To properly position itself to implement and deploy a system like the one contemplated in the Intelligence Reform and Terrorism Prevention Act of 2004, FinCEN would have to: (1) fully define its overall enterprise architecture (a blueprint for its current and future information technology environment); (2) employ a life cycle management technique to govern all aspects of individual information technology projects; (3) establish clear procedures for a technical investment review board to ensure management control of information technology projects and ensure consistency of such projects with both its overall enterprise architecture and OMB's requirements for sound capital planning investment control.

Enterprise Architecture Issues

Whether or not FinCEN implements a cross-border funds transfer reporting system, FinCEN will continue to develop a comprehensive enterprise architecture, or a blueprint for its current and future technology environment. The enterprise architecture will include documentation of FinCEN's information technology development methodology, in order to ensure that every project within FinCEN is managed according to the same set of guidelines. Implementation of an enterprise architecture significantly minimizes the risk of investing in duplicative or poorly integrated technology.

Under Treasury Department guidance, FinCEN is currently completing its enterprise architecture. The final form of FinCEN's enterprise architecture must provide the basis for the final decisions FinCEN makes in developing the cross border electronic funds transfer system.

FinCEN began this effort by completing the "As Is" phase of the Enterprise Architecture in 2003. According to the Treasury Enterprise Architecture Framework (TEAF), Enterprise Architecture is "a strategic information asset base, which defines the agency's mission and business activities supporting the mission, the information necessary for agency operations, the technologies necessary to support operations and the transitional processes necessary for implementing new technologies in response to changing business needs. An enterprise architecture is an integrated model or representation."

FinCEN recognizes this as stated in the “As Is” Enterprise Architecture documentation: “Data is a crucial FinCEN resource. It has real and measurable value; and does not belong to a particular business unit or individual. Data must be carefully managed to ensure it is accurate, current, available, and properly protected across FinCEN functions and organization and with supported external organizations. An enterprise data architecture is needed to ensure the information ownership is vested in FinCEN as a whole.”

Life Cycle Management Policy

A life cycle management policy governs all aspects of an information technology project, including planning, acquisition, development, testing, operations, and maintenance. As a result, a life cycle management policy provides the framework for standardized, repeatable, and sustainable processes and best practices within the agency for developing information technology systems. Implementation of such a policy also enhances guidance for information technology projects, leverages existing technology, builds institutional knowledge, and ensures that development is consistent with industry- and government-wide best practices.

A life cycle management policy defines phases of the life cycle through which project managers seek senior management review and approval for each progressive step in the development and deployment of a project. This approach provides a framework for ensuring compliance of a given project with the overall enterprise architecture of the agency. The management review at the various stages is based on detailed analysis of the steps taken to accomplish a specific phase and the impact those steps have on the project and the overall information technology environment. The need to obtain management approval necessitates the development of detailed documentation throughout the progressive stages of a project. Life cycle management also ensures that management oversight is applied at important junctures in the progress of a technology project and that agency management adequately supports the project.

FinCEN includes within its life cycle management policy each of the steps required by the Privacy Act, FISMA, the E-Government Act of 2002, and OMB Circular A-11,⁸⁵ including (1) publication of notice of the development of new systems of records; (2) risk assessment to identify potential vulnerabilities in the planned system architecture and development of countermeasures; (3) development of a security plan for the system; (4) certification and accreditation by management; (5) a response and contingency plan for any compromise of the security or operation of the system; (6) regular testing and evaluation of the system during development and throughout the life of the system; and (7) steps taken to ensure the quality and accuracy of the data contained in the system.

85 See http://www.whitehouse.gov/omb/circulars/a11/2002/may03_memo76.pdf

Technical Investment Review Board

In 2005, FinCEN established its Technical Investment Review Board in order to meet the demands of managing its IT investment portfolio and providing a concentrated level of executive oversight for a growing array of IT management issues. A technical investment review board functions as the management review and approval mechanism at identified phases of an information technology project. At each phase of the project, the project manager prepares documentation related to the project development and presents the relevant information to the board. Review by the board ensures that the project is progressing consistently with the enterprise architecture established by the agency and life cycle management policy. In addition, the close review by management within the agency ensures that the project receives adequate support from a fully informed management structure.

Quality Assurance/Risk Management

All IT projects, regardless of size or scope, entail some level of risk. The key to effective project management is to properly identify and mitigate those risks that threaten the successful outcome of the project. An essential tool in this aspect of an IT project is the risk management plan, a document that establishes the procedures employed to manage risk at all stages of a project. A well-developed risk management plan documents the standard approach the agency takes to risk identification and management and the roles and responsibilities of the members of the project team and contractors. A risk management plan also provides for the tracking and documentation of risks and contingency plans throughout the life of the project.

The project manager is ultimately responsible for reviewing the identified risks and managing the overall response.

Project Management

Project Management Team

To implement the proposed reporting system, FinCEN would establish a project management team specifically dedicated to the development and implementation of this project. A well functioning project management team can significantly reduce the risks that threaten successful implementation of an information technology project. The project management team should be directly responsible for all program execution tasks, including: (1) cost, schedule, and performance oversight; (2) life cycle project reviews; (3) award fee evaluations; (4) primary review and acceptance of contractor documentation; (5) requirements analysis and risk management; and (6) project budget and financial management.

A project management team must be fully staffed with sufficiently skilled employees, stable, and capable of monitoring and managing the project on a daily basis. The objective in staffing the project management office should be

to form an integrated team of subject matter experts to maximize the oversight of the project. The staff of the project management team should be dedicated entirely to the management of this particular project and insulated from other duties that might detract from the time and attention they can give to the effort.

The project management team should be comprised of the project manager, administrative support, systems engineers including a database administrator and network engineer, technical assistance personnel including security experts, budget personnel, a government contracting specialist, and subject matter experts from within FinCEN or from other government agencies and contractors. It is critical that the project management team have stable leadership. The project manager must have sufficient experience, training, and certification in project management.

Project Management Office

FinCEN is currently working to establish an umbrella Project Management Office (PMO) within the Bureau. We have prepared an internal preliminary assessment report of the Strategic Project Office with Plan of Action and Milestones (POA &M) with the goal of implementing the Office in fiscal year 2007. The concept proposes to centralize project management throughout the bureau. FinCEN's PMO will control and oversee projects and initiatives as well as monitor their success.

We also have commenced initial recruitment efforts to staff the PMO in the fourth quarter of fiscal year 2006. The Senior Project Management Officer will provide guidance and oversight to all projects within FinCEN. The Senior Project Management Officer will possess experience in government programs, training in project management principles and certification in project management. A Contract Consultant will give project support to establish the PMO and prepare a report with a detailed action plan and supporting milestones to achieve implementation beginning September 30, 2006. Short-term initiatives for the PMO will afford existing staff Basic Project Management training.

The outline of the potential Strategic PMO will encompass a team support structure of:

- PMO Manager/Director (Assistant Director)
- Program Manager (groups of projects)
- Project Manager
- Project Administrator
- Project Scheduler

The PMO will provide a structure to standardize project management practices, facilitate IT project portfolio management, provide project planning tools and methods, and perform review and analysis of projects. The PMO can incorporate a view of all projects and help manage cross project resources and dependencies. Additionally, since FinCEN has engaged external service providers to outsource most of its application development and operations and maintenance work, the PMO should include processes for vendor acquisition and management.

Departmental and External Oversight

FinCEN participates in regular reviews of its IT investments as part of the Treasury Department's capital planning investment control (CPIC) process. These formal reviews occur on a quarterly basis in which schedule and cost variances data is reported and assessed as part of the Department's portfolio management approach. The Department has assigned a desk officer to work with FinCEN's project management staff in order to facilitate an understanding of the requirements that OMB has levied on the agencies and bureaus in the management of major and non-major IT investments. FinCEN submitted an exhibit 300 business case for the Cross Border Electronic Funds Transfer project to OMB for the FY 2007 budget cycle.

Acquisition Planning and Control

In keeping with OMB's iterative process described in its Capital Programming Guide, FinCEN will form an integrated project team during the planning phase of the project. The Integrated Project Team, or IPT, brings together program officials, IT managers, budget, and procurement officials in order to effectively plan and orchestrate each stage of a complex project such as the subject of this report. The IPT will play a major role in the pre-solicitation phase in developing the statement of work, the release of the RFP, and the evaluation of vendor responses.

Earned Value Management

The standard (and required) approach to evaluating progress and analyzing schedule and performance measures is to apply "earned value management" (EVM) principles in monitoring a project. EVM enables a project manager to track and report progress in a project and compare actual performance to initial baselines. Simply put, EVM provides a disciplined method of ensuring accountability for a project and identifying potential risks to success while there is still an opportunity to take corrective action.

In a memorandum dated August 4, 2005, the Office of Management and Budget required federal Chief Information Officers to manage and measure all information technology projects to within 10 percent variations from the project's baseline goals by applying EVM principles to tracking the project. OMB required each agency to develop agency policies for full implementation of EVM

for information technology projects by December 31, 2005. FinCEN is adhering to the Treasury Department's Earned Value Management Guideline in the management of all of its IT investments. Furthermore, any potential contractor for this project will be required to adhere to an EVM system that is compliant with ANSI/EIA STD -748.⁸⁶

⁸⁶ See <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-23.pdf>

APPENDIX M – ACRONYMS

ACS – Australian Customs Service
AFMLS - Asset Forfeiture and Money Laundering Section, Department of Justice
AFP – Australian Federal Police
ATO – Australian Taxation Office
AUSTRAC – Australian Transaction Reports and Analysis Centre
CBP - Customs and Border Protection, Department of Homeland Security
CSIS – Canadian Security Intelligence Service
DEA - Drug Enforcement Administration, Department of Justice
DHS – Department of Homeland Security
FBI - Federal Bureau of Investigation, Department of Justice
FDIC - Federal Deposit Insurance Corporation
FinCEN - Financial Crimes Enforcement Network, Department of the Treasury
FINTRAC – Financial Transaction Reports and Analysis Centre
HIDTA - High Intensity Drug Trafficking Area
HUD – U.S. Department of Housing and Urban Development
ICE - Bureau of Immigration and Customs Enforcement, Department of Homeland Security
IDW – Investigative Data Warehouse, Federal Bureau of Investigation
IRS - Internal Revenue Service, Department of the Treasury
IRS-CI - Internal Revenue Service - Criminal Investigations,
IRS-SBSE – Internal Revenue Service – Small Business/Self-Employed
JTTF – Joint Terrorism Task Force
NCUA - National Credit Union Administration
OCC - Office of the Comptroller of the Currency, Department of the Treasury
OCDETF - Organized Crime Drug Enforcement Task Force
OIG – Office of Inspector General
ONDCP - Office of National Drug Control Policy
OTS - Office of Thrift Supervision, Department of the Treasury
RCMP – Royal Canadian Mounted Police
TFOS - Terrorism Financing Operations Section, Federal Bureau of Investigation
TTIC - Terrorist Threat Integration Center
SEC - United States Securities and Exchange Commission
USDA – U.S. Department of Agriculture
USSS - United States Secret Service, Department of Homeland Security

U.S. Statutes, Laws, and Reports

BSA - Bank Secrecy Act
C.F.R. - Code of Federal Regulations
UCC - Uniform Commercial Code
U.S.C. - United States Code

Organizations and Related Terms

ABA - American Bankers Association
APEC - Asia Pacific Economic Cooperation
APG - Asia Pacific Group on Money Laundering
BSAAG - Bank Secrecy Act Advisory Group
FATF - Financial Action Task Force on Money Laundering
FIU - Financial Intelligence Unit
GCC - Gulf Cooperation Council
ICBA - Independent Community Bankers Association
IMF - International Monetary Fund
OAS - Organization of American States
OECD - Organization for Economic Cooperation and Development
SWIFT - Society for Worldwide Interbank Financial Telecommunications

General Terminology

ADP - Automatic Data Processing
AML - Anti-Money Laundering
BIC - Bank Identification Code
BMPE - Black Market Peso Exchange
EFT – Electronic Funds Transfer Report (Canada)
EDI - Electronic Data Interchange
GIS – Geographic Information Systems
GTO - Geographic Targeting Order
IFTI – International Funds Transfer Instruction Report (Australia)
LCTR – Large Currency Transaction Report (Australia and Canada)
STR – Suspicious Transaction Report (Australia and Canada)
MOU - Memorandum of Understanding
MSB - Money Services Business

BSA Forms

CMIR - Report of International Transportation of Currency or Monetary Instruments
CTR - Currency Transaction Report
CTRC - Currency Transaction Report by Casinos
CTRC-N - Currency Transaction Report by Casinos - Nevada
FBAR - Foreign Bank Account Report
SAR - Suspicious Activity Report
SAR-C - Suspicious Activity Report for Casinos and Card Clubs
SAR-SF - Suspicious Activity Report by Securities and Futures Industries
SAR-MSB - Suspicious Activity Report for Money Services Businesses

