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 Group[6] 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.