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 charaters 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.

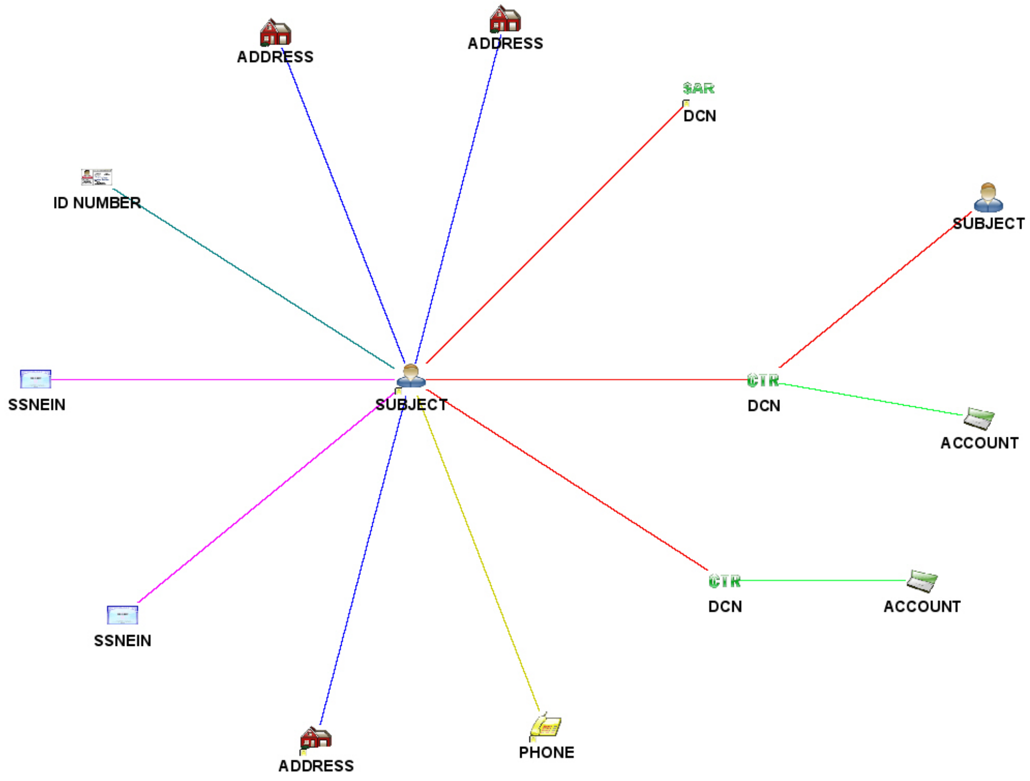
there are many differences between them, there are also many fields common to the various reports. Likewise, even the limited pieces of data necessary to a funds transfer message overlap some of the information collected in these reports. Link analysis looks for matching fields in each of these records. 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.

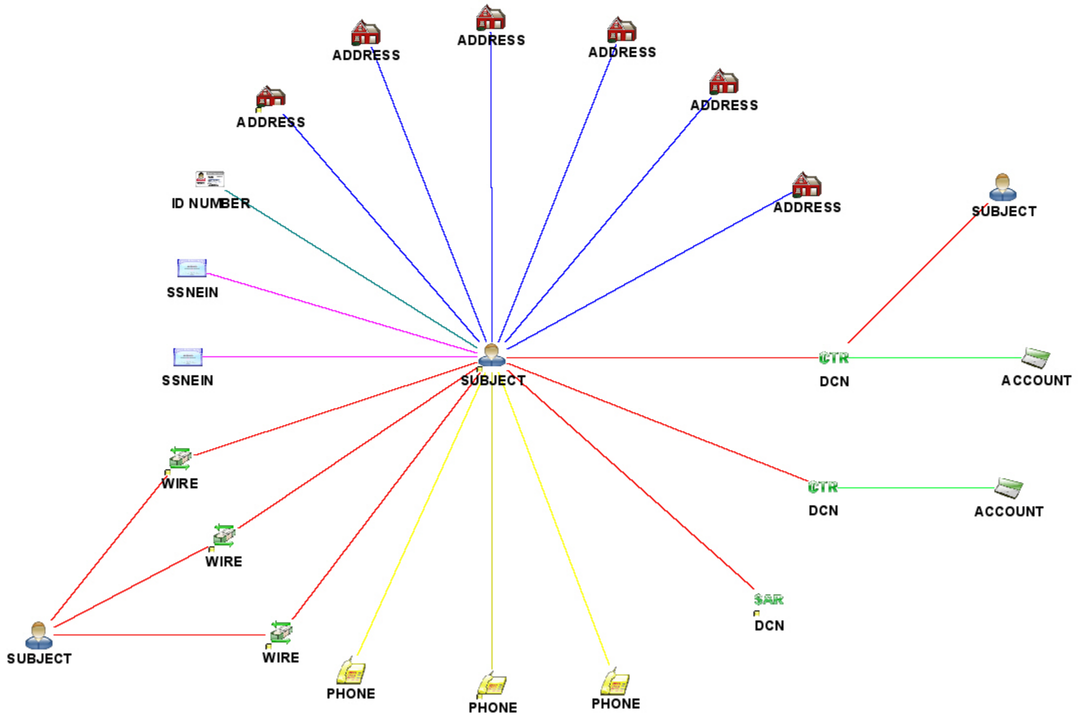
FinCEN analysts use visualization software tools to develop a comprehensive and graphical representation of the link analysis results. The visualization tools assist the user in interpreting, identifying, and analyzing relationships from data by providing a visual mechanism that reflects relationships. 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.

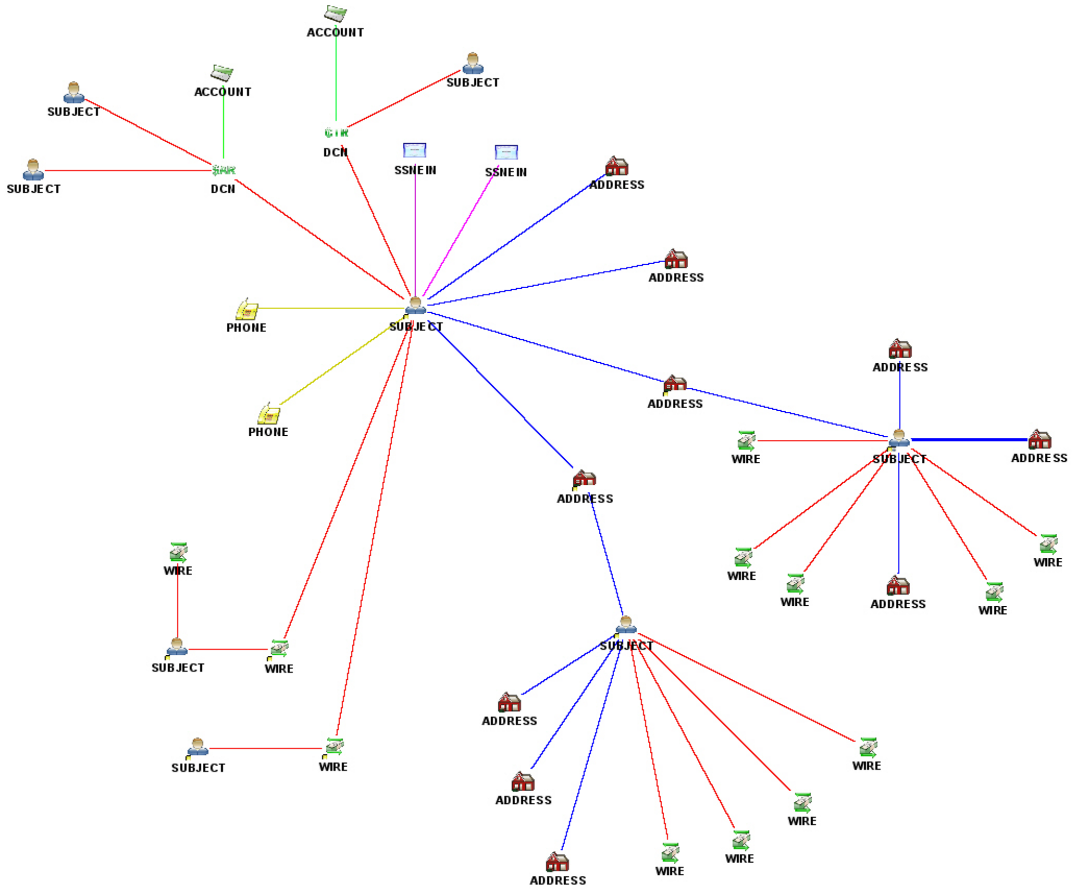


The addition of another set of data for the link analysis provides a richer context for the analysis, and a broader set of data containing potential links. Building upon the example illustrated above by adding electronic funds transfer data results in a far more detailed picture. The funds transfer data 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 identify[69] 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 records[71] from financial institutions[72] (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 institutions[74] 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 Staes." 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 Secrect 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 RFPA, 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 RFPA 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.