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.