FEDERAL AGENCY DATA MINING REPORT *(2009)*

Department of the Treasury
January 2010

REPORT TO CONGRESS ON DATA MINING ACTIVITIES WITHIN THE DEPARTMENT OF THE TREASURY

The Department of the Treasury is pleased to provide to the Congress its 2009 report to comply with the *Federal Agency Data Mining Reporting Act of 2007.* As required, this is an update to the Department of the Treasury's 2007 data mining activities.[1] This report provides activities currently deployed in the Department that meet the Act's definition of data mining, and provides the information set out in the Act's reporting requirements for data mining programs. For purposes of this report, data mining activities are defined as pattern-based queries, searches, or analyses of one or more electronic databases to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activities. The report, therefore, does not include "subject-based" query and analysis activities that use personal identifiers or inputs associated with a specific individual or group of individuals, to retrieve information from the database(s).

Two bureaus of the Department of the Treasury are engaged in data mining activities: the Internal Revenue Service (IRS) and the Financial Crimes Enforcement Network (FinCEN). The IRS conducts data mining activities by using two internal software programs and one commercial off-the-shelf product: 1) *Reveal*, 2) *Web Currency and Banking Retrieval System*, and 3) the Electronic Fraud Detection System *Clementine*, respectively. The IRS data mining programs focus on the identification of financial crimes including tax fraud, money laundering, terrorism, and offshore abusive trust schemes. IRS maintains the pursuit of these pattern-based searches to identify potential criminal activity. FinCEN's data mining activities focus on money laundering activities and other financial crimes.

[1] Section 804 of Title VIII, Privacy and Civil Liberties, Public Law 110–53, 121 STAT. 363, requires that the head of each department or agency of the Federal Government that is engaged in any activity to use or develop data mining shall submit a report to Congress on all such activities of the department or agency under the jurisdiction of that official.

TABLE OF CONTENTS

1.0 INTERNAL REVENUE SERVICE (IRS) 3

2.0 FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN) 8

1.0 INTERNAL REVENUE SERVICE (IRS)

A. Data mining activity, goals, and target dates for the deployment of data mining activity, where appropriate

The Internal Revenue Service–Criminal Investigation (IRS-CI) organization uses three software programs that can perform sophisticated search and analytical tasks: *Reveal, Web Currency & Banking Retrieval System (Web-CBRS) and Electronic Fraud Detection System (EFDS).* These programs can be used to perform data mining activities by searching databases of internal and external information. IRS-CI uses these software applications to search for specific characteristics that have been identified as potential indicators of criminal activity.

Reveal is a data query and visualization tool that provides CI analysts and agents with the capability to query and analyze large and potentially disparate sets of data through a single access point, enhancing the user's ability to develop a unified overall picture of suspicious or criminal activity. Information is presented to the user visually, exposing associations between entities in the data that might otherwise remain undiscovered. Visualization diagrams are built by the VisuaLinks tool and are based on the data queried. The analyst is not required to manually construct the link analysis charts. The system is used in IRS-CI Lead Development Centers, Fraud Detection Centers (FDC), and field offices to identify and develop leads in the areas of counterterrorism, money laundering, offshore abusive trust schemes, and other financial crime.

Web-CBRS is a web-based application that accesses a database containing Bank Secrecy Act (BSA) forms and information. IRS-CI accesses the database for research in tax cases, tracking money-laundering activities, investigative leads, intelligence for the tracking of currency flows, corroborating information, and probative evidence.

EFDS is an automated system designed to maximize fraud detection at the time that tax returns are filed to reduce the issuing of questionable refunds. All data items compiled by the *EFDS* are used to cross-reference and verify information that relates to potentially fraudulent tax returns. *EFDS* is leveraged by the Wage & Investment unit and uses a commercial off-the-shelf software product known as *Clementine* to determine data mining scores. This program runs during the nightly load process and assigns a probability factor score to each refund return. These scores range from 0-1; the higher the score, the higher the potential for fraud on that return.

B. Data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity

With *Reveal* and *Web-CBRS*, IRS-CI does not have any specific artificial intelligence capabilities to search for indicators of terrorist or criminal activity. Special agents and investigative analysts have developed "canned queries" based on their experiences. These queries can be as simple as searching for individuals that have had five or more Suspicious Activity Reports (SAR) filed on them by financial institutions in a six month

period using the *Reveal* database. The fraudulent behavior is determined from previous successful investigations of money laundering, counterterrorism, and BSA violations.

Accepted Electronic Filing System (ELF) returns are received via ELF 1001 and loaded into *EFDS* daily. Returns meeting refund and data mining score tolerances are placed into the *EFDS* Prescan queue which allows our Wage and Investment and Scheme Development Center employees to view these returns for suspicious activities. With the implementation of data mining for paper returns, EFDS generates a Return Charge-Out that is sent to Files at the paper processing sites to pull the actual paper tax return which is also viewed for suspicious activities.

Each Fraud Detection Center (FDC) inventory is determined by state code/zip code assignments. If a tax return meets the data mining tolerance and the refund amount tolerance, it is assigned a value and placed into inventory of the FDC assigned to that specific state.

C. Data sources that are being or will be used

a. **IRS**: Third Party Data Store (TPDS); Business Master File (BMF); Individual Master File (IMF); Information Returns Master File (IRMF) and Questionable Refund Program (QRP).
b. **Taxpayer**: The source is the electronically/paper filed return.
c. **Employee**: Source of employee information is the Online 5081.
d. **Other Federal agencies**: Federal Bureau of Prisons; Bank Secrecy Act data.
e. **State and local agencies**: All state and the District of Columbia prisons deliver prisoner listing information annually to CI in electronic format.
f. **Other third party sources**: Commercial public business telephone directory listings/databases are purchased by CI to contact employers for employment and wage information, *e.g., Accurint.*

D. Assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with, and valuable to, the stated goals and plans for the use or development of the data mining activity

The data uncovered during the query searches is only a lead and requires additional investigative steps be taken to verify the quality of the information. There is no empirical data on the efficacy of these searches.

Statistics provided throughout the filing season outline the fraud trends and increases in fraud detection, which may be used in the development of future data mining activity.

E. Assessment of the impact, or likely impact, of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are or will be taken with regard to the property, privacy, or other rights or privileges of any individual as a result of implementing the data mining activity

IRS-CI is tasked to protect IRS revenue streams by detecting current fraudulent activity and preventing future recurrences. Results of data uncovered using these systems may

be reflected in indictments and criminal prosecutions, the same as other information uncovered during the investigative process. Once fraud is determined, laws and administrative procedures, policies and controls, govern the ensuing actions. Except for a few periods in our history, tax information generally has not been available to the public – its disclosure has been restricted. Before 1977, tax information was considered a "public record." Tax information was only open to inspection under Treasury regulations approved by the President or under Presidential Order. Under this approach, the rules regarding disclosure were essentially left to the Executive Branch.

By the mid-1970's, there was increased Congressional and public concern about the widespread use of tax information by government agencies for purposes unrelated to tax administration. This concern culminated with a complete revision of Section 6103 in the *Tax Reform Act of 1976*. Congress eliminated Executive discretion regarding what information could be disclosed to which Federal and state agencies and established a new statutory approach that treated tax information as confidential and not subject to disclosure except to the extent explicitly provided by the Code. In each area of allowable disclosure, Congress attempted to balance the specific agency or office's need for the information with the citizen's right to privacy, as well as the impact of the disclosure upon the continuation of compliance with the voluntary tax assessment system. Further, Congress undertook direct responsibility for determining the types and manner of permissible disclosures.

Although there have been many amendments to the law since that time, the basic statutory approach established in 1976 remains in place today. Congress recognized that the IRS had more information about citizens than any other Federal agency and that other agencies routinely sought access to that information. Congress also recognized that citizens reasonably expected that the tax information they were required to provide to the IRS would be private. If the IRS abused that reasonable expectation of privacy, the loss of public confidence could seriously impair the tax system. There are four basic parts to this statutory approach:

- The general rule that makes tax returns and tax return information confidential except as expressly authorized in the tax code;
- The exceptions to the general rule detailing permissible disclosures. Disclosures for purposes other than tax administration are more limited than disclosures for purposes of tax administration. This is consistent with the policy underlying Section 6103 which is that the need for a particular item of tax information must be balanced against the taxpayer's reasonable expectation of privacy in information provided to the IRS as well as the effect on continued compliance with our voluntary system of self-assessment;
- Technical, administrative, and physical safeguard provisions to prevent the recipients of tax information from using or disclosing the information in an unauthorized manner, and accounting, recordkeeping and reporting requirements that detail what disclosures are made for what purposes to assist in Congressional oversight; and
- Criminal penalties including a: (1) felony for the willful unauthorized disclosure of tax information, (2) misdemeanor for the unauthorized inspection of tax information,

and (3) civil cause of action for the taxpayer whose information has been inspected or disclosed in a manner not authorized by Section 6103.

F. *A list and analysis of the laws and regulations that govern the information being collected, reviewed, gathered, analyzed, or used in the data mining activity*

The disclosure and use of all tax data is governed by 26 U.S.C. 6103. Subsection (a) sets out the general rule of confidentiality. Subsection (b) sets forth definitions of terms commonly used throughout Section 6103. Subsections (c) through (o) of Section 6103 contain exceptions to the general rule of confidentiality. These Subsections permit disclosures as described generally below:

- Section 6103(c) – Disclosures to taxpayer's designees (consent);
- Section 6103(d) – Disclosures to state tax officials;
- Section 6103(e) – Disclosures to the taxpayer and persons having a material interest;
- Section 6103(f) – Disclosures to committees of Congress;
- Section 6103(g) – Disclosures to the President and White House;
- Section 6103(h) – Disclosures to Federal employees and the courts for tax administration purposes;
- Section 6103(i) – Disclosures to Federal employees for non-tax criminal law enforcement purposes and to combat terrorism, as well as the Government Accountability Office;
- Section 6103(j) – Disclosures for statistical purposes;
- Section 6103(k) – Disclosures for certain miscellaneous tax administration purposes;
- Section 6103(l) – Disclosures for purposes other than tax administration;
- Section 6103(m) – Disclosures of taxpayer identity information (generally for Federal debt collection purposes);
- Section 6103(n) – Disclosures to contractors for tax administration purposes; and
- Section 6103(o) – Disclosures with respect to wagering excise taxes.

In addition to disclosures permitted under provisions of Section 6103, other provisions of the Code also authorize disclosure of tax information. For example, Section 6104 authorizes disclosure of certain tax information regarding tax exempt organizations, trusts claiming charitable deductions, and qualified pension plans. Section 6110 authorizes disclosure of certain written determinations and their background files. The information contained in *Web-CBRS* is gathered under the guidelines dictated by the *Bank Secrecy Act,* 31 U.S.C. 5311.

G. *Policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:*

a. *Protect the privacy and due process rights of individuals, such as redress procedures*

All tax information is protected as required in 26 U.S.C. 6103 (see E Above).

The use of *Bank Secrecy Act* information is strictly controlled under the statute that directed its collection.

EFDS does not make any negative determinations. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any other ensuing actions. Due process is awarded during any ensuring criminal investigation or civil action.

b. Ensure that only accurate and complete information is collected, reviewed, analyzed, or used, and guard against any harmful consequences of potential inaccuracies

Tax data is self-reported by the individual/entity submitting the information to the government. *Web-CBRS* data is gathered from information compiled by the reporter based on information provided by their customer or based on the reporter's personal experience. Investigators scrutinize the SARs filed by the subject companies and request grand jury subpoenas for the underlying documentation. The supporting records are examined and individuals of interest are identified.

IRS-CI applications are required to have internal auditing capabilities. The internal audits track user access and queries performed with checks to validate against misuse. In addition, the data is a read-only extract that is validated for missing or duplicative data before entering the CI systems and remains unchanged in the CI systems.

2.0 FINANCIAL CRIMES ENFORCEMENT NETWORK (FinCEN)

A. Data mining activity, goals, and target dates for the deployment of the data mining activity, where appropriate

The Financial Crimes Enforcement Network (FinCEN) of the U.S. Department of the Treasury is statutorily obligated to analyze information to "determine emerging trends and methods in money laundering and other financial crimes." 31 U.S.C. § 310(b)(2)(C)(v). These trend analyses typically involve querying the database FinCEN maintains that contains information reported largely by financial institutions under the *Bank Secrecy Act* (BSA), 31 U.S.C. 5311, et seq. This information (BSA information or BSA reports) is collected where it has a "high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism," 31 U.S.C. 5311.

FinCEN conducts analyses to determine emerging trends and methods in money laundering in three ways: (1) by examining reports filed on specific violations (*e.g.*, terrorism financing) or filed on specific industries or geographic areas and conducting analyses on these subsets to determine whether they contain any identifiable trends, patterns or methods; (2) by conducting statistical analyses of currency flows over time to determine whether the data contains anomalous trends, patterns or methods; and (3) identifying trends, patterns or specific activities indicative of money laundering or financial crimes through the review and evaluation of reports as part of ongoing review processes.

FinCEN also engages in efforts that result in the identification of subjects for investigation either as a result of trend, statistical or strategic analyses or via other past, current or future tactical proactive efforts using link analysis driven software systems (see item B below) and includes the search for unknown subjects by establishing a search criteria based on previously established suspicious or illicit patterns. Other proactive methods include identifying subjects connected through the same addresses or telephone numbers and searching for subjects with the largest number of BSA reports filed on their financial activities.

B. Data mining technology that is being used or will be used, including the basis for determining whether a particular pattern or anomaly is indicative of terrorist or criminal activity

FinCEN utilizes several systems to accomplish its mission.

There is a link analysis-driven FinCEN system that allows users to query several data sets based on user-defined text patterns or data parameters. The following data sets are available for query within that system: (1) all BSA reports authorized by statute or regulation maintained in report-specific files and (2) FinCEN's case management system. This system also enables users to define alert notices based on user-defined data parameters.

There is a large BSA data system hosted by the IRS. Users with access to this system are able to query the BSA data set based on user-defined text patterns or data parameters.

There is a FinCEN system that provides users with the ability to query user-entered case information.

There is a FinCEN system that allows users to query for records based on user-defined text patterns or data parameters.

The basis for determining whether particular patterns or anomalies are indicative of terrorist or criminal activity varies. Because many BSA reports do not reveal the potential underlying criminal activity leading to the reported financial activity, FinCEN attempts to infer illicit cause for suspicious trends, patterns or methods by querying law enforcement databases on subjects or by identifying other financial or commercial records that may reinforce indications of anomalous or illicit activities.

C. *Data sources that are being or will be used*

The underlying data for FinCEN's manual and automated proactive search methods and trend analysis activities are the reports provided under the Bank Secrecy Act (BSA) administered by FinCEN, *e.g.*, a report by a financial institution of a suspicious transaction relevant to a possible violation of law or regulation (31 U.S.C. 5318(g)). Commercially available databases are used to support or further identify information that aids in the identification of the illicit cause for suspicious trends, patterns, or methods. FinCEN's trend analysis utilizes any records available to FinCEN, including subpoenaed financial records, public source information, commercial database information, Census bureau data, Federal Reserve data, etc., and is used to support or amplify conclusions or hypotheses derived from the analysis of BSA data. The authorities governing the filing requirements for such reports are detailed in item F below.

D. *Assessment of the efficacy or likely efficacy of the data mining activity in providing accurate information consistent with, and valuable to, the stated goals and plans for the use or development of the data mining activity*

FinCEN has occasionally experienced difficulty in assessing the efficacy of its proactive activities due to a lack of feedback from law enforcement, not only in reference to numbers of investigations opened, but also to the quality of the potential targets identified, *e.g.*, whether the identified activity was in fact related to illicit activities. FinCEN has, however, produced recent products in support of law enforcement and regulatory efforts to combat terrorism financing, mortgage loan fraud, and Southwest Border narcotics and bulk cash smuggling that received positive feedback.

Since FinCEN redirected its analytical efforts toward specialized analysis of BSA records in Fiscal Year (FY) 2005, FinCEN has produced proactive products for its law enforcement clients that are both strategic and tactical in nature.

From FY 2005 to 2009, proactive tactical products were produced in two categories: (1) referrals based on review and evaluation of Suspicious Activity Reports and, (2) investigative lead information that complemented or arose from strategic assessments of geographic areas, industries or issues. In both categories, FinCEN received feedback indicating positive follow-up to the tactical referrals.

- In an example related to coordination of investigative lead information in efforts to combat fraudulent loan modification schemes, a United States Senator stated, "I believe that, if implemented appropriately, the FinCEN-led Foreclosure Rescue Scam and Loan Modification effort will help both law enforcement combat fraud and consumers avoid scams."
- A senior Federal law enforcement official, commenting on FinCEN efforts to identify fraudulent mortgage modification activity, noted that "[t]he information provided by FinCEN will be used to develop and identify new leads and subjects of possible mortgage fraud investigations in Los Vegas as part of the National Mortgage Fraud Team."
- FinCEN supported a proactive effort to identify unusual or suspect financial transactions (and the related suspects) that might indicate fraud or corruption in the award and administration of contracts and grants. The law enforcement partner was "delighted with the outstanding level of cooperation and the responsiveness of FinCEN."

From FY 2005 to 2009, FinCEN produced strategic-level proactive (self-initiated) threat assessments of geographic areas, violation types, industries and terrorism financing issues. FinCEN received feedback demonstrating that these types of products are useful to law enforcement and the public. For example:

- In responding to a FinCEN terrorism financing assessment of suspicious currency flows, a senior law enforcement official engaged in counterterrorism investigations commented that the "analysis was initially helpful in helping . . . Headquarters, and individually the case agents in our various involved Field Offices, gauge the overall scope of financial activity of groups and individuals who were involved in previously known suspicious financial activity. " The official added that ". . .your analysis which covered five years provided a long term look at a problem which could not have been fully understood without the 'macro' approach you utilized."
- In commenting on a public FinCEN analytical report on the insurance industry, a senior official from an insurance industry association stated, "FinCEN's [insurance] report gives valuable guidance on how to improve SAR narratives for law enforcement. The collective information provides a tangible training tool for life insurers and their compliance departments. With this information at hand, the life insurance industry will be able to more efficiently and effectively fulfill its anti-money laundering responsibilities under the Bank Secrecy Act."
- In an example related to FinCEN's mortgage loan fraud analysis, a senior law enforcement official stated, "[This study] is an excellent example of the value of suspicious activity reporting. These types of SAR-based assessments are not only of benefit to law enforcement in assessing crime problems and trends; they also provide valuable feedback to the financial institutions who report the information." A senior official from a mortgage industry association stated, "This report is the authoritative source for data on fraud perpetrated against mortgage lenders and one which our members rely heavily on to spot trends and stay one step ahead of the fraudsters."
- Since publishing a report on The Role of Domestic Shell Corporations in Financial Crime and Money Laundering, FinCEN continues to receive positive feedback from, and to interact with, Federal and state law enforcement and regulatory agencies on this issue. FinCEN's Offices of Law Enforcement and Global Support continue to support FBI and International Financial Intelligence Unit (FIU) efforts to investigate corrupted corporate

service providers and to identify shell corporations facilitating international money laundering. FinCEN's Regulatory Policy and Programs Division is actively supporting efforts by the Department of the Treasury to improve corporate transparency and mitigate vulnerabilities associated with misuse of legal entities by illicit actors.

E. Assessment of the impact, or likely impact, of the implementation of the data mining activity on the privacy and civil liberties of individuals, including a thorough description of the actions that are or will be taken with regard to the property, privacy, or other rights or privileges of any individual as a result of implementing the data mining activity

The impact of FinCEN's congressionally mandated mission on the privacy and civil liberties of individuals has been and will continue to be small, and is within the confines of the law. As a threshold matter, the financial information held by banks and other financial institutions that FinCEN collects and analyzes pursuant to its authority in 31 U.S.C. 310 and the Bank Secrecy Act (BSA), 31 U.S.C. 5311, et seq., (discussed in more detail in item (F) below), has been found by the Supreme Court to trigger no constitutionally protected "expectation of privacy." U.S. v. Miller, 425 U.S. 435, 442-43 (1976). Moreover, the *Right to Financial Privacy Act of 1978*, 12 U.S.C. 3401, et seq., expressly provides that it gives no protection for financial records or information required to be reported in accordance with any federal statute or regulation, which includes information contained in BSA reports. See 12 U.S.C. 3413(d).

Significantly, FinCEN takes no adverse actions against individuals based on the existence of, or information contained in, BSA data. Rather, FinCEN provides the data, or analytical products analyzing the data, to outside agencies where the information may be relevant to current or potential investigations or proceedings under the jurisdiction of those agencies. Since a BSA report itself is not necessarily indicative of criminal activity, it is only the use of that report in conjunction with other evidence that makes the report useful. BSA information filed by financial institutions is generally used as lead information, which user agencies are instructed to verify with underlying financial institution or other records before relying upon the information. There is thus an inherent system of "checks and balances" with respect to the use of BSA information that ensures the protection of individual rights.

The *Bank Secrecy Act*, the constitutionality of which has been upheld by the Supreme Court (see California Bankers Association v. Schultz, 416 U.S. 21 (1974)), provides standards for proper use of the financial data authorized to be collected. The collected information is also generally subject to the *Privacy Act of 1974*, 5 U.S.C. 552a, discussed in more detail under item (F) below. FinCEN has developed extensive policies and procedures to ensure, to the extent reasonably possible, that (1) the analyzed information is used for purposes authorized by applicable law and (2) the security of the information is adequately maintained. Analytical products produced by FinCEN are subject to clearly specified restrictions regarding use and further dissemination of the products to ensure that the products will only be used by appropriate agencies for statutorily authorized purposes. To the extent such products reference information collected pursuant to the BSA, FinCEN's Re-Dissemination Guidelines for *Bank Secrecy Act* Information (the Re-Dissemination Guidelines) will apply, requiring user agencies to attach warning language to such reports and to follow the detailed procedures specified in the Guidelines when user agencies wish to further disseminate the information. These procedures aim to ensure that (1) only appropriate agencies will have access to the materials; (2) the materials will be used for statutorily authorized purposes; (3)

agencies with access are aware of the sensitivities of the material; and (4) FinCEN will be able to keep track of which agencies have such materials in their possession.

F. A list and analysis of the laws and regulations that govern the information being collected, reviewed, gathered, analyzed, or used in the data mining activity

I. The *Bank Secrecy Act*, 31 U.S.C. 5311, et seq. (BSA) and Implementing Regulations, 31 C.F.R. 103.11, et seq.

31 U.S.C. 5311. Declaration of Purpose

This section specifies that the purpose of the recordkeeping and reporting requirements in the BSA is to "require certain reports where they have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings, or in the conduct of intelligence or counterintelligence activities, including analysis, to protect against international terrorism." FinCEN strives to ensure that all uses of information are consistent with this purpose.

31 C.F.R. 103.12. Determination by the Secretary

This regulation provides the determination that the reports collected pursuant to the BSA are "highly useful" in the areas covered by 31 U.S.C. 5311.

31 U.S.C. 5319. Availability of Reports

This section makes it clear that, upon request, the Secretary (as delegated to FinCEN) is required to provide BSA information for the purposes specified in 31 U.S.C. 5311, to agencies including state financial institutions supervisory agencies, United States intelligence agencies, or self-regulatory organizations registered with the Securities and Exchange Commission or the Commodity Futures Trading Commission. This list of types of agencies is not exhaustive, but those listed are clearly covered. This section also provides that reports collected pursuant to the BSA are exempt from disclosure under the *Freedom of Information Act*, 5 U.S.C. 552.

31 C.F.R. 103.53. Availability of Information

This section authorizes the Secretary to make BSA information available to appropriate agencies for purposes specified in the BSA, and specifies that the information provided is to be received "in confidence" by the requesting agency.

31 U.S.C. 5313. Reports on domestic coins and currency transactions

This section provides for the reporting by financial institutions of reports of certain currency transactions involving more than an amount specified by the Secretary (as delegated to FinCEN).

31 C.F.R. 103.22. Reports of transactions in currency

This regulation implements the reporting requirement of 31 U.S.C. 5313 and specifies the amount of reportable transactions in currency at more than $10,000.

31 U.S.C. 5316. Reports on exporting and importing monetary instruments

This section requires reports by those that transport currency or other monetary instruments of more than $10,000 at one time from outside the U.S. into the U.S., or from the U.S. outside the U.S.

31 C.F.R. 103.23. Reports of transportation of currency or monetary instruments

This regulation implements the reporting requirement of 31 U.S.C. 5316 with respect to currency or other monetary instruments of more than $10,000 imported into the U.S. or exported outside the U.S.

31 U.S.C. 5314. Records and reports on foreign financial agency transactions

This section authorizes the Secretary (as delegated to FinCEN) to prescribe regulations requiring the reporting of certain types of foreign transactions and relationships with foreign institutions.

31 C.F.R. 103.24. Reports of foreign financial accounts

This regulation, implementing 31 U.S.C. 5314, requires that U.S. persons file reports of foreign bank accounts.

31 U.S.C. 5318(g). Reporting of suspicious transactions

This section authorizes the Secretary (as delegated to FinCEN), to require the reporting of suspicious transactions relevant to a possible violation of law. The section also provides for the confidentiality of such reports, barring financial institutions from notifying anyone involved in the transaction that the transaction has been reported. Government employees are subject to the same confidentiality restrictions, except as "necessary to fulfill the official duties" of such employees. The policies and procedures detailed above in response to item (E) are aimed, in large part, at maintaining the confidentiality of these reports.

31 C.F.R. 103.15 – 103.21. Reports of Suspicious Transactions

These regulations implement 31 U.S.C. 5318(g), requiring covered financial institutions to file suspicious activity reports and requiring the maintaining of strict confidentiality of the reports.

31 U.S.C. 5331. Reports relating to coins and currency received in nonfinancial trade or business

This section provides for the reporting of currency transactions of more than $10,000 by businesses other than financial institutions.

31 C.F.R. 103.30. Reports related to currency in excess of $10,000 received in a trade or business

This regulation implements 31 U.S.C. 5331.

II. The Privacy Act of 1974 (Privacy Act), 5 U.S.C. 552a, and Systems of Records Notices

Generally, the reports that FinCEN collects pursuant to the BSA are protected by the *Privacy Act*, in that they are "records" contained in a "system of records" as defined by the *Privacy Act*. 5 U.S.C. 552a (a)(4),(5). The *Privacy Act* provides that covered records may be disclosed without the written permission of the individual to whom the record pertains if they are disclosed pursuant to a "routine use." 5 U.S.C. 552a (b)(3). FinCEN has included sets of "routine uses" in its published Systems of Records Notices, required by the Privacy Act, that cover the areas in which FinCEN routinely shares BSA information. These areas (and specified recipients) are consistent with the purposes for which the information is collected, as specified in the BSA.

FinCEN has three Systems of Records Notices that cover the information it collects. These notices are: Treasury/FinCEN .001 - FinCEN Data Base (70 FR 45756), Treasury FinCEN .002 - Suspicious Activity Report System (70 FR 45757), and Treasury/FinCEN .003 – Bank Secrecy Act Reports System (70 FR 45760). In all cases, FinCEN shares covered information in accordance with these notices and the Routine Uses specified therein.

III. Other Relevant Provisions

31 U.S.C. 310. Financial Crimes Enforcement Network

This section, added by the *USA PATRIOT Act of 2001*, establishes FinCEN as a bureau in the Treasury Department, sets out the duties and powers of the Director, and empowers the Director to administer the BSA to the extent delegated by the Secretary of the Treasury (see below). The section requires FinCEN to maintain a "government-wide data access service" for the information it collects. FinCEN is required to "analyze and disseminate" the data for a broad range of purposes consistent with the BSA. See 31 U.S.C. 310 (b)(2)(C)(i-vii). These purposes include identifying possible criminal activity and supporting domestic and international criminal investigations (and related civil proceedings), determining emerging trends and methods in money laundering and other financial crimes, supporting the conduct of intelligence and counterintelligence activities, including analysis, to protect against international terrorism, and supporting government initiatives against money laundering. Id.

The section further provides, for example, that FinCEN furnish research, analytical, and informational services to financial institutions and domestic and foreign law enforcement agencies for the "detection, prevention, and prosecution of terrorism, organized crime, money laundering and other financial crimes" and provide "computer and data support and data analysis to the Secretary of the Treasury for tracking and controlling foreign assets." 31 U.S.C. 310 (b)(2)(E), (G). In addition, the section provides for the establishment of standards for making the information available through efficient means, and to screen appropriate users and appropriate uses. See 31 U.S.C. 310 (c)(1-2). The activities and procedures described in this document adhere to the tenets of this section.

Treasury Order 180-01 (September 26, 2002)

This document establishes FinCEN as a bureau in the Treasury Department and delegates authority to administer, implement, and enforce the *Bank Secrecy Act* to the Director of FinCEN.

G. Policies, procedures, and guidelines that are in place or that are to be developed and applied in the use of such data mining activity in order to:

a. Protect the privacy and due process rights of individuals, such as redress procedures

A description of the policies, procedures, and guidance in place to protect the analyzed reports and any privacy and property interests of the individuals that are the subject of the reports in question have been discussed in Item (E) above. With respect to redress procedures, due to the sensitivity of reports collected pursuant to the BSA, these reports have been exempted from such procedures in accordance with 5 U.S.C. 552a (j)(2) and (k)(2). See FinCEN's Systems of Records Notices (citations under item F (II) above) for further discussion. Specifically, such reports are exempt, for example, from the provisions in the Privacy Act allowing for: a subject's access to the reports, notification to the subject when reports shall be shared, the contesting of the contents of such reports by the subject, and the civil remedies covering these areas.

b. Ensure that only accurate and complete information is collected, reviewed, analyzed, or used and guard against any harmful consequences of potential inaccuracies

As discussed in item (E) above, FinCEN itself does not take adverse actions against individuals (outside the context of enforcing the requirements of the BSA itself) based on the information contained in BSA reports. In addition, because BSA information is only relevant in a particular proceeding based on the existence of other evidence, a BSA report in itself is generally not the basis for adverse actions by user agencies. There is thus an inherent system of "checks and balances" in the use of BSA information, guarding against harmful consequences from inaccuracies that may be contained in BSA reports. Moreover, FinCEN, through its data perfection procedures, ensures that the information contained in the database of BSA reports is accurate and complete.