FEDERAL AGENCY DATA MINING REPORT *(2012)*

Department of the Treasury
April 2013

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

The Department of the Treasury is pleased to provide Congress with its 2012 report to comply with the Federal Agency Data Mining Reporting Act of 2007. This report updates the Department's data mining activities since we issued our last report in 2012.[1] This report describes 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 databases.

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 four internal software programs: (1) Reveal; (2) Web Currency and Banking Retrieval System; (3) Investigative Data Analytics; and (4) the Electronic Fraud Detection System. The IRS data mining programs focus on the identification of financial crimes including tax fraud, money laundering, terrorism, and offshore abusive trust schemes. IRS uses these pattern-based searches to identify potential criminal activity. FinCEN's data mining activities focus on money laundering activities and other financial crimes.

[1] Public Law 110-53, 121 Stat. 363, Section 804 requires the head of each department or agency engaged in any activity to use or develop data mining to submit a report to Congress on those activities.

TABLE OF CONTENTS

1.0 INTERNAL REVENUE SERVICE (IRS)

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

The IRS uses four software programs that can perform sophisticated search and analytical tasks: Reveal, Web Currency & Banking Retrieval System (Web-CBRS), Electronic Fraud Detection System (EFDS), and Investigative Data Analytics (IDA). The IRS can use these programs to perform data mining activities by searching databases of internal and external information. IRS Criminal Investigation (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 the IRS-CI analysts and agents with the ability 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 hidden. The Visual Links tool builds visualization diagrams based on the data queried. The analyst is not required to construct the link analysis charts manually. IRS-CI's Lead Development Centers, Scheme Development Centers, and field offices use the system to identify and develop leads in 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; and 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 compiled by the EFDS are used to cross-reference and verify information that relates to potentially fraudulent tax returns. IRS-Wage and Investment (W&I) and IRS-CI leverage EFDS, which uses specific software to determine data mining scores. This program assigns a score to each refund return. The scores range from 0.0 to 1.0; the higher the score, the greater the potential for fraud on that return. IRS-CI does not directly examine the data mining scores, but rather leverages as a basis for its criminal investigations returns that W&I has determined to be fraudulent.

IDA is a data query tool that provides IRS-CI analysts and agents with the ability to query and analyze large and potentially disparate sets of data through a single access point. IDA enhances these search results by providing relationship linking, which exposes associations with events and other individuals. IDA assists users to expedite the identification and analysis of electronic data from multiple sources. This tool enhances investigation selection and supports investigative priorities. Special Agents and Investigative Analysts proactively identify patterns of illegal activities through this data analysis in support of tax law enforcement, counterterrorism, and other high priority

criminal investigations. IRS-CI Lead Development Centers, IRS-CI Scheme Development Centers, and field offices currently use IDA.

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, IDA, 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 Suspicious Activity Reports (SARs) filed on them by financial institutions in a six month period using the Reveal database. Previous successful investigations of money laundering, counterterrorism, and BSA violations provide indicia of fraudulent behavior.

IRS-W&I uses data mining to find fraudulent activity, and IRS-CI uses the fraudulent tax returns found by IRS-W&I as a basis for its criminal investigations.

Accepted Modernized e-File (MeF) returns are loaded into the EFDS. Returns meeting refund and data mining score tolerances are placed into the EFDS Prescan queue, which allows W&I and Scheme Development Center employees to view these returns for suspicious activities.

EFDS employs a data mining technology called IBM SPSS Modeler. Using this tool, rule sets were created using a standard built-in algorithm called C5.0. The models were trained using examples of current and prior year verified fraud and non-fraud data from which the machine learning models discern patterns or rules that are indicative of fraud. The output of the model is a score where a higher score represents a higher risk of fraud.

If a return meets designated score tolerances and other criteria, IRS-W&I examines the return for fraudulent activity. Fraudulent returns are added to the Scheme Tracking and Retrieval System (STARS) component of EFDS. IRS-CI examines the returns in STARS to find possible schemes that may result in a referral to an IRS-CI field office for investigation.

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

- **Taxpayer**: Filed tax returns.
- **Employers/Payers**: Information from employers/payers captured on Form W-2 and form 1099 as stored in the Information Returns Master File (IRMF).
- **Employee**: Source of employee information is the Online 5081.
- **Other Federal agencies**: Federal Bureau of Prisons for prisoner information; BSA data, Department of Health and Human Services for information on new hires; Social Security Administration for National Accounts Profile (NAP) data for dates of births and deaths.
- **State and local agencies**: Prisons in all states and the District of Columbia deliver prisoner listing information to IRS-W&I in electronic format.

- **Other third party sources**: IRS-W&I purchases commercial public business telephone directory listings/databases (*e.g.*, Accurint) to contact employers for employment and wage information.

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 additional investigative steps are required to verify the quality of the information. There is no empirical data on the efficacy of these searches.

The efficacy of the data mining on EFDS is only measured in terms of fraud prevention. This is measured using a broad range of metrics including the true positive rate/detection rate, false positive rate, and the value of refunds stopped. A key overall measure of efficacy is hit:scan, which represents the number of returns selected for verification that, upon inspection by IRS employees, are found to be fraudulent.

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 tasks IRS-CI with protecting revenue streams by detecting fraudulent activity and preventing 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.

Internal Revenue Code (26 U.S.C.) § 6103, which provides general rules of confidentiality and permissible disclosures, governs the impact or likely impact of the *EFDS* implementation of data mining activities on privacy and civil liberties of individuals. EFDS data mining activities, including its machine learning and scoring process, do not use any personally identifiable information in determining whether a return is likely to be fraudulent.

The tax returns that IRS-CI reviews are the subject of criminal investigations and actions based on tax laws, policies, and criminal procedures that govern them. Other tax returns are subjected to IRS civil treatment and examination procedures that provide for due process and redress procedure through taxpayer notification, appeals, and tax court options.

Internal Revenue Code § 6103 deems all taxpayer data private, confidential, and protected from disclosure, and it delineates the permitted disclosures. Other laws provide for civil and criminal penalties for any unauthorized disclosure of taxpayer data. The willful unauthorized disclosure of tax information is a felony and the unauthorized inspection of tax information is a misdemeanor. There is also a civil cause of action

available for taxpayers 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

Internal Revenue Code § 6103 governs the use of all tax data. 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 Section 6103, other provisions of the Code authorize disclosure of tax information. Section 6104, for example, 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 requirements of the BSA, 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 and F above).

The use of BSA strictly controls the information collected under it.

EFDS does not determine whether a return is fraudulent or whether a person is going to be subject to criminal prosecution. Once fraud is suspected, laws and administrative procedures, policies, and controls govern criminal investigations or any other ensuing actions. Due process is extended during any ensuing 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

The individual or entity submitting the information to the government self-reports tax data. 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.

The tax return information and other information stored in EFDS used for data mining are based on outside data sources. The only data generated directly in EFDS are the processing steps and the results of examinations of possibly fraudulent returns. The IRS conducts testing to ensure that the data stored in EFDS is correctly captured and accurate.

IRS applications have internal auditing capabilities that track user access and queries performed with checks to validate against misuse.

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 Treasury Department's Financial Crimes Enforcement Network (FinCEN) 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 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 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.

FinCEN has an advanced analytical system designed to allow users to query across large 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, (2) FinCEN's case management system, and (3) a third party data set. This system also enables users to create scheduled queries on user-defined data parameters.

In FY 2012, the majority of users of BSA data were transitioned from the IRS hosted BSA data system (WebCBRS) to a FinCEN hosted system (FinCEN Query). Users with access to this system are able to query the BSA data set based on user-defined patterns or data parameters.

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

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 and 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 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)). FinCEN uses commercially available databases to support or further identify information that aid 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, and Federal Reserve data, 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

Over the years, FinCEN has experienced some 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, received positive feedback on its recently-produced products in support of law enforcement and regulatory efforts to combat terrorism financing, mortgage loan fraud, identity theft, and Southwest Border narcotics and bulk cash smuggling.

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

Generally, FinCEN produces proactive tactical products in two categories: (1) referrals based on review and evaluation of Suspicious Activity Reports (SARs), and (2) investigative lead information that complemented or arose from strategic assessments of

geographic areas, industries or issues. Examples of both categories, on which we received positive feedback, are provided below.

- Utilizing the model developed for combating mortgage fraud (BSA data combined with other agencies data), FinCEN partnered closely with Health Care Fraud Prevention and Enforcement Action Teams (HEAT) to identify complex large-scale fraud schemes and the most egregious individual perpetrators and organized groups defrauding the health care system through FinCEN data analysis for specific geographic locations. The teams, which include investigators and prosecutors from Department of Justice and the Department of Health and Human Services, are working to strengthen existing programs, investigate fraud, and invest in new resources and technology to prevent future fraud, waste, and abuse.

In FY 2012, FinCEN completed 126 analytical/financial reports and analyzed over 138,000 BSA records concerning our increased analytical/investigative support to partnership agencies on health care fraud. FinCEN provided case support to six federal and three state and local agencies. On several occasions, FinCEN assisted with the analysis of bank records that further identified accounts and funds recovered through the asset forfeiture process. FinCEN assisted in the largest health care fraud takedown in history. Additionally, FinCEN issued a highly anticipated health care advisory and received very positive feedback concerning its use in criminal cases.

- In 2010, FinCEN began querying its BSA databases for SARs with certain types of high-risk financial institutions as subjects. In FY 2010 and 2011, FinCEN submitted referral reports to another financial regulatory agency referencing approximately $38 billion in suspicious activity by these subjects. Per the request of the Financial Fraud Enforcement Task Force (FFETF), FinCEN began providing these referrals to the FBI and selected U.S. Attorneys' offices in 2012. Through October 2012, FinCEN had referred several hundred high-risk financial institutions, appearing in approximately 1,000 SARs, and flagging suspicious activity totaling over $86 billion. The FBI indicated that it found 8-10 new cases for investigation during 2012 based on these FinCEN SAR referrals.

- Since 2009, FinCEN has also been querying its BSA databases for SARs reflecting suspicious use of proceeds from government financial support programs such as the Troubled Asset Relief Program. In FY 2012, FinCEN sent the Special Inspector General for Troubled Asset Relief Program almost 15,000 SARs referencing 18,610 subjects of possible interest that reported suspicious activity aggregating to over $313 billion.

FinCEN also 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:

- FinCEN proactively researches SARs to identify significant suspicious activity in certain foreign countries, particularly with respect to corrupt foreign

officials. These proactive alerts to foreign countries have led to the initiation of several investigations into high-level corruption within those countries. FinCEN has received feedback indicating that these alerts, and the resulting investigations, are generating significant interest within foreign governments.

- FinCEN produces Intelligence Advisories on money laundering trends and methods, primarily based on proactive analysis of various financial data combined with anecdotal reporting from law enforcement. Recent advisories have focused on cross-border currency flows and related suspicious financial activity associated with Mexico and the Southwest Border states. These advisories are disseminated to FinCEN's law enforcement partners and help inform FinCEN's public advisories to the financial and regulatory communities. Following the release of its advisory *Recent Trends in Funnel Account Activity* in April 2012, FinCEN began receiving requests from law enforcement field offices for proactive tactical information on potential funnel account targets. Because the advisory was data driven and not solely based on anecdotal law enforcement field reports, FinCEN was able to provide relevant data to the field offices rapidly and ultimately assist them in the detection of ongoing activity.

FinCEN expands the impact of these advisories by presenting findings at conferences and through various outreach venues. For example, following a briefing on OTI's analysis of the effects of Mexican cash restrictions on regional money laundering and cash flow trends to the Federal Reserve's International Cash Committee, a high-ranking Federal Reserve official commented that the intelligence brief was extremely effective and could impact the Federal Reserve's cash policies.

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 Supreme Court has ruled that the financial information that banks and other financial institutions hold, and that FinCEN collects and analyzes pursuant to its authority in 31 U.S.C. § 310 and the BSA (discussed in more detail in item (F) below), carries no constitutionally protected "expectation of privacy." *United States v. Miller*, 425 U.S. 435, 442 (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 useful in conjunction with other evidence. BSA information filed by financial institutions generally is used as lead information, which user agencies are instructed to verify with underlying financial institution or other records before relying upon. 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 BSA 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 has issued guidelines that 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 sensitivity of the material; and (4) FinCEN will be able to track 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. Chapter X

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. § 1010.301 — Determination by the Secretary

This regulation provides the determination that the reports collected pursuant to the BSA have a "high degree of usefulness" 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. § 1010.950 — 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. §§ 1010.311, 1021.311 — Reports of transactions in currency

These regulations implement the reporting requirement of 31 U.S.C. § 5313 and specify 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. § 1010.340 — 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. § 1010.350 — 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. §§ 1010.320, 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320 — 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. § 1010.330 — 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 Privacy Act protects reports that FinCEN collects pursuant to the BSA in that the reports are "records" contained in a "system of records." 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 Investigations and Examinations System (77 FR 60016), Treasury FinCEN .002 – Suspicious Activity Report System (77 FR 60017), and Treasury/FinCEN .003 – Bank Secrecy Act Reports System (77 FR 60020). In all cases, FinCEN shares covered information in accordance with these notices and the routine uses specified in them.

III. Other Relevant Provisions

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

This section 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 collected under the BSA as well as records and data maintained by other government agencies and other publicly and privately available information. 31 U.S.C. § 310(b)(2)(B). FinCEN is required to "analyze and disseminate" the data for a broad range of purposes consistent with the law. *See* 31 U.S.C. § 310 (b)(2)(C)(i) - (vii). These purposes include identifying possible criminal activity; 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 (March 24, 2003)

This document establishes FinCEN as a bureau in the Treasury Department and delegates authority to administer, implement, and enforce the BSA 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 normally 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 the information contained in the database of BSA reports is accurate and complete.