Currency & Banking Retrieval System (WebCBRS) – Privacy Impact Assessment

Approval Date: April 2, 2010

System Overview

The Currency & Banking Retrieval System (WebCBRS) is an on-line database that contains Bank Secrecy Act (BSA) information. Field agents in Examination, Collection and Criminal Investigation, as well as federal law enforcement, access 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. Federal regulatory agencies (Federal Reserve, Securities and Exchange Commission, etc) also use WebCBRS for general examination, compliance and enforcement efforts.

Systems of Records Notice (SORN):

- Treasury/IRS 34.037 IRS Audit Trail and Security Records
- Treasury/IRS 42.031 Anti-Money Laundering/Bank Secrecy Act (BSA) and Form 8300 Records
- Treasury/lRS 46.050 Automated Information Analysis System
- Treasury/FinCEN .002 Suspicious Activity Report System (the "SAR" System)
- Treasury/FinCEN .003 Bank Secrecy Act Reports System-Treasury/FinCEN

Data in the System

1. Describe the information (data elements and fields) available in the system in the following categories:

A. Taxpayer – Form TD F 90-22.1: Report of Foreign Bank and Financial Accounts (5 U.S.C. 552(e)(3) 91-508; 31 U.S.C. 1121; 5 U.S.C. 301, 31 CFR Part 103). PII data includes: Filers' name, address, taxpayer identification numbers, date of birth, and financial institutions' account numbers.

- Form 8300, Report of Cash Transactions Greater than $10,000 Received in a Trade or Business (IRC 6050I): PII data includes: Transactor's name, address, taxpayer identification number, and date of birth; subjects name, address, and taxpayer identification number; filer's taxpayer identification number.

- Form 7501: Entry Summary (Excise Tax). PII data includes: Importer of record name, address, and taxpayer identification number; Ultimate consignee name and address.

B. Employee – Userid and password

C. Audit Trail Information:

User Query DescriptionTable – for each query a user executes will contain:

- User_ID – Identification of user executing the query
- Query_Tmsp – timestamp when the query was initiated
- Query_Desc – a short description of the query (optional)
- Query_Elapsed_Time – run time of the query
- Query_Result_Count – number of rows returned

User_Query Parms Table – for each query description row, contains parameters entered:

- User_ID – identification of user executing the query

- Query_Tmsp – timestamp when the query was executed (each time)
- Parm_Seq – parameter sequence number
- Query_Group, Condition, Part_Data_Value, IDN_Data_Value, Locn_data_value, Relational_operatr, Query_Doc_types – these fields contain the query parameters entered by the end user
- Target_table_Name – tables access by the query

User_Query_Log Table – contains all document control numbers that were viewed, in full or partially, by end users.

- Qrylog_Tmsp – timestamp when the data was viewed
- User_ID – user identification of the user that viewed the data
- DCN – document control number of the document(s) that were viewed
- Query-tmsp – timestamp when the query was initiated
- Hitlist_Ind – switch showing if the data was viewed on the screen as part of the users selected data elements. The user viewed those fields on the listed document.
- Drilldown_Ind – switch indicating the named user opened the listed document for viewing
- Doc_type – type of document that was viewed

User_Download_Log – contains a list of all documents that were downloaded by an end user.

- Dwnlog_Tmsp – timestamp when the listed document was downloaded
- User_Id – user identification of the user that downloaded the documents
- DCN – document control number of the document(s) that were downloaded by the named user
- Query_Tmsp – timestamp when the query was that returned the DCNs

D. Other – The external users all have profiles that control the information forms they may access on the database. WebCBRS also contains the following types of Information Returns:

- FinCEN 104: Currency Transaction Report (31 U.S.C. 5313 and 31 CFR Part 103 PII information contained on this form includes: transactors' name, address, taxpayer identification number, and date of birth; subjects' name, address, taxpayer identification number, and date of birth; transaction account numbers; taxpayer identification number for reporting institution.

- Form 8300: Report of Cash Payments Over $10,000 Received in a Trade or Business (26 U.S.C. 6050I and U.S.C. 5331). PII data includes: Transactors' name, address, taxpayer identification number, and date of birth; subject's name, address, and taxpayer identification number; filer's taxpayer identification number.

- FinCEN Form 103: Currency Transaction Report by Casinos (31 U.S.C. 5313 and 31 CFR Part 103).

- FinCEN Form 103-N: Currency Transaction Report by Casinos – Nevada (Nevada Gaming Commission Regulation 6A in lieu of 31 U.S.C. 5313 and 31 CFR Part 103) Note: Form 103N is no longer in use. However, information from older filings remains on the Web-CBRS data base. PII information contained on Forms 103 and 103N includes: Transactors' name, address, date of birth, and taxpayer identification number; Casino reporting transactions taxpayer identification number.

- Form TD F 90-22.47: Suspicious Activity Report (31 U.S.C. 5318(g)(3)). PII information contained on this form includes: Taxpayer identification number for institution reporting the suspicious activity; Name, address, taxpayer identification number, telephone number, and date of birth of suspects.

- FinCEN Form 102: Suspicious Activity Report by Casinos (31 U.S.C. 5318(g), Nevada Revised Statute 463.125, or New Jersey Casino Control Act 5:12-129.1)1. PII information contained on this form includes: Subjects' name, address, taxpayer identification number, account number, drivers license number, date of birth, and telephone number; taxpayer identification number of casino reporting the transaction; a narrative may also include PII information.

- FinCEN Form 101: Suspicious Activity Report by Securities and Future Industries. PII information contained on this form includes: Subjects' name, address, taxpayer identification number, account numbers, drivers license number, date of birth, and telephone number; taxpayer identification number of financial institution reporting the transaction; a narrative may also include PII information.

- FinCEN Form 109/TD F 90-22.56: Suspicious Activity Report by Money Service Business. PII information contained on this form includes: Subjects' name, address, taxpayer identification number, drivers license number, date of birth, and telephone number; taxpayer identification number of business reporting the transaction; a narrative may also include PII information.

- FinCEN Form 107/TD F 90.22.55: Registration of Money Service Business. PII information contained on this form includes: Registrant's taxpayer identification number; Address, telephone number, date of birth, and taxpayer identification of owner or controlling person; Primary transaction account number.

- FinCEN Form 110/Form TD F 90-22.53: Designation of Exempt Person (31 CFR 103.22). Note: As a result of a change in the regulations, effective 01/05/2009, Biennial Renewal Certifications will no longer be required for exempt businesses. PII information contained on this form includes: Name, address, and taxpayer identification of exempt person; Filer name, address, and taxpayer identification number.

- FinCEN Form 105: Report of International Transportation of Currency or Monetary Instruments 1 U.S.C. 5316; 31 CFR 103.23 and 103.25). PII information contained on this form includes: Name, address, and date of birth of subject.

- Form 7501: Entry Summary (Excise Tax). PII data includes: Importer of record name, address, and taxpayer identification number; Ultimate consignee name and address.

2. Describe/identify which data elements are obtained from files, databases, individuals, or any other sources.

A. IRS – Taxpayer identification numbers are validated for paper document filings using an IRS data file.

B. Taxpayer – The only information collected directly from the taxpayer is from Form TD F 90-22.1, Report of Foreign Bank and Financial Accounts.) PII data includes: Filers' name,

address, taxpayer identification numbers, date of birth, and financial institutions' account numbers.

C. Employee – IRS Employee information could be posted to WebCBRS if the employee conducts cash transactions with a financial institution, casino, or a trade/business for $10,000 or more. This information would be the same as for any other subject, and include: name, address, date of birth, taxpayer identification numbers, and account identification numbers.

D. Other Federal Agencies:

- United States Customs and Enforcement Service [Homeland Security – ICE] Entry Summary Form 7501, PII data includes: Importer of record name, address, and taxpayer identification number; Ultimate consignee name and address, and FinCEN Form 105, Report of International Transportation of Currency or Monetary Instruments CMIR. PII information contained on this form includes: Name, address, and date of birth of subject.

- United States Postal Service City/State Zip code tables

E. None

F. Other Third Party Sources – Transactional reports come from a variety of sources, including banks, financial institutions, casinos, non-bank financial institutions and retail businesses. This information would include: subject name, address, date of birth, taxpayer identification numbers, and account identification numbers. Suspicious Activity Reports could also include PII information in a narrative format.

3. Is each data item required for the business purpose of the system? Explain.
Yes. All data items are required for the business purpose of the system. The Secretary of the Treasury has determined that the information contained in Bank Secrecy Act forms "have a high degree of usefulness in criminal, tax, or regulatory investigations or proceedings." IRS Examination, Collection and Criminal Investigation, as well as federal law enforcement, access 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. Federal regulatory agencies (Federal Reserve, Securities and Exchange Commission, etc) also use WebCBRS for general examination, compliance and enforcement efforts.

The specific data items collected in Web-CBRS through BSA forms are approved by FinCEN with input from agencies and Treasury Bureaus that use the data for the purposes identified in the Bank Secrecy Act and subsequent legislation. Every form is reviewed for reissuance on the Office of Management and Budget [OMB] schedule.

4. How will each data item be verified for accuracy, timeliness, and completeness?
As data is posted to WebCBRS, information is checked for accuracy. If errors are detected, correspondence letters are mailed to the filer asking for missing and incomplete information. Correspondence replies are posted to WebCBRS upon receipt.

5. Is there another source for the data? Explain how that source is or is not used.
No

6. Generally, how will data be retrieved by the user?
IRS users access Web-CBRS through a web-based front end or a desktop application. Users, however, must have the appropriate approved security authority to do this. External users are approved by FinCEN for access to data in the Web-CBRS application. External users must access Web-CBRS through the FinCEN Secure Gateway application.

7. Is the data retrievable by a personal identifier such as name, SSN, or other unique identifier?
Yes. Users with the appropriate security access generally will search the database using an Identification Number, name, date of birth, account number or address.

Access to the Data

8. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Others)?
Data access permissions are based on the need to know and job responsibilities for each position. Employees having access to the data include Revenue Officers, Revenue Agents, Special Agents, Bank Secrecy Act (BSA) Specialists, BSA Tax Examiners, BSA Tax Law Specialists, BSA Legal Instrument Examiners, BSA Management Analysts, and Managers. Users will generally have access to transaction reports, but not Suspicious Activity Reports. The Financial Crime Enforcement Network (FinCEN), IRS Criminal Investigators, IRS Title 31 employees, and a limited number of other personnel will have access to all form types. (To clarify, note that FinCEN is an agency of the Department of Treasury as is IRS.) Treasury Application developers and systems administrators will not have access to live data without an approved waiver. All IT contractors must obtain a security clearance through the Treasury National Background Investigative Center [NBIC] before they begin to work on this application.

9. How is access to the data by a user determined and by whom?
Access to the data is determined by agency and information supplied on Form 5081. The 5081 contains rules of behavior for accessing information systems. Both the employee and the employee's manager sign an electronic Form 5081. When the employee signs this document, they are accountable for his/her misuse of the system.

Users of WebCBRS are granted least use access (Read Only). Additionally, system profiles limits or grants access to the various Bank Secrecy Act (BSA) data depending on the agency the employee works for. All users of WebCBRS are profiled for least access "Read Only". Users are then categorized as IRS or Non-IRS users, and are further categorized on each individual users profile if they have access to each form. An MOU with FinCEN is in place to manage access by the Non-IRS users, through the FinCEN Secure Outreach (SO) network.

For example, IRS Revenue Officers, Revenue Agents and Special Agents have access to all forms. A non-IRS user from the Nevada Gaming Control Board will have access to FinCEN Form 103-N, Currency Transaction Report by Casinos – Nevada (reported only from filers in the State of Nevada), and FinCEN Form 102, Suspicious Activity Report by Casinos. (Note: Form 103N is currently obsolete, and was replaced with FinCEN Form 103, although some older forms are still on WebCBRS.) WebCBRS does not generate audit cases. However, IRS Revenue Officers, Revenue Agents and Special Agents are required to query WebCBRS on all open cases before closure.

10. Do other IRS systems provide, receive, or share data in the system? If YES, list the system(s) and describe which data is shared.
Yes. The Automated Magnetic Media Processing System AMMPS, Receives information on Currency Transaction Reports from WebCBRS. AMMPS is an IRS Small Business Self-employed (SBSE)

application used to track, schedule, submit, and process underreporter data from Information Return Forms 1099. It is a non-FISMA application which serves as an interface between WebCBRS and the IRS Masterfile.

The following data is shared through the AMMPS interface into the IRS Masterfile:

- FinCEN 104: Currency Transaction Report (31 U.S.C. 5313 and 31 CFR Part 103. PII information contained on this form includes: transactors' name, address, taxpayer identification number, and date of birth; subjects' name, address, taxpayer identification number, and date of birth; transaction account numbers; taxpayer identification number for reporting institution.

- Form 8300: Report of Cash Payments Over $10,000 Received in a Trade or Business (26 U.S.C. 6050I and U.S.C. 5331). PII data includes: Transactors' name, address, taxpayer identification number, and date of birth; subject's name, address, and taxpayer identification number; filer's taxpayer identification number.

- FinCEN Form 103: Currency Transaction Report by Casinos (31 U.S.C. 5313 and 31 CFR Part 103)

- FinCEN Form 103-N: Currency Transaction Report by Casinos – Nevada (Nevada Gaming Commission Regulation 6A in lieu of 31 U.S.C. 5313 and 31 CFR Part 103). Note: Form 103N is no longer in use. However, information from older filings remains on the Web-CBRS data base. PII information contained on Forms 103 and 103N includes: Transactors' name, address, date of birth, and taxpayer identification number; Casino reporting transactions taxpayer identification number.

- AMMPS receives fact of filing (file or did not file) information only from Form TD F 90-22.1, Report of Foreign Bank and Financial Accounts. PII data for this form, generally available in WebCBRS is not available in AMMPS.

11. Have the IRS systems described in Item 10 received an approved Security Certification and Privacy Impact Assessment?
No. AMMPS is a non-FISMA application which serves as an interface between WebCBRS and the IRS Masterfile.

12. Will other agencies provide, receive, or share data in any form with this system?
Yes. The following agencies have least access (read only) to WebCBRS, except for the United States Customs Service which provides data from Form 7501, Entry Summary (Excise Tax). Form 7501 PII data includes: Importer of record name, address, and taxpayer identification number; Ultimate consignee name and address.

An MOU with FinCEN is in place to manage access by the Non-IRS Agencies, through the FinCEN Secure Outreach (SO) network. (To clarify, note that FinCEN is an agency of the Department of Treasury as is IRS.)

- Alcohol, Tobacco and Firearms
- Comptroller of the Currency
- Department of Justice
- Drug Enforcement Administration
- Executive Offices of the United States Attorney General
- Federal Bureau of Investigation

- Federal Deposit Insurance Corporation
- Federal Reserve System
- Financial Crime Enforcement Network
- National Credit Union Administration
- Nevada Gaming Control Board
- Office of Thrift Supervision
- Securities and Exchange Commission
- Treasury Inspector General for Tax Administration
- U.S. Customs Service
- U.S. Postal Inspector
- U.S. Secret Service
- Over 75 State and Local Law Enforcement Agencies across the 50 States

Administrative Controls of Data

13. What are the procedures for eliminating the data at the end of the retention period?

- Paper Storage: The current year plus three prior years are kept on-site at the Detroit Computing Center. Documents are retired to the Federal Records Center three years after the end of the processing year, and destroyed eleven years after the end of the processing year. Procedures are documented in the Records Control Schedule for the Detroit Computing Center IRM 1.15.18, Exhibit 1.15.18-1, Item 15.

- On-Line: WebCBRS holds 11 years of data: one for the current year and ten prior years. Data is archived to magnetic media as a year is dropped from the system. FinCEN is working with NARA to develop a formal Records Retention Schedule for electronic records. FinCEN has an extension from NARA to complete this records retention schedule. The documentation is available from FinCEN's Records Officer.

14. Will this system use technology in a new way?
No

15. Will this system be used to identify or locate individuals or groups? If so, describe the business purpose for this capability.
Yes. The purpose of WebCBRS is to house currency transactions reportable under U.S.C. 26 and 31 requirements. Individuals can be located by QUERY using the PII fields for each form.

16. Will this system provide the capability to monitor individuals or groups? If yes, describe the business purpose for this capability and the controls established to prevent unauthorized monitoring.
Yes. Management reviews employee access audits at least annually to ensure that employees are accessing and using the information from the system for assigned casework. FinCEN also monitors use by non-IRS agency employees. WebCBRS is a database that contains information on cash transactions of $10,000 or more and is a mandated research tool used by agents during tax-related cases. For IRS personnel, there is a clearly defined and documented procedure, the use of an automated Form 5081, for requesting access to WebCBRS. The automated OL5081 system contains rules of behavior for access to the information system. The employee and manager sign the electronic OL5081. By signing this document, the user is accountable for his/her misuse of the system.

17. Can use of the system allow IRS to treat taxpayers, employees, or others, differently?
No. There is no disparate treatment of individuals or groups. The goal of WebCBRS is to provide law enforcement and regulatory agencies access to the currency transaction data, which could be useful when conducting criminal, tax, and regulatory investigations and proceedings. Each of the categories under suspicion is treated the same way.

18. Does the system ensure "due process" by allowing affected parties to respond to any negative determination, prior to final action?
Yes. The system allows amendments and corrections. Currency Transaction Report filers (banks, financial institutions, casino, non-bank financial institutions and retail businesses) can correct previously filed erroneous information.

19. If the system is web-based, does it use persistent cookies or other tracking devices to identify web visitors?
WebCBRS does not use any form of persistent cookies. When a user logs into WebCBRS, a session cookie is created, which is kept in memory by the web browser, but never stored on disk for return visit tracking? WebCBRS tracks users through audit logs kept after a user logins into the system.

View other PIAs on IRS.gov