Audit Report

OIG-24-030

ANTI-MONEY LAUNDERING/TERRORIST FINANCING

Audit of FinCEN's Management of BSA Data – User Access Report

August 1, 2024

Office of Inspector General
Department of the Treasury

This Page Intentionally Left Blank

Contents

Audit Report

Appendices

Abbreviations

BSA	Bank Secrecy Act
CTR	Currency Transaction Report
FinCEN	Financial Crimes Enforcement Network
GAO	Government Accountability Office
Green Book	*Standards for Internal Control in the Federal Government*
JAMES	Joint Audit Management Enterprise System
LE	law enforcement
MOU	memoranda of understanding
OIG	Office of Inspector General
SAR	Suspicious Activity Report
SOP	Standard Operating Procedure
technicians	Application Help Desk Technicians
Treasury	Department of the Treasury

Audit Report

August 1, 2024

Andrea Gacki
Director
Financial Crimes Enforcement Network

This report is the second in a series of reports presenting the results of our audit of the Department of the Treasury's (Treasury) Financial Crimes Enforcement Network's (FinCEN) management of Bank Secrecy Act (BSA)[1] data. Our audit objective was to determine if FinCEN manages BSA data access, use, and retention in compliance with laws, regulations, and Treasury policies and procedures (hereinafter referred to as standard operating procedures (SOP)). We previously issued an audit report regarding FinCEN's management of BSA data retention, including suppression of certain sensitive records.[2] This audit report addresses FinCEN's management of BSA data access, specifically, granting and revoking access to FinCEN Portal.[3] This report does not include audit results related to granting bulk data access. In the future, we will issue an additional audit report, the third in this series, also addressing FinCEN's management of BSA data access, including FinCEN's processes for: (1) maintaining a compliant system of records notice, (2) establishing and maintaining memoranda of understanding (MOU) with external agencies that use BSA data,

[1] Titles I and II of P.L. 91-508, Currency and Foreign Transactions Reporting Act (commonly referred to as the "Bank Secrecy Act" or "BSA") (October 26, 1970), requires U.S. financial institutions to retain records and file reports to assist U.S. government agencies in detecting and preventing money laundering. The BSA is codified at 12 U.S.C. 1829b and 1951-1960 and 31 U.S.C. 5311-5314 and 5316-5336, and includes notes thereto. FinCEN is responsible for implementing, administering, and enforcing compliance with the BSA and associated regulations.

[2] Treasury OIG, *Anti-Money Laundering/Terrorist Financing: Audit of FinCEN's Management of BSA Data – Suppression Report*, OIG-23-030 (August 31, 2023)

[3] FinCEN Portal is a web-based application that allows authorized users access to the BSA database. Portal users can access the BSA data through queries (FinCEN Query application) or by receiving bulk data. Bulk data is the transfer of entire copy sets of FinCEN BSA data to an external agency. While FinCEN previously used the term, "bulk data" during our audit scope period, it now uses the term, "Agency Integrated Access."

and (3) granting bulk data access. Publication of the fourth and final report in this series, addressing FinCEN's management of BSA data use, specifically FinCEN's monitoring processes, will conclude our audit of FinCEN's management of BSA data.

As mandated by the BSA, FinCEN maintains a government-wide data access service that includes reports or records,[4] collectively referred to as BSA data. This data is useful in a range of governmental efforts to combat money laundering, including, criminal, tax, or regulatory investigations and risk assessments, as well as intelligence or counterintelligence activities to protect against terrorism. To comply with its mandate, FinCEN maintains the BSA data filed in its BSA database. FinCEN provides BSA database access to employees from FinCEN and external intelligence, law enforcement (LE), and regulatory agencies.

To accomplish our objective as it relates to this audit report, we reviewed applicable laws, regulations, SOPs, and guidance; interviewed FinCEN personnel; and non-statistically selected and tested whether FinCEN properly managed active and disabled BSA database user accounts. The scope of our audit, related to this report, covered the period from October 2016 through January 2020. We conducted fieldwork related to this report from June 2019 through March 2023. Appendix 1 provides a more detailed description of our audit objective, scope, and methodology.

Results in Brief

FinCEN did not manage aspects of BSA data access in compliance with applicable SOPs, MOUs, and government-wide standards. Specifically, FinCEN did not: (1) have proper controls to ensure that external agencies provided proper notification to FinCEN when disabling accounts, (2) maintain proper records of the dates and reasons internal user accounts were disabled, (3) timely disable internal user accounts, (4) properly complete out-processing forms for departed employees, and (5) require agencies to identify whether users received background checks.

Accordingly, we are making eight recommendations to improve FinCEN's management of BSA data access. We recommend that

[4] 31 U.S.C. 310, *Financial Crimes Enforcement Network*

the Director of FinCEN: (1) implement internal controls to ensure that agencies properly notify FinCEN when agencies revoke user access for non-routine actions; (2) determine whether the MOU requirement that agencies notify FinCEN when they revoke user access for routine personnel actions is necessary, and if not, communicate this change to agencies, in writing, and remove that language from future MOUs; (3) update MOUs and related guidance to specifically require agencies to disable accounts when their users no longer require or meet criteria for access, and to include a timeliness metric to ensure accounts are disabled promptly; (4) determine if a database software update is warranted to accurately capture a historical record of the dates and reasons user accounts are disabled, and if warranted, implement the update; otherwise, design and implement an alternative tracking method; (5) update the *FinCEN Portal/Query/FIR – Disabled Account Tickets* SOP to add quarterly and "spot-check" reviews of disabled user accounts to determine if supervisors are providing advance notification of departing employees and if Application Help Desk Technicians (technicians) are appropriately and timely disabling accounts; (6) update the *Account Management* guidance to include a timeliness metric for how quickly technicians must disable an account when a user no longer requires access; (7) implement quality control measures, including a timeliness metric for form completion, to ensure supervisors properly review and complete departed employees' out-processing forms; and (8) ensure the background check field is mandatory for FinCEN Portal user account profiles, and until the related system update takes effect, design and implement a process to ensure only users with background checks can access BSA data, and confirm that background checks were completed for all existing users.

In a written response, included in its entirety as appendix 2, FinCEN management concurred with our recommendations and provided their planned and taken corrective actions. In response to our first three recommendations, management stated they updated their SOPs, are finalizing updates to their MOUs, and plan to implement corresponding internal controls. For recommendation four, management stated they are replacing their database software to accurately capture all changes to users' accounts. For recommendations five and six, management stated they plan to update their SOPs to include the additional reviews and metrics described in our recommendations. For recommendation seven, management stated they are implementing a more automated

process to ensure timely completion of out-processing forms. Lastly, for recommendation eight, management stated they are updating their application control system to make the background check field mandatory. Management anticipates completing all corrective actions by the end of calendar year 2024. We have not verified FinCEN management's corrective actions taken, however the stated corrective actions meet the intent of our recommendations. Management should include its stated corrective actions and expected completion dates in the Joint Audit Management Enterprise System (JAMES), Treasury's audit recommendation tracking application.

Background

FinCEN is responsible for maintaining a government-wide data access service for BSA records, which include Suspicious Activity Reports (SAR),[5] Currency Transaction Reports (CTR),[6] and other BSA reports (collectively referred to as "BSA data"), in its BSA database. Our report refers to FinCEN's data access service as the BSA database. Filers of BSA data submit approximately 55,000 BSA records to FinCEN per day. Filers of BSA data are mostly businesses. The most common business sector entities filing BSA data are financial institutions, most of which are required to file SARs and CTRs. However, other BSA reports are also filed with FinCEN, including by filers that are not businesses. For example, U.S. Customs and Border Protection, a federal government LE agency of the U.S. Department of Homeland Security, collects Reports of International Transportation of Currency or Money Instruments from individuals and provides that information to FinCEN. In addition, individuals file reports of foreign bank and financial accounts to FinCEN. FinCEN allows its employees and external LE, intelligence, and regulatory agency users to access the BSA database to conduct official agency business. The external users have access to BSA data under the terms of an MOU between FinCEN and the users' agency.

[5] SARs must be filed with FinCEN to report known or suspected violations of law or regulation or suspicious activity observed by financial institutions for transactions exceeding $5,000; money service businesses must report any such transactions exceeding $2,000.

[6] CTRs must be filed with FinCEN when a financial institution receives transactions in currency over $10,000, or multiple transactions that total more than $10,000 in a single day, conducted by or on behalf of one person.

User Access

To gain access to the BSA database, an agency submits a written request to FinCEN, and FinCEN personnel determine if the agency has sufficient need to access the data. If FinCEN approves the request, it will execute an MOU with the agency. Once an MOU is in place, FinCEN personnel provide the agency's employees access to the database in conjunction with training. FinCEN has approximately 475 MOUs with participating external agencies.

Agencies are typically provided BSA data by either obtaining direct access to FinCEN Portal, a web-based application that allows authorized users access to the BSA database, or by receiving bulk data. Agencies' users can directly retrieve BSA data through FinCEN Query, an online database query application within FinCEN Portal that allows users to search, access, and analyze the data. There are nearly 14,000 FinCEN Portal users with direct access to the BSA database.

Once an MOU is executed, the agency appoints an Agency Coordinator who, among other things, is responsible for adding agency users to FinCEN Portal. The Agency Coordinator also is required to complete the account fields[7] in the users' profiles. FinCEN's Strategic Operations Division personnel determine if users are approved by the agency, and if so, instruct FinCEN's Technology Division personnel to enable the users' FinCEN Portal accounts. For FinCEN employees, the user's supervisor must provide approval before the Technology Division personnel establish the user's access to their FinCEN Portal account. Upon accessing the BSA database through FinCEN Portal, the user must accept a *User Acknowledgement* agreement listing the conditions for obtaining and maintaining access to FinCEN Portal; users must re-acknowledge the agreement annually. New users must also complete FinCEN's Data Certification training,[8] and retake the training every two years thereafter.

If FinCEN personnel determine that an internal user no longer needs access to the Portal due to separation of employment, reassignment, or security concerns, FinCEN should disable the

[7] The following fields are required in the users' profiles: email address, phone number, mailing address, completed background check, and agency name.

[8] FinCEN Data Certification training is designed to ensure users understand the requirements for the proper use and disclosure of BSA data.

user's account. FinCEN personnel should also revoke the Personal Identity Verification cards for all internal users who depart FinCEN, which prevents future access to FinCEN facilities and systems, including the Portal. For external users, an Agency Coordinator has the responsibility to disable an agency user's account if the agency determines that the user no longer qualifies for or needs access. All users are required to log in to their FinCEN Portal account every 90 days; otherwise, the account is automatically temporarily disabled. After 365 days of inactivity, the FinCEN Portal system will automatically delete the user's account.

Audit Results

This report relates only to the BSA data access portion of our audit objective, specifically whether FinCEN manages BSA data access in compliance with laws, regulations, and Treasury SOPs. FinCEN maintains a government-wide direct data access service and has related SOPs, as mandated by the BSA. We non-statistically tested 104 of 12,614 active FinCEN Portal user accounts and found that those users' agencies (external to FinCEN) executed MOUs with FinCEN. Additionally, 91 of the 104 users signed a *User Acknowledgement* agreement and completed training as required. The remaining 13 users did not perform a search of the BSA database during our scope period of May 2017 to May 2019, and therefore, were not required to sign the *User Acknowledgement* agreement or complete training at the time of our testing. Although we found that MOUs and *User Acknowledgement* agreements were signed and training was completed, FinCEN did not otherwise manage BSA data access in compliance with its SOPs and MOUs, and government-wide standards. Specifically, FinCEN did not: (1) have proper controls to ensure that external agencies provided proper notification to FinCEN when disabling accounts, (2) maintain proper records of the dates and reasons internal user accounts were disabled, (3) appropriately and timely disable internal user accounts, (4) properly complete out-processing forms for departed employees, and (5) require agencies to identify whether users received background checks.

Finding 1 FinCEN Did Not Have Proper Controls to Ensure That External Agencies Provided Proper Notification to FinCEN When Disabling Accounts

FinCEN employees told us that external agencies did not notify FinCEN when those agencies revoked user access for routine personnel actions, such as an employee leaving an agency. In addition, FinCEN could not provide documentation showing that agencies notified FinCEN when revoking user access for non-routine personnel actions, such as an employee conducting improper searches. FinCEN MOUs require external agencies to notify FinCEN if agencies revoke a user's access to FinCEN Portal. Agencies can revoke user access due to routine or non-routine personnel actions. However, the FinCEN employee responsible for receiving these notifications stated they were sent infrequently.

A FinCEN employee told us the requirement that agencies notify FinCEN of routine personnel actions is unnecessary, and the related MOU language is old and needs to be updated. The employee also told us that, although the requirement that agencies provide notification when revoking a user's access for non-routine personnel actions is necessary. FinCEN employees told us they found the requirement difficult to enforce, and therefore, did not consistently monitor or impose it. Nevertheless, the requirement that agencies notify FinCEN when revoking user access is set forth in current MOUs, and FinCEN did not implement internal controls to ensure agencies complied with the requirement.

Moreover, FinCEN's written guidance did not require agencies to disable external user accounts or specify a related timeliness metric. Therefore, in addition to not notifying FinCEN, agencies may not be appropriately and timely revoking user access. Without the proper revocation of access and related notifications, FinCEN cannot ensure agencies are appropriately managing user accounts. As a result, FinCEN may be unaware of system use violations, and delays in disabling user accounts may result in unauthorized users having access to BSA data.

Recommendations

We recommend that the Director of FinCEN:

1. Implement internal controls to ensure that agencies properly notify FinCEN when agencies revoke user access for non-routine personnel actions.

Management Response

FinCEN management concurred with our recommendation. Management stated they revised their MOUs to require agencies to disable users for non-routine personnel actions and notify FinCEN within stated timelines. Additionally, management stated they updated their SOPs to verify that these timelines are being adhered to and take appropriate remedial action, if required. Management expects to complete this work by July 31, 2024.

OIG Comment

We have not verified FinCEN management's corrective actions taken, however the stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

2. Determine whether the MOU requirement that agencies notify FinCEN when they revoke user access for routine personnel actions is necessary, and if not, communicate this change to agencies, in writing, and remove that language from future MOUs.

Management Response

FinCEN management concurred with our recommendation. Management stated they revised their MOUs to only require agencies to notify FinCEN for non-routine personnel actions, but not for routine personnel actions. Management anticipates providing written guidance to the agencies to communicate this change. Management expects to complete this work by July 31, 2024.

OIG Comment

We have not verified FinCEN management's corrective actions taken, however the stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

3. Update MOUs and related guidance to specifically require agencies to disable accounts when their users no longer require or meet criteria for access, and to include a timeliness metric to ensure accounts are disabled promptly.

Management Response

FinCEN management concurred with our recommendation. Management stated they revised their MOUs and relevant documents to require agencies to disable users for routine and non-routine personnel actions within stated timelines and will provide written guidance to the agencies. Management expects to complete this work by July 31, 2024.

OIG Comment

We have not verified FinCEN management's corrective actions taken, however the stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

Finding 2 FinCEN Did Not Maintain Sufficient Records of the Dates and Reasons Internal User Accounts Were Disabled

FinCEN did not maintain sufficient historical records of the dates and reasons that internal user accounts were disabled in all cases. Using historical access control system logs, FinCEN generated and provided us a list of 136 internal user accounts that were disabled, some only temporarily, between October 1, 2017, and October 1, 2018. However, FinCEN technicians did not intentionally disable all 136 internal user accounts. Rather, the system repeatedly disabled and re-activated many accounts during this period. Therefore, the list FinCEN provided was not useful for identifying the intentionally disabled accounts in our requested timeframe. In order to identify the date an account was disabled, system administrators must manually search account activity logs. FinCEN employees told us that, "because the logs capture both user-initiated and system-initiated activity performed over time, they are not user-friendly, and can potentially be impacted by outages or other system events [;] these logs can be difficult to interpret over time for historical purposes." Accordingly, FinCEN "cannot provide specific disabled dates for [all internal] users."

The Government Accountability Office's (GAO) *Standards for Internal Control in the Federal Government* (Green Book) Principle 11.01, *Design Activities for the Information System*, states that management should design the entity's information system and related control activities to achieve objectives and respond to risks.[9] Without an accurate record of the dates user accounts were disabled, FinCEN is unable to effectively determine whether the accounts were disabled in a timely manner.

The inability to distinguish between system- and user-initiated actions in the account activity logs and a lack of complete and consolidated records limited the scope of our audit procedures, and we were unable to test or determine whether FinCEN timely disabled all applicable internal accounts. We initially non-statistically selected 62 of the 136 (46 percent) FinCEN internal user accounts that FinCEN employees told us were disabled between October 1, 2017, and October 1, 2018, to determine if FinCEN properly and timely disabled them. Due to FinCEN's system issues, and its inability to identify when all users should have been disabled and to provide related disabled dates, we were unable to determine if all 62 accounts were timely and appropriately disabled. However, we were able to perform testing on employees that departed FinCEN.

FinCEN maintains human resource records related to users that depart FinCEN and those users' accounts should have been contemporaneously disabled. We requested that FinCEN identify which of the 62 users in our sample departed FinCEN.[10] FinCEN personnel told us that 43 of the 62 internal users departed FinCEN between October 12, 2016,[11] and January 30, 2020. For those 43 departed users, we obtained documentation regarding their last day of employment at FinCEN. We manually reviewed system logs capturing account events through January 2020 to test the timeliness of the user accounts' disabled dates compared to their

[9] GAO, *Standards for Internal Control in the Federal Government,* GAO-14-704G, (Sept. 2014), p. 51

[10] We made this request on February 6, 2020, so FinCEN identified all users in our selection that had departed prior to this date. The last departure date for one of these employees before February 6, 2020, was January 30, 2020.

[11] Two users in our sample departed FinCEN prior to October 1, 2017 (start of the scope period for the 62 internal users), and their accounts were disabled and deleted by their respective departure dates; however, the accounts were re-created in the system after the users' departures. The two users were included in our initial sample because their re-created accounts were disabled between October 1, 2017 – October 1, 2018. FinCEN was unable to provide an answer why the accounts needed to be re-created after the users' departures.

respective departure dates. We found that FinCEN personnel did not timely disable all departed internal user accounts (see finding 3). Of the 43 departed users, one account belonged to an individual that was hired, but never on-boarded and her account was set up and disabled on the same date.

We were unable to determine whether FinCEN timely disabled the remaining 19 user accounts. While accounts experienced at least one disabling event between October 1, 2017, and October 1, 2018, the event(s) did not relate to the employees departing and thus FinCEN did not have historical records stating the reason(s) the accounts were disabled. However, we determined that technicians disabled one of the 19 user accounts erroneously (the wrong user's account was disabled). FinCEN subsequently corrected this error.

Recommendation

We recommend that the Director of FinCEN:

1. Determine if a database software update is warranted to accurately capture a historical record of the dates and reasons user accounts are disabled. If warranted, implement the software update; if not warranted, design and implement an alternative tracking method.

Management Response

FinCEN management concurred with our recommendation. Management stated they are replacing their user account management software with a new system, which will allow them to accurately capture historical records. Management expects to complete this work by the end of 2024.

OIG Comment

FinCEN management's stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

Finding 3 FinCEN Did Not Timely Disable Departed Internal User Accounts

FinCEN did not timely disable 6 of 43 (14 percent) internal user accounts that were for departed users, including one account disabled 24 days after the employee left FinCEN. The *FinCEN Portal/Query/FIR – Disabled Account Tickets* SOP required technicians to disable a user's account on the requested date.[12]

FinCEN employees told us that the six accounts identified were not disabled timely due primarily to staff error. In addition, for 2 of 6 accounts that were disabled late, supervisors did not notify technicians that the employees were leaving FinCEN until after their departure, despite FinCEN's *Personnel Separation Process* SOP requiring 2 weeks advance notice. At the time we performed our testing, FinCEN did not require staff to perform a review of disabled accounts, which would have helped ensure supervisors and technicians timely disabled the accounts. Subsequent to our testing, FinCEN employees told us they implemented quarterly and "spot-check" reviews of disabled accounts starting in 2019. However, we noted that, as of March 2023, FinCEN SOPs did not include this review. In addition, the SOP's timeliness metric was not included in FinCEN's *Account Management* guidance, which instructs FinCEN employees on how to disable accounts; this could be a contributing factor to the technicians' delay.

If properly implemented, the quarterly and "spot-check" reviews, as well as a timeliness metric for how promptly to disable user accounts, should mitigate the number of delays and errors that may occur when disabling accounts. Such errors can deprive authorized users of access to the system, resulting in workflow inefficiencies, while delays in disabling user accounts may result in unauthorized users maintaining access to BSA data.

Recommendations

We recommend that the Director of FinCEN:

1. Update the *FinCEN Portal/Query/FIR – Disabled Account Tickets* SOP to add quarterly and "spot-check" reviews of disabled user

[12] For departed employees, the requested date should typically be the employee's last day of employment.

accounts. The reviews should allow FinCEN to determine if supervisors are providing advance notification of departing employees and if technicians are appropriately and timely disabling accounts.

Management Response

FinCEN management concurred with our recommendation. Management stated they plan to update their user access SOPs to include quarterly and spot-check reviews to determine if technicians are appropriately and timely disabling accounts. Management expects to complete this work by the end of 2024.

OIG Comment

FinCEN management's stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

2. Update the *Account Management* guidance to include a timeliness metric for how quickly technicians must disable an account when a user no longer requires access.

Management Response

FinCEN management concurred with our recommendation. Management stated they plan to update their user access SOPs to include a timeliness metric for disabling internal user accounts when users no longer require access. Management expects to complete this work by the end of 2024.

OIG Comment

FinCEN management's stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

Finding 4 FinCEN Did Not Properly Complete Out-processing Forms for Departed Employees

FinCEN did not have sufficient quality control measures in place to ensure supervisors properly out-processed departing employees. FinCEN supervisors did not complete 6 of 42 (14 percent)

out-processing forms for departed employees. Supervisors also did not properly review 23 of the 36 (64 percent) completed forms to ensure that the forms were signed by the proper personnel and dated, as required by FinCEN SOPs. Supervisors also completed 3 of the 36 (8 percent) out-processing forms at least one week after the employees' last day at FinCEN.

FinCEN's *Personnel Separation Process* SOP required supervisors to complete an out-processing form when employees depart FinCEN, and to: (1) review the form to ensure the departing employee and all relevant FinCEN Divisions completed, signed, and dated it; and (2) sign and date the form. This SOP did not specify a timeliness metric for supervisors to complete an out-processing form after an employee departs. Green Book Principle 10.01, *Design Control Activities*, states that management should design control activities to achieve objectives and respond to risks.[13]

When we asked about the issues with out-processing, FinCEN employees told us that regardless of whether out-processing is properly conducted, FinCEN personnel revoke the Personal Identity Verification cards for all departed internal users, which prevents access to FinCEN facilities and systems, including the Portal. We did not attempt to verify the disabling of the Personal Identity Verification cards. Regardless, when out-processing forms are not properly and timely completed, there is an increased risk that departed employees may have unauthorized access to FinCEN resources, including BSA data.

Recommendation

We recommend that the Director of FinCEN:

1. Implement quality control measures, including a timeliness metric for form completion, to ensure supervisors properly review and complete departed employees' out-processing forms.

Management Response

FinCEN management concurred with our recommendation. Management stated they are implementing a more automated

[13] GAO, Green Book, p. 45

process to ensure timely completion of out-processing forms in compliance with their new metrics. Management expects to complete this work by the end of 2024.

OIG Comment

FinCEN management's stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

Finding 5 FinCEN Did Not Require Agencies to Identify Whether Users Received Background Checks

FinCEN did not require agencies to confirm that users received background checks when agencies established user account profiles in FinCEN Portal. We non-statistically selected 104 of the 12,614 FinCEN Portal user accounts active on May 29, 2019. Agencies did not indicate that users received background checks for 49 of the 104 (47 percent) active FinCEN Portal user account profiles we reviewed.

FinCEN's MOUs required that all external users granted direct access to FinCEN Portal had received a satisfactory background investigation. However, FinCEN Portal improperly allowed Agency Coordinators to set up an account and subsequently access the BSA database without checking the "yes" box in the background field. Therefore, agencies are not currently required to affirm that their users have met the background check requirement. As a result, FinCEN cannot easily verify if agencies have investigated users and cleared them to access the BSA database. FinCEN employees told us they plan to conduct a FinCEN Portal system refresh to configure the background check field as mandatory.

Recommendation

We recommend that the Director of FinCEN:

1. Ensure the background check field is mandatory for FinCEN Portal user account profiles. Until the related system update takes effect, design and implement a process to ensure only users with background checks can access BSA data. FinCEN

should also confirm that background checks were completed for all existing users.

Management Response

FinCEN management concurred with our recommendation. Management stated they are updating their application control system to make the background check field mandatory. Management expects to complete this work by the end of 2024. Management stated they have also taken interim steps to manually review all existing and newly established authorized users to ensure they have undergone a background check.

OIG Comment

FinCEN management's stated corrective actions meet the intent of our recommendation. Management should include its stated corrective actions and the expected completion date(s) in JAMES.

* * * * * *

We appreciate the cooperation and courtesies provided to our staff during this audit. If you wish to discuss the report, you may contact me at (202) 607-7851 or Nick Slonka, Audit Manager, at (202) 486-1721. Major contributors to this report are listed in appendix 3.

Gregory J. Sullivan /s/
Audit Director

Appendix 1: Objective, Scope, and Methodology

The objective of our audit was to determine if the Financial Crimes Enforcement Network (FinCEN) manages Bank Secrecy Act (BSA) data access, use, and retention in compliance with laws, regulations, and Department of the Treasury standard operating procedures (SOP). We previously issued an audit report addressing BSA data retention, which specifically addressed suppression. This report addresses FinCEN's management of BSA data access, specifically, granting and revoking access to FinCEN Portal. We plan to issue an additional audit report, the third in the series, addressing BSA data access, including FinCEN's processes for: (1) maintaining a compliant system of records notice, (2) establishing and maintaining memoranda of understanding (MOU) with external agencies that use BSA data, and (3) granting bulk data access. Publication of the fourth and final report, addressing FinCEN's management of BSA data use, specifically FinCEN's monitoring processes, will conclude our audit of FinCEN's management of BSA data. The scope of our audit, related to this report, covered the period from October 2016 through January 2020. We conducted fieldwork related to this report from June 2019 through March 2023.

To accomplish our objective, we reviewed laws, regulations, SOPs, and guidance related to BSA data access, including:

- Titles I and II of P.L. 91-508, Currency and Foreign Transactions Reporting Act (October 26, 1970); codified at 12 U.S.C. 1829b and 1951-1960 and 31 U.S.C. 5311-5314 and 5316-5336 (including notes thereto)
- 31 CFR Chapter X, *Financial Crimes Enforcement Network, Department of the Treasury* (February 3, 2023)
- 31 U.S.C. 310, *Financial Crimes Enforcement Network* (December 27, 2021)
- Government Accountability Office, *Standards for Internal Control in the Federal Government* (GAO-14-704G; Sept. 2014)
- Treasury, Order 180-01, "Financial Crimes Enforcement Network" (January 14, 2020)

- Treasury, Directive 80-05, "Department of the Treasury Records Management" (January 31, 2018)
- FinCEN, *Bank Secrecy Act Information Access Security Plan* (August 10, 2018)
- FinCEN, *Information Systems Security Policy for Access Control* (February 7, 2018)
- FinCEN, *Personnel Separation Process* (January 30, 2014)
- FinCEN, *Inspection Program* (August 19, 2019)
- FinCEN, *Data Access Policy* (March 18, 2014)
- FinCEN, *Query User Manual* (June 2018)
- FinCEN, *Account Management* (n.d.)
- FinCEN, *Roles and Responsibilities of Agency Coordinator and Designated Agency Representative* (n.d.)
- FinCEN, *FinCEN Portal/Query/FIR – Disabled Account Tickets* (June 2019)

We interviewed FinCEN personnel involved in the management of the BSA database, including those from the Strategic Operations Division and Technology Division.

We non-statistically selected 104 of the 12,614 FinCEN Portal user accounts active on May 29, 2019, to determine if FinCEN properly granted access to the BSA database, which included ensuring the:

- user's agency had an MOU with FinCEN;
- user accepted/signed the most recent, required annual *User Acknowledgement* agreement listing the conditions for obtaining and maintaining access to FinCEN Portal between May 2018 and May 2019;
- user completed the most recent, required biennial training between May 2017 and May 2019; and
- Agency Coordinator documented that the user had a proper background check (see finding 5).

To assess the reliability of FinCEN's data used in our active user testing, we analyzed the active accounts listing that FinCEN provided to us for errors in accuracy and completeness and compared the data against corroborating sources. We were not able to verify the list's completeness, but we found the data used

to make our non-statistical selection to be reliable strictly for the purposes of assessing whether the active accounts selected were granted access only if the user's agency had an MOU with FinCEN, a *User Acknowledgement* agreement was signed, training was completed, and a background check was affirmed as completed. Although we were able to document our findings related to active users with the data provided to us (see finding 5), because we could not verify the completeness of the data and our selection was non-statistical, our results cannot be extrapolated to the entire population and are not representative of all active users in FinCEN Portal.

We also initially non-statistically selected 62 of the 136 internal FinCEN user accounts that FinCEN employees told us were disabled, some only temporarily, between October 1, 2017, and October 1, 2018, to determine if FinCEN properly and timely disabled them. However, FinCEN Application Help Desk Technicians did not intentionally disable all 136 internal user accounts. Rather, the system repeatedly disabled and re-activated many accounts during this period. This resulted in a scope limitation as our selection was based on an incomplete and inaccurate list (see finding 2). However, since FinCEN maintains human resource records related to users that depart FinCEN and those users' accounts must be contemporaneously disabled, in February 2020 we requested that FinCEN identify which of the 62 users in our sample departed FinCEN. FinCEN personnel told us that 43 of the 62 internal users departed FinCEN between October 12, 2016, and January 30, 2020.

For those 43 departed users, we obtained documentation regarding their last day of employment at FinCEN and we were able to manually review system logs capturing account events through January 2020 to test the timeliness of the user accounts' disabled dates compared to the employees' respective departure dates. We found that FinCEN personnel did not timely disable all departed internal user accounts (see finding 3).

We were unable to test or determine whether FinCEN timely disabled the remaining 19 accounts of users who had not departed FinCEN because FinCEN personnel were not able to readily identify when, or if, the 19 accounts should have been disabled (see finding 2). While accounts experienced at least one disabling event between October 1, 2017, and October 1, 2018, the event(s) did

not relate to the employees departing and thus FinCEN did not have historical records stating the reason(s) the accounts were disabled. Of the 43 departed users, one account belonged to an individual that was hired but never on-boarded, and her account was set up and disabled on the same date. For the 42 remaining users that departed FinCEN, we also reviewed their out-processing forms to ensure they were properly signed, dated, and reviewed by the appropriate personnel (see finding 4).

To assess the reliability of FinCEN's data used in our disabled user accounts testing, we reviewed the list of disabled accounts and related documentation provided by FinCEN for errors in accuracy and completeness and worked closely with FinCEN employees to discuss the data issues found. We concluded that FinCEN attempted to compile a list of disabled accounts, but because FinCEN employees did not design their system to maintain a historical record of the disabled accounts, or the dates and reasons FinCEN disabled them, the list was incomplete and inaccurate. We determined that the data was not sufficiently reliable to fully conclude on our audit objective as it relates to disabled user accounts, and therefore, we only relied on the data for the purpose of testing departed internal users to ensure (1) their accounts were disabled timely and appropriately and (2) their related out-processing forms were properly completed. We were able to conclude that 6 of 43 departed users were not disabled timely, as stated in finding 3, and 1 of 19 non-departed users was not disabled appropriately, as stated in finding 2. Although we were able to document our findings related to disabled users with the data provided to us (see findings 1 through 4), because the data were incomplete and inaccurate and our sample was non-statistical, our results cannot be extrapolated to the entire population and are not representative of all users in FinCEN Portal.

We did not test if external users were disabled timely and appropriately because external agencies are required to disable their employees' accounts and FinCEN does not receive the documentation necessary for us to complete a test related to disabling external users.

We assessed internal controls and compliance with laws and regulations necessary to conclude on our audit objective. Specifically, we determined that the Information and Communication and Control Activities components in Government

Accountability Office's *Standards for Internal Control in the Federal Government*, including the following principles, were significant to our audit objective as it relates to this report:

- Principle 10: *Management should design control activities to achieve objectives and respond to risks*;
- Principle 11: *Management should design the entity's information system and related control activities to achieve objectives and respond to risks*;
- Principle 12: *Management should implement control activities through policies*; and
- Principle 15: *Management should externally communicate the necessary quality information to achieve the entity's objectives*.[14]

We assessed management's design, implementation, and operating effectiveness of internal controls related to granting access to the BSA database primarily by reviewing FinCEN's SOPs and conducting interviews and tests, as necessary. While we planned to assess management's design, implementation, and operating effectiveness of internal controls related to disabling access to the BSA database, we were unable to perform the intended testing due to the scope limitation explained above. Ultimately, we only tested internal controls related to FinCEN's process of disabling internal accounts for departed employees. Because our review was limited to these aspects of internal control, our audit may not disclose all internal control deficiencies that may have existed at the time of this audit. The internal control deficiencies are stated in the findings of this report.

We conducted this performance audit in accordance with generally accepted government auditing standards, with the exception that we were unable to complete all aspects of our testing due to FinCEN's improperly maintained records. FinCEN was unable to provide us with a complete and accurate listing of the dates that users' accounts were disabled. While we selected and tested accounts identified as disabled during our scope period, we are not reasonably assured that those accounts are representative of the actual population of disabled accounts. Furthermore, we were unable to test whether FinCEN timely disabled all the accounts in

[14] GAO, Green Book, pp. 45, 51, 56, and 62

our sample. Generally accepted government auditing standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained, with the exception of the limitations described, provides a reasonable basis for our findings and conclusions based on our audit objective.

Appendix 2: Management Response

Financial Crimes Enforcement Network
U.S. Department of the Treasury

Office of the Director *Washington, D.C. 20220*

May 17, 2024

Deborah L. Harker
Assistant Inspector General for Audit
Department of the Treasury – Office of Inspector General
1500 Pennsylvania Avenue
Washington, DC 20220

Dear Ms. Harker:

I write regarding the Office of Inspector General's (OIG) draft report entitled *Audit of FinCEN's Management of BSA Data – User Access Report* (Draft Report), which includes OIG's findings for its audit covering the time period from October 2016 through January 2020. The Financial Crimes Enforcement Network (FinCEN) appreciates OIG's efforts to support FinCEN's management of user access to data filed with FinCEN pursuant to the Bank Secrecy Act (BSA) and its implementing regulations.

As you know, FinCEN maintains a statutorily mandated, government-wide data access service that includes reports and records filed with FinCEN pursuant to the Treasury Department's BSA authorities, collectively referred to herein as BSA Data. As set forth in the BSA, these reports and records are highly useful in a range of governmental efforts to combat money laundering and other forms of illicit finance, including, but not limited to, criminal, tax, or regulatory investigations; intelligence or counterintelligence activities, including analysis, to protect against terrorism; and facilitation of the tracking of money that has been sourced through criminal activity or is intended to promote criminal or terrorist activity. FinCEN maintains these reports and records in its BSA System of Record, also referred to herein as the "BSA Systems."

As part of its management of BSA Data, FinCEN provides BSA data access to authorized users—both FinCEN employees and authorized individuals from intelligence, law enforcement, and regulatory agencies (Agencies). FinCEN provides such access consistent with the BSA, FinCEN's implementing regulations, and Memoranda of Understanding (MOU) that Agencies enter into with FinCEN before accessing BSA data. FinCEN is committed to ensuring that its management of user access to the BSA Systems complies with all relevant laws, regulations, policies, and procedures. As such FinCEN considers rigorous oversight of its user access management efforts to be a critical aspect of FinCEN's mission. FinCEN agrees that the eight

recommendations set forth in the draft report will improve FinCEN's management of BSA Data. As explained below, FinCEN has already implemented or is in the process of implementing these recommendations.

The first three recommendations generally call for FinCEN to evaluate its policies and procedures relating to disabling user accounts for external agency users, and to implement appropriate updates to those policies and procedures as well as corresponding internal controls to ensure these policies and procedures are timely followed. FinCEN has taken several steps to implement these recommendations and anticipates completing this work by July 31, 2024. Specifically, FinCEN has revised the relevant MOU documents to distinguish between routine and non-routine personnel actions. The revised MOU documents also explicitly require Agencies to disable users within stated timelines for both routine and non-routine causes, as well as provide notification for disablement due to non-routine causes to FinCEN within stated timelines. FinCEN has also updated internal SOPs to verify that these timelines are being adhered to and take appropriate remedial action if required. FinCEN is finalizing updates to the relevant documents and anticipates communicating these changes to the Agencies through written guidance in the coming weeks.

Recommendations four through seven generally call for FinCEN to evaluate its policies and procedures relating to internal FinCEN employee access to BSA Data, particularly with respect to timely disabling of user accounts. FinCEN is in the process of implementing these recommendations. FinCEN anticipates that system updates and capabilities described below relating to recommendations four through seven will be implemented in the next several months. In conjunction with these updates, FinCEN will implement appropriate SOPs relating to these upgrades. Unless otherwise noted below, FinCEN anticipates the updates and related SOPs will be finalized by the end of 2024. We note that these enhancements will serve as additional safeguards of BSA Data over and above FinCEN's existing security measures, which require that access to all FinCEN facilities and systems, including the BSA Portal and all BSA applications, be removed upon the revocation of an individual's PIV card.

Regarding recommendation four, FinCEN is in the process of fully replacing the Identity Management and Access Control System software (for user account management) with a new system as part of its overall migration to Multi-Factor Authentication (MFA) and cloud-based systems. In the new system, additional fields have been added to permit FinCEN to track the reasons for user disablement. In addition, in the new system, accounts inactive after 90 days are automatically deleted. All changes to user accounts will be captured by the new system in system logs. FinCEN is also in the process of updating its policies for internal FinCEN user account management unrelated to off-boarding to ensure that FinCEN's SOPs for internal user disablement are consistent with the standards and procedures imposed on our third-party Agency users described above and anticipates these policies will be implemented by July 31, 2024.

Ms. Deborah L. Harker, Assistant Inspector General for Audit
May 17, 2024

With respect to recommendations five and six, helpdesk user access SOPs will be updated to include: (1) a timeliness metric for disablement of internal user accounts when an internal user no longer requires access; and (2) quarterly and spot-check reviews to determine if technicians are appropriately and timely disabling accounts.

To address the concerns identified in recommendation seven, FinCEN is also working with the Administrative Resource Center's HR Connect Program Office to implement a more automated employee offboarding capability in HR Connect intended to replace some existing paper processes. Specifically, under the new automated process, the system will (when FinCEN has greater than fourteen days' advance notice from an employee of departure) automatically generate emails on the fourteenth day prior to the employee's effective departure date to all affected divisions with offboarding responsibilities (including but not limited to account disablement).[1] In addition, if the system has not received a fully completed, digitally signed offboarding form three days after the employee's effective date of departure, the system will generate additional emails to the affected divisions to help ensure timely completion.

Recommendation eight calls for FinCEN to revise its procedures to ensure that all authorized agency users have completed a background check and indicated as such to FinCEN prior to accessing BSA Data. FinCEN is in the process of implementing this recommendation. As part of its MOUs with Agencies, FinCEN requires all authorized users who access BSA Data to have undergone a background check. FinCEN relies on Agencies to ensure, via a designated Agency Coordinator, that this requirement is met and to timely notify FinCEN of compliance with this requirement when establishing new user accounts. FinCEN is currently updating the system that controls access to FinCEN applications. As part of this update, populating the existing background check field for each authorized user will be mandatory, and the Agency Coordinator will be required to indicate on a user-by-user basis that each authorized user has completed a background check before they are able to access BSA Data. This update should be completed by the end of 2024. While this update is underway, FinCEN has also taken interim steps in the current system to manually review the background check field for all existing and newly established authorized users and worked with Agency Coordinators to ensure that each authorized user has undergone a background check.

We appreciate the opportunity to comment on the Draft Report, and we look forward to continuing to work with your office on the remaining aspects of your BSA data management

[1] In the event that FinCEN has less than fourteen days' advance notice of an employee's departure, the system will immediately generate the emails to affected divisions with offboarding responsibilities.

Ms. Deborah L. Harker, Assistant Inspector General for Audit
May 17, 2024

audit efforts. Proper management of the data filed with FinCEN pursuant to the BSA and its implementing regulations is vital to FinCEN's mission to protect the U.S. financial system from illicit finance threats while enhancing the public's confidence in the management and oversight of BSA data.

Sincerely,

Jimmy Kiley for Andrea Gacki

Andrea Gacki
Director, Financial Crimes Enforcement Network

4

Appendix 3: Major Contributors to This Report

Nick Slonka, Audit Manager
Justin Summers, Auditor-in-Charge
Gerald Kelly, Auditor
Darren Wright, Auditor
Mark Humboldt, Referencer

Appendix 4: Report Distribution

Department of the Treasury

Secretary
Deputy Secretary
Under Secretary, Office of Terrorism and Financial Intelligence
Office of Strategic Planning and Performance Improvement
Office of the Deputy Chief Financial Officer, Risk and Control Group

Financial Crimes Enforcement Network

Director
Office of Inspector General Audit Liaison

Office of Management and Budget

Office of Inspector General Budget Examiner

U.S. Senate

Chairwoman and Ranking Member
Committee on Appropriations

Chairman and Ranking Member
Committee on Banking, Housing, and Urban Affairs

Chairman and Ranking Member
Committee on Finance

Chairman and Ranking Member
Select Committee on Intelligence

U.S. House of Representatives

Chairwoman and Ranking Member
Committee on Appropriations

Chairman and Ranking Member
Subcommittee on Oversight and Investigations
Subcommittee on National Security, Illicit Finance, and International Financial Institutions
Committee on Financial Services

Chairman and Ranking Member
Permanent Select Committee on Intelligence

This Page Intentionally Left Blank

REPORT WASTE, FRAUD, AND ABUSE

Submit a complaint regarding Treasury OIG Treasury Programs and Operations using our online form: https://oig.treasury.gov/report-fraud-waste-and-abuse

TREASURY OIG WEBSITE

Access Treasury OIG reports and other information online: https://oig.treasury.gov/