Office of Inspector General | United States Postal Service

Audit Report

U.S. Postal Inspection Service Oversight of Its Use of Cryptocurrency

Report Number 21-067-R21 | August 26, 2021

Table of Contents

Cover
Highlights....1
Objective....1
Findings....1
Recommendation....2
Transmittal Letter....3
Results....4
Introduction/Objective....4
Background....4
Investigative Use of Cryptocurrency....4
Cryptocurrency Seizure and Forfeiture....5
Findings Summary....5
Finding #1: Use of the Cryptocurrency Fund Program....6
Recommendation #1....6
Finding #2: Cryptocurrency Transaction Data....7
Recommendation #2....8
Finding #3: Cryptocurrency Training Program....8
Recommendation #3....8
Finding #4: National Cryptocurrency Fund Management....9
Recommendation #4....10
Management's Comments....10
Evaluation of Management's Comments....10
Appendices....11
Appendix A: Additional Information....12
Objective, Scope, and Methodology....12
Appendix B: Cryptocurrency Background....13
What is Cryptocurrency?....13
How is Cryptocurrency Acquired?....13
How is Cryptocurrency Stored?....13
How Does Cryptocurrency Work?....13
Appendix C: Management's Comments....15
Contact Information....18

Highlights

Objective

Our objective was to evaluate the effectiveness of U.S. Postal Inspection Service policies and procedures for managing cryptocurrency in its law enforcement activities.

Cryptocurrency is a decentralized form of digital currency that uses a blockchain, or public ledger, to record transactions. The anonymity of cryptocurrency transactions and the significant fluctuations in the value of cryptocurrency create opportunities for abuse or theft when used during law enforcement activities. We evaluated the Postal Inspection Service's use and seizure of cryptocurrency in cases closed in fiscal years (FY) 2019 and 2020. The Postal Inspection Service established the Cryptocurrency Fund Program (the Program) in 2017 to establish standards and policies to account for cryptocurrency transactions and reduce operational risk.

The [redacted] (the Application) is the system used to account for cryptocurrency requested through the Program for use during an investigation, such as when an inspector purchases illegal narcotics through an online marketplace. In FYs 2019 and 2020, the Postal Inspection Service closed nine cases that used cryptocurrency managed under the Program. During this time, the Postal Inspection Service closed four additional cases in which postal inspectors seized cryptocurrency as evidence.

Findings

Overall, we found that the Postal Inspection Service is sufficiently managing seized cryptocurrency by recording seized assets and collecting proceeds of sale. However, opportunities exist to improve its management of cryptocurrency used for investigative purposes.

Postal inspectors are not required to go through the Program to request cryptocurrency for investigative use. This occurs because the Program only supports [redacted] of cryptocurrency. When an inspector does not use one of the [redacted] of cryptocurrency managed under the Program, the funds are requested through the traditional investigative funds process. In these instances, it is the discretion of the team leader to inform the Cryptocurrency Fund Program manager (the Program manager) that some other type of cryptocurrency is being used for investigative purposes. However, this notification is not always done, and the Program manager does not have oversight of these cases. This limits the Program's ability to effectively reduce the operational risk associated with cryptocurrency use.

We also found there are inaccuracies in the data in the Application's *Transaction Review Report*. The purpose of the report is to show cryptocurrency transactions associated with a particular case. Because of the way the report obtains information from the Application, the report contains duplicate transactions and transactions unrelated to the case being queried. As a result of these data integrity issues, the *Transaction Review Report* cannot be used to accurately track and manage cryptocurrency transactions or to assist in validating the final balance of funds for each case.

Further, the Postal Inspection Service does not have a comprehensive cryptocurrency training program for postal inspectors. Internal guidance states that postal inspectors must be approved to conduct undercover operations and training must be completed prior to requesting cryptocurrency funds. However, the guidance does not specify what training courses should be taken or how frequently refresher training is required.

Because of the lack of standardized training, we found that two of the nine cases in our scope were only opened to support on-the-job cryptocurrency training. Postal inspectors used undercover identities and completed purchases during this training but did not comply with existing guidance. For example, postal inspectors transferred cryptocurrency between one another, which is prohibited by the guidance. Without a comprehensive training program, the Postal Inspection Service is at increased risk while using cryptocurrency to support investigations.

Finally, the Postal Inspection Service guidance does not include documented procedures related to certain aspects of the headquarters' management of cryptocurrency. Specifically, there are no procedures in the guidance that detail the process for purchasing cryptocurrency for the national wallet which stores the Program's cryptocurrency, the amount of cryptocurrency that should be

maintained in the national wallet, how to reconcile transactions, or how to conduct an annual review of the account.

Documentation of internal controls provides a means to retain organizational knowledge, to ensure operational needs are met, and to minimize risk. By developing such procedures, the Postal Inspection Service will help ensure the program's objectives will be met.

Recommendation

We recommended management:

- Ensure that the Cryptocurrency Fund Program has the information needed to provide oversight of the investigative use of cryptocurrency.
- Modify the [redacted] to ensure duplicates and unrelated transactions are not included in the *Transaction Review Report* and that the report provides sufficient information to differentiate between transactions.
- Develop a comprehensive cryptocurrency training program.
- Develop written procedures for the management and oversight of the national wallet and its associated exchange account.

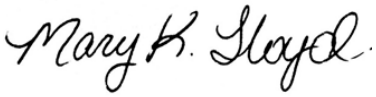
Transmittal Letter

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

August 26, 2021

MEMORANDUM FOR: GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

CRAIG GOLDBERG
DEPUTY CHIEF POSTAL INSPECTOR, HEADQUARTERS



FROM: Mary Lloyd
Acting Deputy Assistant Inspector General
for Inspection Service and Cybersecurity & Technology

SUBJECT: Audit Report – U.S. Postal Inspection Service Oversight of Its Use of Cryptocurrency (Report Number 21-067-R21)

This report presents the results of our audit of the U.S. Postal Inspection Service's Oversight of Its Use of Cryptocurrency.

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Elizabeth Kowalewski, Director, Inspection Service, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the U.S. Postal Inspection Service's Oversight of Its Use of Cryptocurrency (Project Number 21-067). Our objective was to evaluate the effectiveness of the U.S. Postal Inspection Service's policies and procedures for managing cryptocurrency in its law enforcement activities. See Appendix A for additional information about this audit.

Background

The mission of the U.S. Postal Inspection Service is to support and protect the Postal Service and its employees, infrastructure, and customers; enforce the laws that defend the nation's mail system from illegal or dangerous use; and ensure public trust in the mail. To support its mission, postal inspectors may use cryptocurrency while conducting investigations online and may seize cryptocurrency as evidence during an investigation. Cryptocurrency is a decentralized form of digital currency that uses a blockchain, or ledger, to record transactions. The anonymity of cryptocurrency transactions and the significant fluctuations in the value of cryptocurrency create opportunities for abuse or theft when used during law enforcement activities. For additional information about cryptocurrency and the blockchain, see Appendix B.

> *"To support its mission, postal inspectors may use cryptocurrency while conducting investigations online."*

Investigative Use of Cryptocurrency

The U.S. Postal Inspection Service established the Cryptocurrency Fund Program (the Program) in 2017 to account for cryptocurrency transactions[1] and reduce operational risk to individual inspectors and the organization through its policies and standards. The Program also serves as a centralized point for purchasing cryptocurrency within the Postal Inspection Service and is designed to minimize challenges associated with managing cryptocurrency value fluctuations.[2] Guidance related to the Program's mission and governance is outlined in the *Cryptocurrency Fund Program Guide* (Program Guide).

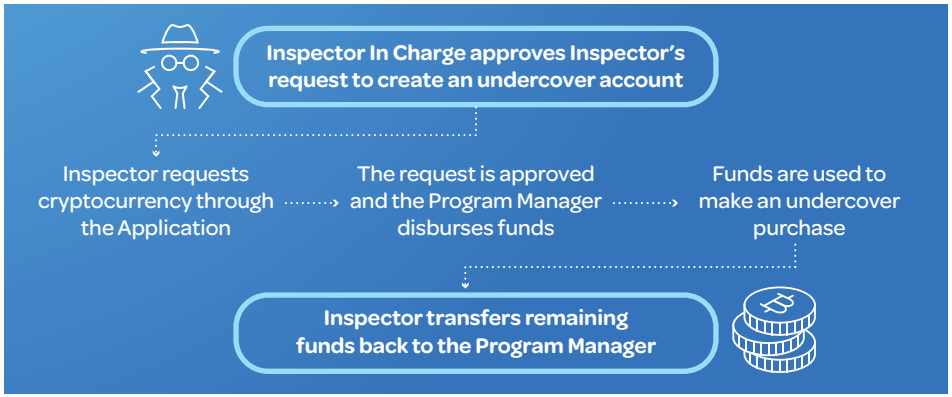
The Postal Inspection Service identified nine cases closed in FYs 2019 and 2020 that requested cryptocurrency through the Program for investigative purposes, such as purchasing illegal narcotics through an online marketplace. In these nine cases, postal inspectors requested about [redacted].[3] The Cryptocurrency Fund Program manager (the Program manager) is responsible for maintaining a centralized exchange account and national wallet, which stores the Program's cryptocurrency. These are used to disburse cryptocurrency to the individual wallets of postal inspectors for investigative use. For additional information about cryptocurrency wallets and exchanges, see Appendix B.

To facilitate and account for cryptocurrency transactions, including transfers between wallets and purchases made with cryptocurrency, the Program established the [redacted] (the Application) within the Case Management System (CMS). The Application stores inspectors' cryptocurrency wallet information, monitors transactions, and enables reporting. Within the Application, postal inspectors submit requests for cryptocurrency intended for investigative use, which includes information about the inspector's cryptocurrency exchange account and wallet that will be used for the case. The Application tracks all cryptocurrency activity associated with an inspector's exchange account by cross-referencing the public blockchain daily. Tracked activity includes disbursements of funds to postal inspectors from the Program's national wallet and purchases made in online marketplaces. Guidance related to the use of the Application is detailed in the *Cryptocurrency Program Application User Guide* (the User Guide).

1 Includes the initial acquisition of cryptocurrency, disbursement of cryptocurrency to postal inspectors, investigative purchases made by postal inspectors, and the return of excess funds.
2 For example, at the beginning of fiscal year (FY) 2019 (October 2018) [redacted] was valued at about [redacted]. By February 2019, the value had dropped to [redacted]. By June 2019, the value increased to about [redacted] and by April 2021, a [redacted] was valued at more than [redacted].
3 Cryptocurrency Fund Program records do not convert cryptocurrency to U.S. dollars. Based on the average exchange rate of [redacted] in FYs 2019 and 2020, we estimate [redacted] were worth $20,212 during the scope of the audit.

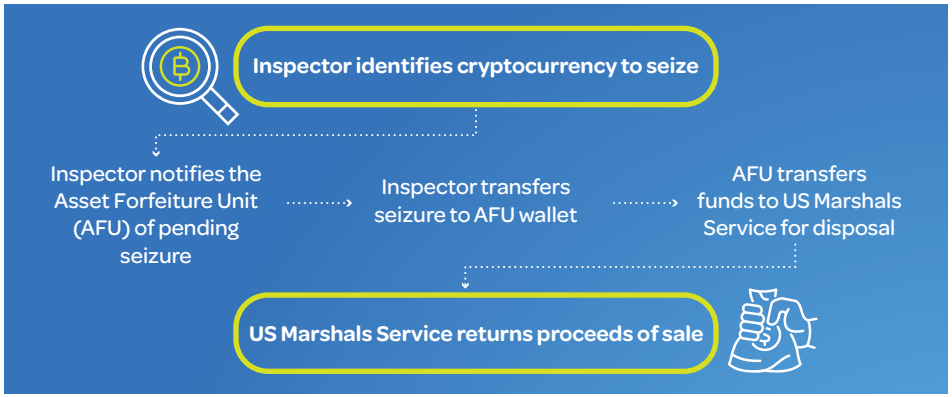
Figure 1 describes the process for requesting and using cryptocurrency through the Program.

Figure 1. Investigative Use of Cryptocurrency Process



Source: OIG summary of the Inspection Service's *Cryptocurrency Program Management Guide*, dated August 2019.

Figure 2. Cryptocurrency Seizure Process



Source: OIG summary of the Inspection Service's *Cryptocurrency Program Management Guide*, dated August 2019.

Cryptocurrency Seizure and Forfeiture

In FYs 2019 and 2020, the Postal Inspection Service identified four closed cases where postal inspectors seized cryptocurrency as evidence during an investigation. Postal inspectors seized [redacted] in these four cases.[4] The Program does not manage the cryptocurrency seizure process. The Postal Inspection Service's Asset Forfeiture Unit (AFU) provides oversight and guidance for the process of seizing cryptocurrency, as described in Figure 2.

Findings Summary

Overall, the Postal Inspection Service's management of seized cryptocurrency, including the recording of seized assets and the collection of proceeds of sale, is sufficient.[5] However, we found that opportunities exist to improve its management of cryptocurrency used for investigative purposes. Specifically, we found that the use of the Program is not required when requesting cryptocurrency for investigative support. We also found that the Application's *Transaction Review Report* contains inaccurate data associated with cryptocurrency transactions. Finally, we found that the Postal Inspection Service does not have a comprehensive training program for the use

> *"We found that opportunities exist to improve Inspection Service management of cryptocurrency used for investigative purposes."*

4 When cryptocurrency is seized, inspectors are required to record the value of the cryptocurrency at the time of seizure. The recorded value of the cryptocurrency at the time of seizure was about $62,000.
5 We identified a minor error in the documentation process for cryptocurrency seizures, but it did not result in the breakdown of the seizure process. Therefore, this error did not rise to the level of a finding that warranted management's attention.

of cryptocurrency in investigations and existing guidance does not clearly outline procedures associated with the national wallet.

Finding #1: Use of the Cryptocurrency Fund Program

We found that while the Postal Inspection Service created the Program in 2017 to account for cryptocurrency transactions and reduce operational risk associated with the investigative use of cryptocurrency, postal inspectors are not required to use the program when requesting cryptocurrency to support investigations. The Program's cryptocurrency exchange account supports the distribution and use of [redacted] cryptocurrency: [redacted].[6] These types of cryptocurrency are sufficient for most investigative needs and, according to the Program manager, if an inspector wants to use these types of cryptocurrency, they will generally go through the Program because it simplifies the process.

However, according to the Program manager, there are legitimate circumstances in which cryptocurrency can be obtained for investigative use outside of the Program. Specifically, postal inspectors may occasionally require the use of different types of cryptocurrency in their investigations. For example, some vendors may only accept payment in the form of [redacted] a type of private cryptocurrency not supported by the Program. In such cases, postal inspectors would request standard investigative funds in the form of U.S. dollars. The approval and distribution of these funds occur at the division level and the inspector is personally responsible for exchanging the dollars for cryptocurrency. Because any unused funds must be returned as U.S. dollars, the inspector must also be able to account for fluctuations in the value of the cryptocurrency to ensure the proper amount is returned.

According to the manager, if a different type of cryptocurrency is obtained outside of the Program for operations, the postal inspector's team lead should notify the Program manager. However, notifying the Program manager is not required by existing guidance and is not always done. As a result, the Program manager does not have oversight of these cases, and management could not readily identify how many cases used cryptocurrency outside of the Program. Therefore, the Program cannot account for the total amount of cryptocurrency used for investigative purposes across the Postal Inspection Service. To better understand how many cases could potentially involve cryptocurrency use outside of the Program, we conducted a keyword search of the CMS for various cryptocurrency-related terms. This search resulted in 1,064 unique case numbers, each of which would have to be reviewed manually to determine whether cryptocurrency had been used for investigative purposes.[7]

The *Standards for Internal Control in the Federal Government* state that management should receive quality information that flows up reporting lines from personnel to help achieve the entity's objectives.[8] Thus, the Program manager requires quality information about cryptocurrency use to ensure the Program accomplishes its objectives. Without this information, the Program's ability to effectively reduce the operational risk associated with cryptocurrency use is limited. In particular, the Program is unable to carry out one of its primary purposes—to help postal inspectors manage the challenges associated with cryptocurrency's inherent volatility—which ultimately leaves the Postal Inspection Service susceptible to theft, abuse, and mismanagement of federal funds.

Recommendation #1

We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, ensure that the Cryptocurrency Fund Program has the information needed to provide oversight of the investigative use of cryptocurrency.

6 According to the Program manager, the Program limits its support to [redacted] cryptocurrency because the Application verifies each transaction against the blockchain every 24 hours. Each type of cryptocurrency has its own blockchain with its own protocols that must be integrated into the Application to ensure the reliability of the daily verifications.

7 Anytime a cryptocurrency-related term is included in a case file, that case would appear in the search results. Consequently, cases are included in these search results for many reasons other than cryptocurrency use by an inspector.

8 *Standards for Internal Control in the Federal Government* (Report Number GAO-14-704G, Section 14.04, dated September 10, 2014). While the Postal Service is not subject to the requirements of Federal Managers' Financial Integrity Act (FMFIA) of 1982 (31 U.S.C. §3512), the *Standards for Internal Control in the Federal Government* can be used as the framework for establishing and maintaining an effective internal control system and may be adopted by state, local, and quasi-government entities, as well as not-for-profit organizations.

Finding #2: Cryptocurrency Transaction Data

We found that the Application's *Transaction Review Reports* contain inaccurate data associated with cryptocurrency transactions. Specifically, we found evidence of missing, duplicate, and unrelated transactions when querying transactions for the cases in our scope.

Based on the review of the nine cases within our scope, we found:

- One of the cases we reviewed had no transactions in the report, but the case file in the CMS contained supporting documentation for three transactions;
- Ninety-two of the 212 (44 percent) cryptocurrency transactions contained in the report appear to be duplicate transactions recorded under unique payment identification numbers; and
- Twenty of the 212 (9 percent) cryptocurrency transactions we reviewed were not related to the queried case.

The Application User Guide encourages postal inspectors, team leaders, division leaders and the manager to use the *Transaction Review Report* to track and manage transactions within their cases. The *Standards of Internal Control in the Federal Government* state that management must use quality information to achieve the entity's objectives. Specifically, management must obtain relevant data from reliable internal and external sources. This data should be reasonably free from error and bias to help management perform monitoring activities.[9]

According to the National Inspection Service Analytics team, if an inspector incorrectly enters their account information, transactions associated with that account would not appear in the *Transaction Review Report* even though funds would still be available for use. The Postal Inspection Service addressed this issue in May 2020 by creating a system-generated error message when an inspector enters invalid account information into the application. This error message will not allow an inspector to proceed with entering transaction information until the invalid account information is corrected.

In September 2019, an inspector informed the National Inspection Service Analytics team of the appearance of duplicate transactions in the *Transaction Review Report*. These potential duplicates included identical dates, wallet addresses, transaction amounts, and descriptions. According to the Program manager and analytics team, these transactions appear identical because of the limited information the Application includes in the *Transaction Review Report*. According to management, they have additional information which allows them to manually remove duplicate transactions before reconciling accounts. However, the duplicates still affect the balance presented in the *Transaction Review Report.*

Additionally, according to the Program manager and the analytics team, the *Transaction Review Report* may contain transactions from other cases because it pulls information from the inspector's exchange account, rather than an individual wallet within that account.[10] In February 2020, the Application's developers implemented a new drop-down field in the Application that allows the inspector to indicate that a transaction is not related to the case. However, the Program manager stated that inspectors do not always use the drop-down option. Further, when the drop-down field is used, the unrelated transactions are still included in the *Transaction Review Report* final balance.

Because of the data integrity issues in the *Transaction Review Report*, it cannot be used to accurately track and manage cryptocurrency transactions or to assist in validating the final balance of funds for each case. Postal Inspection Service management provided the team with a list of nine cases within our scope showing that postal inspectors requested [redacted]. Based on the average value of [redacted] during the scope of the audit, this equals $20,212

> *"Because of the data integrity issues in the Transaction Review Report, it cannot be used to accurately track and manage cryptocurrency transactions."*

9 *Standards for Internal Control in the Federal Government* (Report Number GAO-14-704G, Sections 13.01 and 13.04, dated September 10, 2014).
10 To receive and use cryptocurrency, each inspector must set up an exchange account in which they have multiple wallets. An inspector may use different wallets in different cases, but these are connected to the same exchange account. See Appendix B for additional information on exchange accounts and wallets.

worth of transactions.[11] By modifying the Application to ensure the integrity of the data in the *Transaction Review Report*, the Postal Inspection Service will be better positioned to minimize the risk of theft, abuse, and mismanagement of cryptocurrency.

Recommendation #2
We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, modify the [redacted] to ensure duplicates and unrelated transactions are not included in the *Transaction Review Report* and that the report provides sufficient information to differentiate between transactions.

Finding #3: Cryptocurrency Training Program

We found that the Postal Inspection Service does not have a comprehensive cryptocurrency training program for inspectors. The User Guide and the Program Guide state that undercover training must be completed by any postal inspector requesting cryptocurrency funds before the funds will be disbursed. However, the guidance does not specify what training courses should be taken or how frequently refresher training is required. According to Postal Inspection Service officials, the Career Development Unit offers a basic and advanced Online Undercover Operations Training course; however, these courses are not required nor are they offered regularly. Additionally, the specific course is not referenced in documented guidance and cryptocurrency management is only a portion of the material covered in the course.[12]

> *"We found that the Postal Inspection Service does not have a comprehensive cryptocurrency training program for inspectors."*

Because of the limited cryptocurrency-related training provided by the Postal Inspection Service, we found that two of the nine cases that management identified as using cryptocurrency were only opened to facilitate cryptocurrency training. Specifically, two divisions opened area cases to conduct on-the-job training courses in which trainees utilized cryptocurrency to make purchases of narcotics. Postal Inspection Service management was unable to provide documentation that 21 of 23 inspectors who made undercover purchases as part of these two cases were authorized to do so.

Additionally, when reviewing the case files associated with the two training cases, we found evidence that several of the guidelines and procedures for managing cryptocurrency during investigative use were not followed.[13] Specifically, we noted that:

- Cryptocurrency was transferred between postal inspectors;
- Transactions sometimes did not have supporting documentation in CMS, such as screenshots; and
- Transactions did not include a transaction description.

These requirements were developed to protect the Postal Inspection Service from the risk of fraud, mismanagement, and compromised investigations. Without establishing a comprehensive training program that incorporates cryptocurrency requirements, the Postal Inspection Service exposes itself to increased risk during the investigative use of cryptocurrency. If inspectors are untrained or trained in methods that do not reflect documented guidance, the likelihood of theft, abuse, and compromised undercover investigations remains high.

Recommendation #3
We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, develop a comprehensive cryptocurrency training program.

11 To determine the value of [redacted] for FYs 2019 and 2020, we took the average exchange rate of [redacted] during FYs 2019 and 2020 and applied it to the [redacted] requested. The average exchange rate of one [redacted] was worth [redacted]
12 The Online Undercover Operations Training course teaches postal inspectors how to use different tools for Dark Web investigations.
13 Due to reliability concerns with the *Transaction Review Report* noted in Finding #2, we could not determine the extent of these issues.

Finding #4: National Cryptocurrency Fund Management

The Postal Inspection Service's cryptocurrency guidance does not include documented procedures in place related to certain aspects of managing the national wallet or how to conduct an annual review of the national wallet. The Program Guide and the User Guide define the procedures that postal inspectors must follow when requesting and using cryptocurrency to support investigations, such as documenting the information that must be incorporated into the cryptocurrency ledger and identifying the documentation that must be stored to support each cryptocurrency transaction. However, the guidance does not contain procedures that the Program manager must follow when managing the national wallet and its associated exchange account. Specifically, existing guidance does not identify requirements associated with (1) purchasing cryptocurrency for the national wallet, (2) the amount of cryptocurrency that should be maintained in the wallet, (3) verifying national wallet transactions, or (4) conducting an annual review.

The *Standards for Internal Control in the Federal Government* state that documentation of internal controls provides a means to retain organizational knowledge and ensure operational needs are met.[14] The *Standards* also highlight the importance of documenting internal controls to assist management with identifying deficiencies on a timely basis and designing appropriate corrective actions.[15]

According to the Program manager, the national wallet is legally considered to be an investigative fund subject to the existing investigative fund policies and procedures in the *Inspection Service Manual*. While these policies and procedures outline the process for establishing an investigative fund, they do not include specific information related to purchasing cryptocurrency with investigative funds, managing the national wallet to maintain a certain level of funds, or verifying national wallet transactions.[16] These policies and procedures are unique to the roles and responsibilities of the Cryptocurrency Fund Program manager and are not documented in the *Inspection Service Manual* or the Program's documented guidance.

Similarly, while the Program Guide and the User Guide state that the Program manager, an appointed cryptocurrency auditor, and an independent postal inspector should conduct the annual national wallet review, the guidance does not provide additional procedural guidance for how to conduct this review. For instance, the guidance does not include documented procedures for choosing the independent postal inspector or what evidentiary documentation should be analyzed during the review. The FYs 2019 and 2020 reviews include a description of documentation and review procedures followed by the auditor, but they are inconsistent. According to the Inspection Service, the procedures in the FY 2020 report are now considered the standard procedures to be used for the annual review.[17] However, these procedures are not documented in or referenced by Program guidance.

The Program manager is responsible for drafting all procedures associated with the Program. Because the Program manager is also solely responsible for the management of the national wallet and its exchange account, the Postal Inspection Service did not find it necessary to document procedures pertaining to the manager's role. Further, because review procedures are not documented in the Program guidance, there may be a lack of consistency in the quality of the review, potentially exposing the Postal Inspection Service to theft, abuse, and mismanagement of funds.

Well-documented procedures will help ensure that the Program's objectives can be met and will provide reasonable assurance that national wallet cryptocurrency controls are operating effectively and minimizing risk.

The Program manager agreed that documenting such procedures would be beneficial and stated that he would begin drafting them.

14 *Standards for Internal Control in the Federal Government* (Report Number GAO-14-704G, dated September 10, 2014), Sections 3.10 and 3.11.
15 *Standards for Internal Control in the Federal Government* (Report Number GAO-14-704G, dated September 10, 2014), Section OV4.08, para. 17.05.
16 Section 2.6.2.3 of the *Inspection Service Manual*, dated October 2020, outlines the process for obtaining investigative funds.
17 Although FY 2021 is outside of the scope of this audit, the Inspection Service provided the Annual Review for FY 2021 for our review. We found that the review followed the same procedures as the FY 2020 Annual Review.

Recommendation #4

We recommend that the **Postal Inspector in Charge, Analytics and Cybercrime**, develop written procedures for the management and oversight of the national wallet and its associated exchange account.

Management's Comments

Management agreed with all recommendations in the report. They also agreed with findings 2, 3, and 4. Management partially agreed with finding 1.

Regarding finding 1, management did not agree that the Program is unable to help Postal Inspectors manage the challenges inherent with the volatility of cryptocurrency. They stated that existing controls mitigate the risks for cryptocurrency transactions that take place within the Cryptocurrency Fund Program and within the Investigative Funds Program. However, management did agree with the need for the Program manager to be made aware of all cryptocurrency transactions regardless of funding source.

Regarding recommendation 2, management stated that as of July 30, 2021, they modified the [redacted] to ensure that duplicates and unrelated transactions are not in the *Transaction Review Report* and that the report provides sufficient information to differentiate between transactions.

See Appendix C for management's comments in their entirety.

Evaluation of Management's Comments

OIG considers management's comments responsive to the recommendations in the report.

Regarding finding 1, management could not provide us with the number of cases that used cryptocurrency outside of the Program. As we noted in this report, this demonstrated limitations in their oversight.

Regarding recommendation 2, management did not provide documentation that supports that they implemented the recommendation on July 30, 2021. Management provided a revised target implementation date of September 30, 2021.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information 12
Objective, Scope, and Methodology 12
Appendix B: Cryptocurrency Background 13
What is Cryptocurrency? 13
How is Cryptocurrency Acquired? 13
How is Cryptocurrency Stored? 13
How Does Cryptocurrency Work? 13
Appendix C: Management's Comments 15

Appendix A: Additional Information

Objective, Scope, and Methodology

The scope of our audit included a review of cases closed in FYs 2019 and 2020. We reviewed the Postal Inspection Service's management of cryptocurrency through the Program in support of investigations, including the Program's acquisition, disbursement, and reconciliation of cryptocurrency. We also reviewed the Postal Inspection Service's management of cryptocurrency seizures.

To accomplish our objective, we:

- Obtained and analyzed policies, procedures, and guidance pertaining to the management of the Program and the seizure of cryptocurrency to identify and document management controls.
- Interviewed relevant officials including the Assistant Inspector-in-Charge of the Analytics and Cybercrime Group, the Cryptocurrency Fund Program manager, the Asset Forfeiture Program manager, and the Management Analyst in the Inspection Service's Asset Forfeiture Unit to gain an understanding of their roles and responsibilities in managing cryptocurrency.
- Reviewed cases closed in FYs 2019 and 2020 that used cryptocurrency and assessed compliance with identified management controls.
- Obtained supporting documentation for cases closed in FYs 2019 and 2020 where cryptocurrency was seized to assess compliance with identified controls.
- Obtained and reviewed cryptocurrency-related training requirements for postal inspectors.

We conducted this performance audit from March through August 2021, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management July 28, 2021, and included their comments where appropriate.

We assessed the reliability of the Application's *Transaction Review Report*, which contains cryptocurrency transaction data for the nine cases in our scope, by tracing entries to source documents and conducting tests to identify missing, duplicate, and illogical data. As reported in finding 2, we determined that the data contained in the *Transaction Review Report* were not sufficiently reliable for the purposes of this report.

The OIG did not identify any prior audits or reviews related to the objective of this audit within the last five years.

Appendix B: Cryptocurrency Background

What is Cryptocurrency?

Cryptocurrency is a type of virtual currency that can be used to pay for goods and other services. The Internal Revenue Service has described virtual currency as a digital representation of value that functions as a medium of exchange, a unit of account, or a store of value. Most cryptocurrencies are decentralized or peer-to-peer based, meaning they lack a central administrator, such as a bank, to issue currency and maintain payment ledgers.

How is Cryptocurrency Acquired?

Cryptocurrency can be acquired through a cryptocurrency ATM, directly from a cryptocurrency holder, through an online exchange, or by mining it.[18] Cryptocurrency ATMs are internet-connected kiosks that allow customers to purchase [redacted] or other cryptocurrency by depositing cash.

Cryptocurrency exchanges, such as Coinbase, are digital marketplaces where traders can buy and sell cryptocurrencies, similar to a brokerage. Users can purchase cryptocurrency by completing a bank wire, bank draft, credit card draft, or check mailing with traditional currencies, such as U.S. dollars. It Is also possible to use a cryptocurrency exchange to trade one type of cryptocurrency for another.

How is Cryptocurrency Stored?

To use an online exchange, the user must set up an account with the exchange. Within the exchange account, the user can store cryptocurrency in wallets. There is no limit to the number of wallets that can be created for an exchange account. All cryptocurrency is stored in wallets. Each wallet has an address, which is a string of numbers and letters that cryptocurrency can be sent to and from, similar to an email address. Some cryptocurrency exchangers will generate a new wallet address each time a transaction is made. This protects the privacy of the wallet holder so that a third-party viewer cannot identify all transactions associated with the wallet.

How Does Cryptocurrency Work?

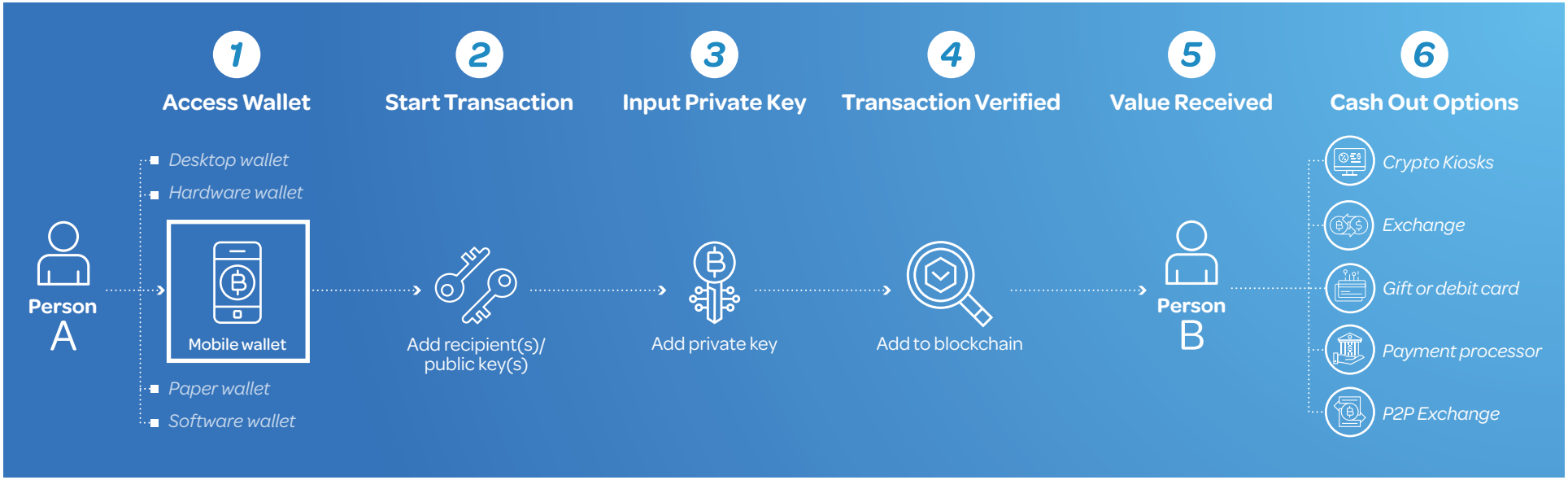
Cryptocurrencies depend on a distributed public ledger that is often referred to as the "blockchain," and a network of peer-to peer users to maintain an accurate system of payments and receipts. Records of cryptocurrency transactions are stored on its blockchain, which is available to the public as a distributed ledger that contains records of all cryptocurrency transactions in code. Some private cryptocurrencies, such as Monero, do not make the blockchain public.

Blockchain does not require a central authority because all transactions are confirmed through consensus protocol, an agreement among the users that the new transaction can be added. In the blockchain, transactions are stored in blocks and each block of transactions is linked to the previous block.

Any changes to the existing linked blocks will alert other users, making it impossible for someone to manipulate the blockchain. This prevents fraudulent activities, such as double spending, which is the act of using the same cryptocurrency twice. See Figure 3 for illustration.

18 Mining is the process by which blockchain transactions are verified and new cryptocurrency is created.

Figure 3: How the Blockchain Facilitates Cryptocurrency Payments



Source: GAO Science & Tech Spotlight, Blockchain & Distributed Ledger Technologies, dated September 2019.

Appendix C: Management's Comments

UNITED STATES POSTAL INSPECTION SERVICE

CYBERCRIME AND ANALYTICS

August 18, 2021

JOSEPH WOLSKI
DIRECTOR, AUDIT OPERATIONS

SUBJECT: U.S. Postal Inspection Service Oversight of its Use of Cryptocurrency (Project Number 21-067-DRAFT)

Thank you for the opportunity to review and comment on the findings and recommendations contained in the draft audit report, *U.S. Postal Inspection Service Oversight of its Use of Cryptocurrency*.

Management agrees with Findings #2, #3 and #4.

Management agrees in part with Finding #1: *Use of the Cryptocurrency Fund Program*. We disagree that the Program is unable to help postal inspectors manage the challenges associated with cryptocurrency's inherent volatility and that this leaves the Postal Inspection Service susceptible to theft, abuse, and mismanagement of federal funds. We have management oversight and internal controls related to the investigative use of cryptocurrency including transactions funded via the program's cryptocurrency exchange account as well as transactions funded via investigative funds. We believe the controls currently in place mitigate risks related to theft, abuse and mismanagement of funds.

However, we do agree that our cryptocurrency program oversight could be enhanced by adding different types of cryptocurrency to the [redacted] when demand for those particular types of cryptocurrency for investigative use is high. For those emerging cryptocurrencies where demand is low or unique to an investigative need, it may not be practical to add use of those types of cryptocurrency to the [redacted] Nevertheless, we do recognize the need for the Program Manager to be made aware of all cryptocurrency transactions regardless of funding source, which will support more comprehensive oversight of cryptocurrency utilization across the agency.

The U.S. Postal Inspection Service agrees with the recommendations and will address them below.

Recommendation 1: We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, ensure that the Cryptocurrency Fund Program has the information needed to provide oversight of the investigative use of cryptocurrency.

475 L'Enfant Plaza SW Washington, DC 20260

Management Response/Action Plan: Management agrees with this recommendation. The investigative use of cryptocurrency is tracked within the [redacted] as well as through the Investigative Funds process. The Cryptocurrency Fund Program, and its Program Manager, will continue to assess any future controls needed for full visibility across the program. This includes developing protocols for the Program Manager to be notified of the acquisition and investigative use of cryptocurrency outside of the [redacted]

Target Implementation Date: August 1, 2022

Responsible Official: Postal Inspector in Charge, Analytics and Cybercrime

Recommendation 2: We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, modify the [redacted] to ensure duplicates and unrelated transactions are not included in the *Transaction Review Report* and that the report provides sufficient information to differentiate between transactions.

Management Response/Action Plan: Management agrees with this recommendation, and this has already been implemented as of July 30, 2021.

Target Implementation Date: Completed July 30, 2021

Responsible Official: Postal Inspector in Charge, Analytics and Cybercrime

Recommendation 3: We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, develop a comprehensive cryptocurrency training program.

Management Response/Action Plan: Management agrees with this recommendation. A comprehensive cryptocurrency training program will be developed.

Target Implementation Date: June 30, 2022

Responsible Official: Postal Inspector in Charge, Analytics and Cybercrime

Recommendation 4: We recommend the **Postal Inspector in Charge, Analytics and Cybercrime**, develop written procedures for the management and oversight of the national wallet and its associated exchange account.

Management Response/Action Plan: Management agrees with this recommendation. Written procedures will be developed for the management and oversight of the national wallet and its associated exchange account.

Target Implementation Date: January 31, 2022

Responsible Official: Postal Inspector in Charge, Analytics and Cybercrime

Sincerely,

Michael Ray Digitally signed by Michael Ray Date: 2021.08.19 15:03:58 -04'00'

Michael J. Ray
Postal Inspector in Charge, Analytics and Cybercrime

cc: Manager, Corporate Audit Response Management

OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, please email
press@uspsoig.gov or call 703-248-2100