



FinCEN NOTICE

FIN-2024-NTC1

April 15, 2024

FinCEN Notice on the Use of Counterfeit U.S. Passport Cards to Perpetrate Identity Theft and Fraud Schemes at Financial Institutions

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Notice by including the key term “**FIN-2024-NTC1**” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative and select SAR field 34(z) (Fraud – other) and include the term “**Passport Card**” in the text box.

The U.S. Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN), in close coordination with the U.S. Department of State’s Diplomatic Security Service (DSS),¹ is issuing this Notice to financial institutions² urging them to be vigilant in identifying and reporting suspicious activity related to the use of counterfeit U.S. passport cards³ for identity theft and fraud schemes (hereinafter, “U.S. passport card fraud”). Since 2018, DSS has identified a concerning increase in the use of counterfeit U.S. passport cards by individuals and fraud rings to gain access to victim accounts at financial institutions nationwide. This fraud occurs in person at financial institutions and involves an individual impersonating a victim by using a counterfeit U.S. passport card that contains the victim’s actual information. DSS assesses that from 2018 to 2023, these schemes have resulted in \$10 million in actual losses and \$8 million in additional attempted losses, with over 4,000 victims in the United States. However, DSS and other law enforcement agencies assess that losses associated with U.S. passport card fraud and associated identity theft are likely significantly greater and seek increased reporting by financial institutions to identify additional illicit activity.

FinCEN is issuing this Notice to ensure that financial institutions identify and report suspicious activity potentially related to U.S. passport card fraud. This Notice: (i) provides an overview of several typologies related to U.S. passport card fraud; (ii) highlights select technical, behavioral, and financial red flags to assist financial institutions in identifying and reporting suspicious activity; and (iii) reminds financial institutions of their reporting requirements under the Bank Secrecy Act (BSA).

1. DSS is the federal law enforcement and security bureau of the U.S. Department of State (State). It is tasked with securing diplomacy and protecting the integrity of U.S. travel documents. For more information on DSS, see State, [About Us – Bureau of Diplomatic Security](#) (Sept. 28, 2022).
2. 31 U.S.C. § 5312(a)(2); 31 CFR § 1010.100(t).
3. See State, “[Get a Passport Card](#)” (last updated Feb. 13, 2024); State, “[Passport and Visa Fraud](#).”

Fraud, including identity theft and impersonation schemes, is the largest source of illicit proceeds in the United States⁴ and represents one of the most significant money laundering threats to the United States as highlighted by the Department of the Treasury in its latest National Money Laundering Risk Assessment.⁵ Combating fraud is one of FinCEN’s Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.⁶

The information contained in this Notice is derived from open-source reporting and information provided by DSS and other law enforcement partners.

Emerging Risks and Typologies of Identity Theft and Fraud Schemes Involving Counterfeit U.S. Passport Cards

Counterfeiting of U.S. Passport Cards

According to DSS and other law enforcement agencies, individuals and fraud rings are falsely making, selling, and using counterfeit U.S. passport cards to impersonate and defraud persons holding accounts at financial institutions.⁷ Illicit actors are counterfeiting U.S. passport cards because U.S. passport cards are a less familiar form of U.S. government-issued identification, thereby potentially decreasing the likelihood of detection by financial institutions. U.S. Passport cards are also significantly cheaper to counterfeit compared to U.S. passport books.⁸

-
4. Fraud, to include identity theft, was the most reported typology in BSA reports throughout 2021. Additionally, identity-related suspicious activity accounted for approximately 42% of total BSA reports and \$212 billion in activity, and approximately 69% of these BSA reports indicate the use of impersonation to defraud victims. See FinCEN Financial Trend Analysis, [Identity-Related Suspicious Activity: 2021 Threats and Trends](#) (Jan. 2024), pp. 1-2.
 5. U.S. Department of the Treasury, “[2024 National Money Laundering Risk Assessment](#)” (Feb. 2024), pp. 5-18.
 6. FinCEN, “[Anti-Money Laundering and Countering the Financing of Terrorism National Priorities](#)” (June 30, 2021).
 7. See U.S. Department of Homeland Security, Immigration and Customs Enforcement, “[HSI Probe Leads to Federal Charges Against 3 Los Angeles-Area Men for Running Counterfeit Document Ring that Created and Sold Dozens of False Passports, IDs](#)” (Feb. 23, 2021); Department of Justice (DOJ), U.S. Attorney’s Office for the District of Vermont, “[Florida Man Charged with Passport Card Fraud, Bank Fraud, Identity Theft](#)” (Jan. 5, 2024); and DOJ, U.S. Attorney’s Office for the Western District of Michigan, “[Florida Man Sentenced To 48 Months In Federal Prison For Using Counterfeit U.S. Passport Cards In Check-Cashing Scheme](#)” (“DOJ USAO Western District of Michigan”) (Aug. 18, 2023).
 8. See DOJ USAO Western District of Michigan, *supra* note 7. The fraudulent reproduction and use of U.S. passport books is also used by criminals to perpetuate ID-theft and account takeovers, see e.g. DOJ, U.S. Attorney’s Office for the District of Massachusetts, “[New York Man Arrested for Bank Fraud Scheme Involving Stolen Identities of Three Massachusetts Residents](#)” (Nov. 7, 2023).

U.S. Passport Card

The U.S. passport card is a REAL ID compliant identity and travel document issued by the U.S. Department of State for use by U.S. citizens. It can be used for purposes of identity, proof of U.S. citizenship, domestic air travel, and land and sea border crossings into the United States from Canada, Mexico, the Caribbean, and Bermuda. The U.S. Department of State began issuing the passport card in July 2008 as an alternative travel document to the U.S. passport book. The passport card provides a less expensive, smaller, and convenient alternative to the U.S. passport book for those who travel frequently to these destinations by land or by sea.⁹

Illicit actors acquire a potential victim's personal identifiable information (PII) from either the U.S. Mail or the Darknet.¹⁰ Using the stolen PII, the illicit actors create—or order and purchase from other fraud rings—a counterfeit U.S. passport card that includes a passport photo of themselves or of a “money mule”¹¹ they have recruited to participate in the scheme, but which reflects the PII of the victim.

Identity Theft and Fraud Typologies Using Counterfeit U.S. Passport Cards

U.S. Passport Card Fraud

It is a federal crime to make, forge, counterfeit, mutilate, or alter any passport card with the intent to use it. It is also a federal crime to willfully and knowingly use, or attempt to use, or furnish to another for use any such false, forged, counterfeited, mutilated, or altered passport card.¹²

After creating a fraudulent U.S. passport card, the illicit actor or the money mule will use the fraudulent identification to impersonate the victim at a branch of the victim's known financial institution. The illicit actors may avoid branches of the financial institution the victim frequents to evade detection by employees who may be familiar with, or recognize, the victim. If the illicit actor's identity is called into question by financial institution staff and they are asked to present a second form of identification, they may present a counterfeit credit card bearing the name of the victim they are impersonating as proof of identity.

-
- 9. See “Get a Passport Card” *supra* note 3, p. 1.
 - 10. The Darknet are areas of the Internet accessible only via specialized anonymizing software, such as “The Onion Router” (Tor) network. While Darknet content is varied, it is also home to hidden services such as criminal marketplaces that allow individuals to buy and sell illegal items, such as drugs, firearms, and other hazardous materials with greater anonymity than is possible on the traditional Internet. Generally, these Darknet market websites use a variety of anonymizing and encryption technologies in an attempt to shield communications and transactions from interception and monitoring. For more information pertaining to fraud involving theft from the U.S. Mail, see FinCEN, “[FinCEN Alert on Nationwide Surge in Mail Theft-Related Check Fraud Schemes Targeting the U.S. Mail](#)” (Feb. 27, 2023).
 - 11. A money mule transfers or moves illicit funds at the direction of or on behalf of another, either wittingly or unwittingly. See DOJ, [Money Mule Initiative](#) (updated Apr. 25, 2023); Federal Bureau of Investigation (FBI) Internet Crime Complaint Center Public Service Announcement, “[Money Mules: A Financial Crisis](#)” (Dec. 3, 2021); FBI, “[Money Mules](#).” For additional context on money mules, see also, FinCEN, “[Advisory on Imposter Scams and Money Mule Schemes Related to Coronavirus Disease 2019 \(COVID-19\)](#)” (July 7, 2020).
 - 12. [18 U.S.C. § 1543](#).

F I N C E N N O T I C E

However, these credit cards are also usually fraudulent and not tied to any account or third-party vendor. DSS has indicated that it is a common tactic for illicit actors to work in pairs and that money mules may be directed by phone from a vehicle outside of the financial institution or located somewhere off premises. In the event an imposter cannot answer specific questions regarding their victim's identity, they may be fed information from their co-conspirator or handlers through an earpiece or other inconspicuous device.

Upon successfully bypassing account access security protocols at the branch location, DSS has observed that illicit actors may attempt the following transactions:

1. The illicit actor will seek to gain information about a victim's account, by, for example, asking questions regarding the account balance and withdrawal limits. Once such information is obtained, the illicit actor will quickly withdraw large amounts of cash below the Currency Transaction Reporting (CTR) threshold, purchase cashier's checks or money orders, or initiate wires.¹³ To evade the CTR threshold, the illicit actor may visit other bank branch locations and repeat the process, using the same victim's information.¹⁴
2. The illicit actor cashes stolen or forged checks to obtain funds from a victim's account.¹⁵
3. The illicit actor establishes a new joint account, using the victim's account information, with a second illicit actor as a joint owner. After the joint account is established in person, the illicit actor will then transfer funds out of the victim's existing account into the newly established joint account. The funds in the joint account are then wired to other accounts wholly controlled by illicit actors.¹⁶

In each of these cases, the objective is to expeditiously remove all remaining funds from a victim's account. Once successful, the illicit actor may quickly move on to their next victim with a new counterfeit U.S. passport card and repeat the fraud scheme.

Case Study

Fraudster Sentenced to 13+ Years in \$1.9 Million Scheme

Nohmaan Malik, 30, pleaded guilty in November 2022 to conspiracy to commit bank fraud, passport fraud, and aggravated identity theft. Malik, the mastermind behind the \$1.9 million bank fraud, was sentenced to more than 13 years in federal prison. The Court ordered

13. See DOJ, U.S. Attorney's Office for the Eastern District of Louisiana Press Release, "[Georgia Pair Plead Guilty to Conspiracy to Use False or Counterfeit Passports](#)" (Sep. 15, 2022); DOJ, U.S. Attorney's Office for the Eastern District of Louisiana Press Release, "[New York Woman Pleads Guilty to Passport Fraud Conspiracy](#)" (Oct. 19, 2020); and DOJ, USAO Western District of Michigan, *supra* note 7, p. 2.
14. The activity would violate 31 U.S.C. § 5324, which prohibits the structuring of transactions to evade certain reporting and recordkeeping requirements. See 31 U.S.C. § 5324(d) (criminal penalties); 31 U.S.C. § 5317(c) (civil and criminal forfeiture); 31 U.S.C. § 5321(a)(4) (civil penalties); 31 CFR § 1010.100(xx) (definition of "structuring").
15. See DOJ, USAO Western District of Michigan, *supra* note 7, p. 2.
16. See DOJ, U.S. Attorney's Office for the Northern District of Texas Press Release, "[Fraudster Sentenced to 13+ Years in \\$1.9 Million Scheme](#)" (Mar. 30, 2023).

restitution in the amount of \$1.9 million, the amount of loss the victims suffered. According to plea papers, Mr. Malik admitted he and coconspirators defrauded Chase Bank customers. They selected customers with sizeable balances at Chase and created counterfeit passport cards using the customers' names and identifying information but with conspirators' photographs. Using those counterfeit passport cards, conspirators imitating the bank customers opened fraudulent joint bank accounts with other conspirators acting as money mules. The impersonator or the money mule then transferred money from the customers' actual account to the joint bank account, and then transferred the money from the joint account into a third bank account controlled solely by the conspirators.¹⁷

Red Flag Indicators of Identity Theft and Fraud Involving Counterfeit U.S. Passport Cards

FinCEN, in consultation with DSS, has identified the following red flag indicators to help detect, prevent, and report potential suspicious activity related to the use of counterfeit passport cards in identity theft and fraud schemes. Because no single red flag is determinative of illicit or other suspicious activity, financial institutions should consider the surrounding facts and circumstances, such as a customer's historical financial activity, whether the transactions are in line with prevailing business practices, and whether the customer exhibits multiple red flags, before determining if a transaction or attempted transaction is indicative of identity theft and fraud involving the use of counterfeit U.S. passport cards or is otherwise suspicious.

Technical Red Flags¹⁸

- 1 The photo on the presented U.S. passport card has a white, blurry border; a dark gray square surrounding the photo; or is in color. Legitimate U.S. passport cards are laser engraved, which produces a clear and crisp grayscale portrait image.
- 2 The photo of the account holder on file does not match the individual present who is pictured in the counterfeit U.S. passport card.
- 3 The card bearer's date of birth and other areas of text are flat and do not feel raised when touched. Legitimate U.S. passport cards have tactile text on certain areas of the card and should feel textured.
- 4 The holographic U.S. Department of State seal is missing or has been substituted with a seal from an unrelated agency.
- 5 The smaller portrait is blurry and does not contain micro-printed text with information specific to the bearer of the card, or the portraits are of different people. On legitimate U.S. passport cards, the secondary photo is a complex image that contains personalized details that are microprinted to create the image.

17. *Id.*

18. See Appendix: Security Features of Legitimate U.S. Passport Cards on pp. 7-9 of this Notice for visual images and tips from DSS of how to identify fraudulent passport cards.

- 6 The signature of a customer presenting a U.S. passport card for identification does not match the customer's signature card on file.

Behavioral Red Flags

- 7 A customer presenting a U.S. passport card as identification may not know or be able to reference personal identifiers, including date of birth or social security number.
- 8 If a customer presenting a U.S. passport card as identification does know or is able to reference personal identifiers, including date of birth or social security number, they nevertheless lack basic account knowledge and are excessively interested in specific details about their account balances and withdrawal limits.
- 9 A customer appears to be following directions by phone from a third-party.
- 10 A customer presents a U.S. passport card for identification and opens a new joint account with a third-party with whom the customer has no prior relationship.
- 11 A customer conducts transactions characteristic of U.S. passport card fraud at branch locations outside of their geographical footprint.

Financial Red Flags

- 12 A customer presents a U.S. passport card as a form of identification and subsequently withdraws cash, purchases a cashier's check, purchases money orders, or initiates wire transfers for a large amount for no business or apparent lawful purpose.
- 13 A customer presents a U.S. passport card as a form of identification and attempts to negotiate an uncharacteristic, sudden, or abnormally large volume of checks made payable to cash.
- 14 A customer presents a U.S. passport card as a form of identification, asks for daily withdrawal and transfer limits, and subsequently withdraws cash, initiates a wire transfer, or purchases a cashier's check made payable to a third party.
- 15 A customer presents a U.S. passport card before transferring funds out of an existing account to a recently established joint account, and the funds are then rapidly withdrawn or wired from the joint account to a separate, unrelated account.
- 16 A customer makes withdrawals from an account at multiple branch locations for no business or apparent lawful purpose using a U.S. passport card as identification.
- 17 A customer engages in behavior that suggests efforts to evade the CTR filing requirements (*e.g.*, the customer alters or cancels a transaction when informed of the CTR filing requirement, or engages in structuring by conducting multiple cash withdrawals below \$10,000 during one business day).

Appendix: Security Features of Legitimate U.S. Passport Cards

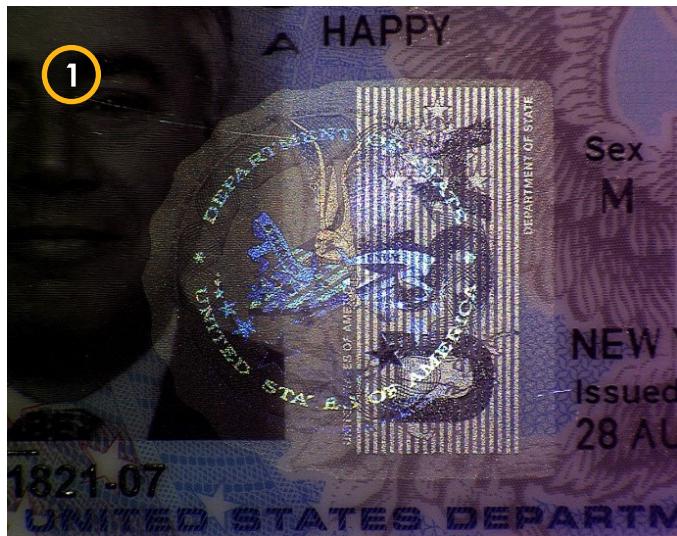


U.S. passport card front and back sides, showing the locations of security features.



FIN CEN NOTICE

CHECK VISUALLY



A complex holographic security feature overlaps the lower right of the card bearer's portrait. Tilt the hologram to see animation. Be suspicious if the hologram artwork is poor or the colors don't change.

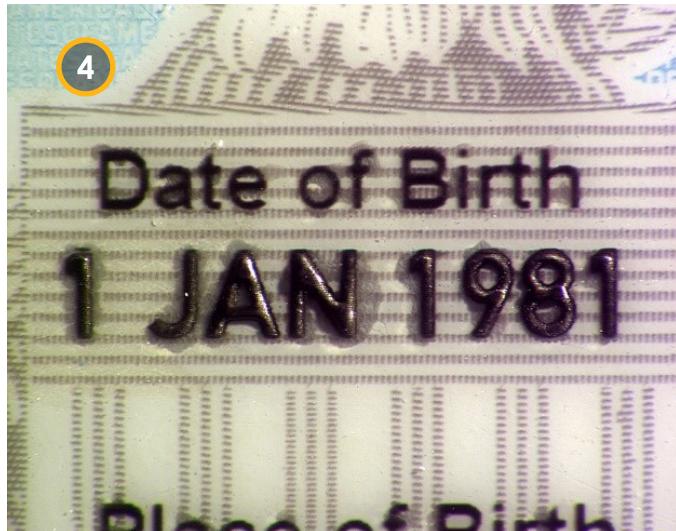


The back of the card contains a patch of color shifting ink. When tilted, it changes from gold to green. Be suspicious if the quality of the artwork is poor or the ink does not change color when tilted.

CHECK VISUALLY AND BY TOUCH



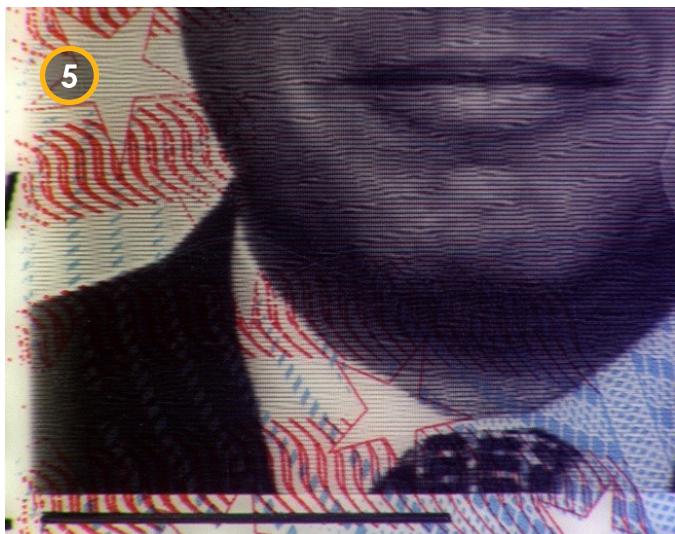
Textured, clear artwork of the Great Seal of the United States intersects the upper left of the card bearer's portrait. Be suspicious if the artwork is missing, blurry, or does not have a texture.



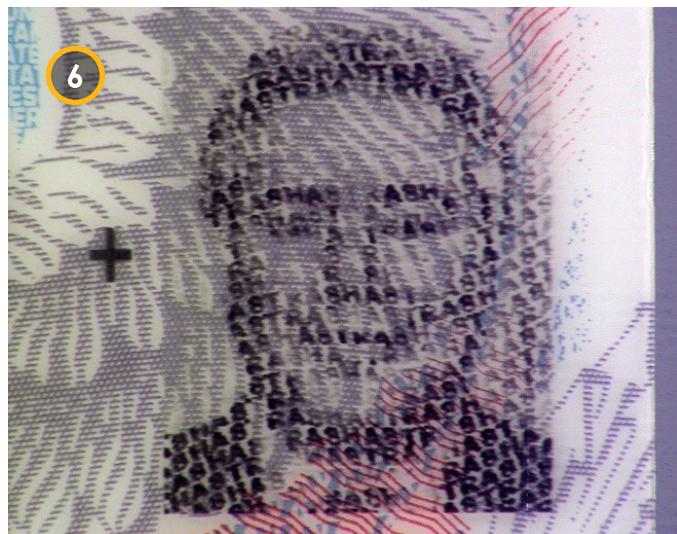
The card bearer's date of birth, and some other areas of the text, is deep black and has a distinct texture. Be suspicious if the date of birth print does not feel rough when touched.

FIN CEN NOTICE

CHECK WITH MAGNIFICATION OR ULTRAVIOLET LIGHT



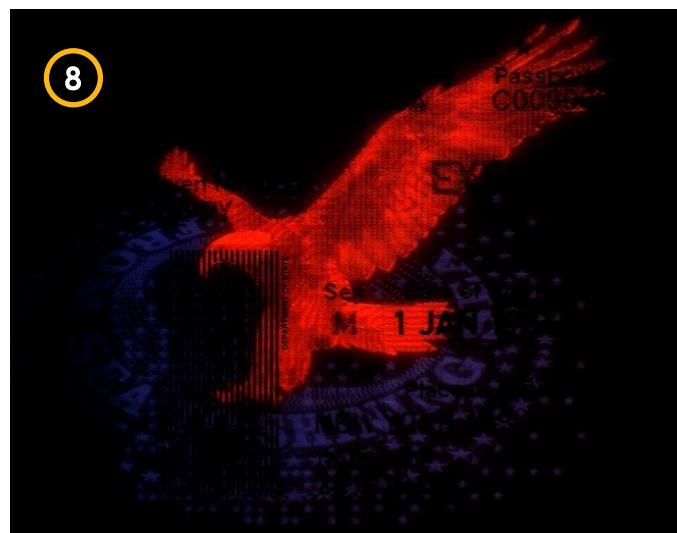
The large portrait on the left is grayscale and contains fine lines that can be inspected with a magnifier. Be suspicious if the portrait is in color, is of poor quality, or obscures the red and blue art behind it.



When checked with a magnifier, the small portrait contains tiny text with information specific to the owner of the card. Be suspicious if the text is blurry or the two portraits are of different people.



The colorful background artwork contains tiny text in several different locations. When checked with a magnifier, be suspicious if this microprinting is unreadable or if the background art is blurry.



Passport cards contain invisible printing that can only be inspected with ultraviolet (UV) light. Be suspicious if the UV art is missing, shows different graphics, or is discontinuous over the portrait.

Reporting U.S. Passport Card Fraud to DSS

In addition to filing a SAR, financial institutions are encouraged to refer their customers who may be victims of U.S. passport card fraud to DSS. Victims and financial institutions can report U.S. passport card fraud by contacting their nearest [DSS field office](#) or sending an email to DSS at DS_DO_USPCFraud@state.gov.

Reminder of Relevant BSA Obligations and Tools for U.S. Financial Institutions

Suspicious Activity Reporting

Other Relevant BSA Reporting

USA PATRIOT ACT Section 314(b) Information Sharing Authority

Suspicious Activity Reporting

A financial institution is required to file a SAR if it knows, suspects, or has reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity; is intended or conducted to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity.¹⁹ All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.²⁰

When a financial institution files a SAR, it is required to maintain a copy of the SAR and the original or business record equivalent of any supporting documentation for a period of five years from the date of filing the SAR.²¹ Financial institutions must provide any requested SAR and all documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.²² When requested to provide supporting documentation, financial institutions should take special care to verify that a requestor of information is, in fact, a representative of FinCEN or an appropriate law enforcement or supervisory agency. A financial institution should incorporate procedures for such verification into its BSA compliance or AML program. These procedures may include, for example, independent employment verification with the requestor's field office or face-to-face review of the requestor's credentials.

19. See 31 CFR §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320.

20. See 31 U.S.C. § 5318(g)(3). Financial institutions may report suspicious transactions regardless of amount involved and still take advantage of the safe harbor.

21. See 31 CFR §§ 1020.320(d), 1021.320(d), 1022.320(c), 1023.320(d), 1024.320(c), 1025.320(d), 1026.320(d), 1029.320(d), 1030.320(d).

22. *Id.* See also FinCEN, "[Suspicious Activity Report Supporting Documentation](#)" (June 13, 2007).

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping U.S. passport card identity theft and fraud schemes. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this notice by including the key term “**FIN-2024-NTC1**” in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional advisory or notice keywords in the narrative, if applicable.

Financial institutions should select SAR Field 34(z) (FRAUD-Other) as the associated suspicious activity type and include the term “**Passport Card**” in the text box. Financial institutions also should select all other relevant suspicious activity fields, such as those in SAR Fields 36 (Money Laundering) and 38 (Other Suspicious Activities), if applicable.

Financial institutions should include all available information relating to the account and locations involved in the reported activity, identifying information related to other entities and persons involved in the depositing or cashing of suspicious checks and the status of their accounts with the institution. Financial institutions also should provide all available information regarding other domestic and foreign financial institutions involved in the activity; where appropriate, financial institutions should consider filing a SAR jointly on shared suspicious activity.²³

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons also may have other relevant BSA reporting requirements to provide information in connection with the subject of this notice. These include obligations related to the Currency Transaction Report (CTR),²⁴ Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),²⁵ Report of Foreign Bank and Financial Accounts (FBAR),²⁶ Report of International Transportation of Currency or Monetary Instruments (CMIR),²⁷ Registration of Money Services Business (RMSB),²⁸ and Designation of

- 23. See 31 CFR §§ 1020.320(e)(1)(ii)(A)(2)(i), 1021.320(e)(1)(ii)(A)(2)), 1022.320(d)(1)(ii)(A)(2), 1023.320(e)(1)(ii)(A)(2)(i), 1024.320(d)(1)(ii)(A)(2), 1025.320(e)(1)(ii)(A)(2), 1026.320(e)(1)(ii)(A)(2)(i), 1029.320(d)(1)(ii)(A)(2), 1030.320(d)(1)(ii)(A)(2).
- 24. A report of each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through, or to a financial institution that involves a transaction in currency of more than \$10,000. Multiple transactions may be aggregated when determining whether the reporting threshold has been met. See 31 CFR §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
- 25. A report filed by a trade or business that receives currency in excess \$10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/IRS form when not otherwise required to be reported on a CTR. See 31 CFR § 1010.330; 31 CFR § 1010.331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.
- 26. A report filed by a U.S. person that has a financial interest in, or signature or other authority over, foreign financial accounts with an aggregate value exceeding \$10,000 at any time during the calendar year. See 31 CFR § 1010.350; FinCEN Form 114.
- 27. A form filed to report the transportation of more than \$10,000 in currency or other monetary instruments into or out of the United States. See 31 CFR § 1010.340.
- 28. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. See 31 CFR § 1022.380.

Exempt Person (DOEP).²⁹ These standard reporting requirements may not have an obvious connection to illicit finance, but may ultimately prove highly useful to law enforcement.

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this Notice, FinCEN requests that the filer select *Box 1b* (“suspicious transaction”) and include the key term “FIN-2024-NTC1” in the “Comments” section of the report.

Information Sharing

Information sharing among financial institutions is critical to identifying, reporting, and preventing identity theft and fraud schemes involving counterfeit U.S. passport cards or other illicit financial activity. Financial institutions and associations of financial institutions sharing information under the safe harbor authorized by section 314(b) of the USA PATRIOT Act are reminded that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.³⁰ FinCEN strongly encourages such voluntary information sharing. FinCEN encourages U.S. financial institutions to use, and potentially expand, their existing processes to collect and share information with foreign financial institutions in furtherance of investigations that involve cross-border activity.

For Further Information

FinCEN’s website at <https://www.fincen.gov/> contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Notice should be addressed to the FinCEN Regulatory Support Section at frc@fincen.gov.

The mission of the Financial Crimes Enforcement Network is to safeguard the financial system from illicit use, combat money laundering and its related crimes including terrorism, and promote national security through the strategic use of financial authorities and the collection, analysis, and dissemination of financial intelligence.

29. A report filed by banks to exempt certain customers from currency transaction reporting requirements. See 31 CFR § 1010.311.

30. See FinCEN, “[Section 314\(b\) Fact Sheet](#)” (Dec. 2020).