FinCEN ALERT

FIN-2026-Alert004

July 24, 2026

FinCEN Alert on Fraud Schemes Targeting Federal Student Aid

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert in SAR field 2 (Filing Institution Note to FinCEN) and the narrative by including the key term "**FIN-2026-FSAFRAUD**" and select SAR field 34(z) (Fraud – Other) and include the term "**Federal Student Aid Fraud**" in the text box.

The U.S. Department of the Treasury's (Treasury) Financial Crimes Enforcement Network (FinCEN) is issuing this Alert, in consultation with the U.S. Department of Education's (ED) Office of Inspector General (ED-OIG) and the Federal Bureau of Investigation (FBI), to urge financial institutions[1] to be vigilant in detecting, identifying, and reporting suspicious activity connected to fraud schemes targeting ED's Office of Federal Student Aid (FSA) programs. Fraud rings use stolen and fraudulent identities, as well as other tactics, to enroll in educational institutions and unlawfully acquire funds from Federal student aid programs. The schemes not only result in losses to Federal student aid programs, but also, in some cases, real students face difficulties enrolling in classes because of the number of fraudulently enrolled "students."[2]

The Department of Education has launched a nationwide effort to prevent fraud in Federal student aid programs to protect taxpayers while significantly reducing associated administrative burdens on colleges and universities.[3] ED and ED-OIG have consistently worked to detect, investigate, and facilitate the prosecution of fraudsters, as well as to communicate emerging fraud risks associated with Federal student aid and other ED programs.[4] In late 2025, ED announced that it had prevented $1 billion in Federal student aid fraud during that calendar year.[5]

1. *See* 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).
2. *See, e.g.*, Inside Higher Ed, "California Community Colleges Battle Against the Bots" (May 23, 2025); NBC Bay Area, "South Bay community colleges flag more than a third of applications over possible fraud" (June 27, 2024); Fortune, "'Ghost' students are hijacking millions from colleges—and locking real human students out of classes" (June 12, 2025).
3. *See* ED, Press Release, "U.S. Department of Education Launches Comprehensive, Nationwide Federal Student Aid Fraud Prevention Effort" (Apr. 27, 2026); ED, Press Release, "U.S. Department of Education to Implement New Identity Validation Processes to Combat Student Aid Fraud" ("ED: New Identity Validation Processes") (June 6, 2025).
4. *See generally* ED, Press Release, "Victories for American Taxpayers: Eliminating Fraud, Waste, and Abuse Across Federal Student Aid Programs" (Apr. 2, 2026); ED, "U.S. Department of Education Fights Fraud in Student Aid to Protect the American Taxpayer" (May 28, 2025); ED-OIG, "Free Materials" (last accessed July 2026); FSA, APP-25-16, "Significant Actions to Prevent Fraud through Identity Verification" (July 6, 2025).
5. *See* ED, Press Release, "U.S. Department of Education Prevents More Than $1 Billion in Federal Student Aid Fraud This Year, Additional Crackdowns Expected in 2026" (Dec. 11, 2025).

On March 25, 2025, President Trump issued Executive Order (E.O.) 14249, *Protecting America's Bank Account Against Fraud, Waste, and Abuse*, declaring that it "is the policy of the United States to defend against financial fraud and improper payments . . . .[,]" which threaten the integrity of Federal programs and undermine trust in government.[6] Fraud, including government benefits fraud, continues to be one of the largest sources of illicit proceeds in the United States, according to Treasury's 2026 National Money Laundering Risk Assessment.[7] Fraud and cybercrime are two of FinCEN's Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) National Priorities.[8]

The information in this Alert is derived from Bank Secrecy Act (BSA) data, open-source reporting, and information provided by law enforcement and foreign financial intelligence units.

Overview of Federal Student Aid

FSA awards more than $120 billion per year in grants, work-study funds, and low-interest loans to approximately 13 million students.[9] FSA also oversees the Free Application for Federal Student Aid (FAFSA), which students and parents use to apply for financial aid for post-secondary education.[10] Awarded student financial aid is initially paid directly to the educational institution at which a student is enrolled. After a school applies the financial award to a student's tuition and fees, any remaining balance is refunded to the student for other educational and living expenses.[11] In order to receive a full refund, however, students must be enrolled at an educational institution for 60 percent of the enrollment period, often necessitating completion of some coursework to remain enrolled.[12]

According to ED-OIG and the FBI, student aid refunds may be paid by deposits directly from an educational institution, an intermediary payment facilitator contracted by an educational institution, or, less commonly, by check. In instances where educational institutions use a payment intermediary to process student aid refunds, the payment intermediary will typically send an email to the email address of the student on file with the educational institution. This email instructs the student to create an account on the payment intermediary's platform where students are typically only required to provide a routing and account number.

Defrauding Federal Student Aid Programs

According to law enforcement, foreign and domestic fraud rings are perpetrating schemes exploiting Federal student aid programs, including by leveraging stolen personally identifiable information (PII) and complicit individuals to submit fraudulent enrollment applications to educational institutions and

6. *See* The White House, Executive Order on Protecting America's Bank Account Against Fraud, Waste, and Abuse, 90 Fed. Reg. 14,011 (Mar. 25, 2025); The White House, "Fact Sheet: President Donald J. Trump Protects America's Bank Account Against Waste, Fraud, and Abuse" (Mar. 25, 2025).
7. Treasury, "2026 National Money Laundering Risk Assessment" (Mar. 2026).
8. *See* FinCEN, "Anti-Money Laundering and Countering the Financing of Terrorism National Priorities" (June 30, 2021).
9. *See* ED, "About Federal Student Aid" (last reviewed Feb. 12, 2026).
10. *Id.*
11. *See* ED, "Receiving Financial Aid" (last accessed July 2026).
12. *See* FSA, "General Requirements for Withdrawals and the Return of Title IV Funds" (last modified Jan. 28, 2026).

FAFSA submissions.[13] The fraudsters perpetrating these schemes often exploit educational institutions that offer open admissions and online programs to defraud Federal student aid programs.[14]

Ghost Students[15]

Some fraud rings use "ghost students" to exploit the Federal student aid process and illegally obtain refunds. To create ghost students, fraudsters may illegally obtain PII to impersonate an identity theft victim and pose as a legitimate student.[16] Fraudsters may also use artificial intelligence (AI) or other tools to overcome identity verification by generating fraudulent documents that combine stolen PII with fabricated details, commonly referred to as synthetic identities.[17] Since obtaining a full refund requires a student to remain enrolled for 60 percent of the enrollment period, fraudsters may use AI-powered chatbots to complete coursework on behalf of ghost students.[18] FBI is also aware of fraud rings employing paid accomplices to complete coursework for ghost students.

Victims whose identities are leveraged as part of ghost student schemes, including minors, are unaware that fraudsters are receiving Federal student aid using their PII. As a result of these schemes, the identity theft victims may be blindsided by their resulting ineligibility for Federal student aid or significant debt obligations to student loans taken out in their name.[19]

Complicit Straw Students

In addition to ghost students, fraudsters may organize sophisticated networks of individual "straw students" to obtain Federal student aid. Straw students are complicit individuals who, for a fee, provide their PII to fraudsters, who then enroll them at educational institutions and collect financial aid refunds issued in their names.[20] The straw students do not attend classes, and the fraudsters

13. *See* ED-OIG, "Student Aid Administrators: Help Spot and Stop Student Aid Fraud Rings" (June 2025); ED-OIG Fraudgram Vol. 1, Issue 3 (Feb. 2025), at p. 3.
14. Open admissions, also known as open enrollment, is a college admissions process in which the only qualification for admission is a high school diploma or general educational development (GED) certificate. This typically includes community colleges or other smaller educational institutions which are largely designed to make higher education more accessible. *See* ABC News, "Inside the 'ghost student' scam that uses identity theft to steal college loans and financial aid" (Jan. 28, 2026).
15. The term ghost students refers to stolen identities used for the purpose of enrolling at an educational institution.
16. *See* Forbes, "The FAFSA Fraud Economy: Stolen Identities And Lost Millions" (Aug. 26, 2025); *see generally* Department of Justice (DOJ), "Texas Woman Sentenced for Decade-Long Fraud Conspiracy" (Aug. 2025); DOJ, U.S. Attorney's Office (USAO) for the Northern District of New York, Press Release, "Three Women Indicted for Alleged Scheme that Used Prison Inmates' Identities to Fraudulently Obtain Federal Student Loans" (Mar. 2023).
17. To learn more about synthetic identities and their use in illicit activity, visit The Federal Reserve, FedPayments Improvement, "Synthetic Identity Fraud: Defined to Fight It" (last accessed July 2026) and The Federal Reserve, FedPayments Improvement, "Synthetic Identity Fraud Mitigation Toolkit" (last accessed July 2026). *See generally*, FinCEN, Financial Trend Analysis, "Identity-Related Suspicious Activity: 2021 Threats and Trends" (Jan. 2024); FinCEN, FIN-2024-Alert004, "FinCEN Alert on Fraud Schemes Involving Deepfake Media Targeting Financial Institutions" (Nov. 13, 2024).
18. Associated Press, "How scammers are using AI to steal college financial aid" (June 10, 2025).
19. *See* ABC News, "Inside the 'ghost student' scam that uses identity theft to steal college loans and financial aid" (Jan. 28, 2026); Associated Press, "How scammers are using AI to steal college financial aid" (June 10, 2025); DOJ, USAO for the Southern District of Texas, "Former Professor Guilty in Student Financial Aid Fraud Scheme" (Mar. 20, 2026).
20. *See* DOJ, USAO for the Southern District of Indiana, Press Release, "Serial Scammer Sentenced to Federal Prison after Defrauding Department of Education out of More Than $930,000 in Financial Aid" (July 22, 2025).

may complete coursework for them.[21] Straw students may keep a portion of the Federal student aid refunds as payment for their pseudo-enrollment.[22]

Fayetteville Woman Gets Five Year Federal Prison Sentence for Stealing Over $5 Million in Community College Scholarship Scam[23]

A federal judge sentenced a Fayetteville, North Carolina woman to five years in federal prison for stealing over $5 million from Federal student aid for community colleges across North Carolina. The judge also ordered the perpetrator to pay $3,641,473 in restitution to ED. According to court documents and other information presented in court, between approximately 2016 and 2023, the perpetrator organized, led, and conspired with approximately 80 straw students to fraudulently apply for federal student aid at multiple community colleges in North Carolina. Federal investigators from ED-OIG estimate that the scheme resulted in over $5 million in financial aid awards and more than $3.5 million disbursed.

According to the investigation, the perpetrator collected PII from straw students and submitted fraudulent applications at the targeted schools. She then faked the attendance at classes, completion of work, and interactions with the target schools by impersonating the straw students. The perpetrator submitted FAFSA forms for the straw students through FSA's website and concealed her identity as the preparer. During the execution of a federal search warrant at the perpetrator's home, ED-OIG investigators recovered evidence establishing the operation and mechanics of the scheme, including PII and coursework for straw students, FSA account usernames and passwords, and bank account and routing numbers.

Insider-assisted Federal Student Aid Fraud

Corrupt staff at educational institutions can act as insiders for fraud schemes, taking advantage of their positions to defraud Federal student aid programs. These staff members may recruit straw students, ensure their acceptance and enrollment in educational institutions, and, in some cases, complete coursework on behalf of straw students. Corrupt insiders may also manipulate straw students' educational records to ensure they qualify for a full Federal student aid refund. These corrupt staff members then either steal financial aid refunds entirely or require students to pay them a portion of those funds.[24]

---

21. *See id.*; DOJ, USAO for the Eastern District of Michigan, Press Release, "Detroiter Pleads Guilty to Running Decade-Long Student Aid Fraud" ("DOJ: Detroiter Pleads Guilty") (Mar. 23, 2026).
22. *See, e.g.*, DOJ: Detroiter Pleads Guilty, *supra* note 21.
23. *See* DOJ, USAO for the Eastern District of North Carolina, Press Release, "Fayetteville Grandmother Gets Five Year Federal Prison Sentence for Stealing Over $5 Million in Community College Scholarship Scam" (Jan. 29, 2026); DOJ, USAO for the Eastern District of North Carolina, Press Release, "Fayetteville Woman Pleads Guilty to Defrauding the U.S. Department of Education in $5 Million Student Loan Scam" (Feb. 26, 2025); DOJ, USAO for the Eastern District of North Carolina, Press Release, "Fayetteville Woman Sentenced to Prison in a $3.5 million in Federal Student Aid Scheme" (June 25, 2025).
24. *See* DOJ, Press Release, "Five Individuals Sentenced in $12 Million Federal Financial Aid Fraud Scheme" (Dec. 16, 2022); Indictment, *United States v. Montgomery, et al.*, Case No. 4:20-cr 32-CDL-MSH (M.D. Ga. Oct. 15, 2020); DOJ, USAO for the Southern District of Texas, Press Release, "Former University Financial Advisor Sentenced to Four Years in Federal Prison for Scheme to Fraudulently Obtain More Than $5 Million in Student Loans" ("DOJ: Former University Financial Advisor") (Aug. 30, 2023).

Former University Financial Advisor Sentenced to Four Years in Federal Prison for Scheme to Fraudulently Obtain More Than $5 Million in Student Loans[25]

A former university employee was sentenced to four years in federal prison for conspiracy to commit wire fraud. The judge also ordered the perpetrator to pay restitution in the full amount of the victims' losses, at least $5,648,238, representing the outstanding balance on all federal student loans that the man obtained on behalf of himself and others as part of the scheme.

As detailed in court documents and his plea agreement, from about 2006 until approximately 2021, the perpetrator and his co-conspirators engaged in a scheme to defraud ED. Specifically, the perpetrator was employed as a financial advisor at a university, and his co-conspirators recruited over 60 straw students to apply for and enroll in post-graduate programs at more than eight academic institutions (the "Schools"), including the university where the perpetrator was employed. The perpetrator and his co-conspirators told the straw students that they would assist with the coursework for these programs, including completing assignments and participating in online classes, in exchange for a fee. As a result, the straw students fraudulently received credit for the courses, and in many cases, degrees from the Schools, without doing the necessary work. The perpetrator also admitted that he and his co-conspirators directed the straw students to apply for federal student loans. Many of the straw students were not qualified for the programs to which they applied. The straw students, as well as the perpetrator himself, were awarded aid, which went directly to the Schools and at least 60 straw students also received student loan refunds, which the Schools disbursed to straw students after collecting the tuition. The perpetrator, as the ringleader of the scheme, kept a portion of each of the students' loan refunds.

Laundering the Proceeds of Federal Student Aid-related Fraud

According to law enforcement, fraudsters who have enrolled ghost or straw students at educational institutions are often able to receive student aid refunds at accounts with no discernible connection to the stated student recipient of the refund. Financial institutions may be able to identify student aid refund payments either through deposits made directly by educational institutions or by contracted intermediaries. According to BSA data, payments made by an intermediary typically occur via automated clearing house (ACH) transfers and the associated transaction references may include the term "refund" and the educational institution's name or abbreviation (*e.g.*, "Local Community College Refund," "LCC REFUND"). In some cases, the stated recipient (*i.e.*, the student) may also be listed in the transaction reference (*e.g.*, "LCC REFUND John Doe," "Local Community College REFUND John Doe").

After illicitly obtaining student aid refunds, fraudsters may launder student aid funds, including through money mules, shell companies, and fraudulent accounts.

25. *See* DOJ: Former University Financial Advisor, *supra* note 24.

Money Mules[26]

Law enforcement has identified money mules operating in the United States who may receive or assist with laundering the proceeds of Federal student aid fraud and may receive multiple student aid refunds to their account. These money mules typically have no discernable connection to the stated beneficiaries of the student aid refunds that are credited to their account. After receiving student aid refunds, these money mules may transfer the funds to another account, purchase digital assets that they send to a wallet the scammers can access, or use domestic money services businesses to transfer the funds abroad.

Shell Companies

According to information available to FinCEN, foreign-based fraudsters may create domestic shell companies to ultimately receive funds derived from fraudulent Federal student aid refunds. In certain cases, a business account may directly receive fraudulently obtained student aid refunds for no business or apparent lawful purpose. More commonly, after a money mule account receives a fraudulently obtained student aid refund, the money mule will transfer these funds to an account for a business with shell-like characteristics.[27] The foreign-based fraudsters may then use these shell companies to transfer the funds abroad for further laundering, including investment in real estate.

Fraudulent Accounts

Law enforcement is aware of fraudsters—especially those operating as part of foreign-based fraud rings—who may use fake identities to overcome customer identification processes during account opening at U.S.-based financial institutions to receive student aid refunds. In certain cases, a single account may receive multiple student aid refunds, each intended for a different beneficiary. However, as fraud rings have become more sophisticated, they have employed criminal brokers to open multiple accounts online at depository institutions using a "one-to-one" model—as described by law enforcement—where each fraudulent account receives a student aid refund tied exclusively to a single financial aid applicant. According to law enforcement, the fraud rings perpetrating these schemes may pay criminal brokers that offer their services via the dark web or encrypted messaging platforms to create multiple bank accounts. These criminal brokers typically take a percentage of the student aid refunds that are deposited into the accounts they create as payment before sending the remaining amount to the fraudsters via peer-to-peer (P2P) or wire transfers, or by purchasing and transferring digital assets.

26. Money mules are people who are used, wittingly or unwittingly, to transfer value, either by laundering stolen money or physically transporting goods or other merchandise. *See* Financial Action Task Force, "Professional Money Laundering" (July 2018), at p. 22; FBI, "Money Mules" (last accessed July 2026).
27. These businesses typically have multiple indicators of shell activity, such as no verifiable business activity, little or no internet presence, and use of a "common address" shared with multiple entities. *See* Treasury, "2026 National Money Laundering Risk Assessment" (Mar. 2026), p. 59; FinCEN, "The Role of Domestic Shell Companies in Financial Crime and Money Laundering: Limited Liability Companies" (Nov. 2006).

Abuse of Digital Assets

Fraud rings responsible for perpetrating large-scale Federal student aid fraud schemes may pay criminal brokers to assist with laundering the fraudulently obtained student aid refunds. These criminal brokers may abuse digital assets to layer fraudulently obtained student aid refunds in an attempt to obfuscate the illicit origin of the funds. To do this, as discussed above, criminal brokers establish multiple accounts online at financial institutions to receive fraudulently obtained student aid refunds. Once these accounts receive student aid refunds, the criminal brokers layer the funds through a series of transfers through other accounts they control. Ultimately, these funds are then used to purchase digital assets—typically at smaller digital asset exchanges. Criminal brokers then may transfer these digital assets to a larger exchange where they can then be accessed by the perpetrators of the scheme, who will typically convert the digital assets back into their home country's currency.

Red Flag Indicators of Federal Student Aid-related Fraud

FinCEN has identified the following red flag indicators to help financial institutions detect, prevent, and report potentially suspicious activity related to Federal student aid fraud. 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 related red flags, before determining if a transaction or attempted transaction is indicative of fraud or is otherwise suspicious.

1. A customer who has no previous history of, or customer profile information that would be consistent with, enrollment at an educational institution receives a student aid refund, especially where the stated recipient of the refund listed in the transaction reference is an individual with no known connection to the customer. These funds are then rapidly transferred to another account via P2P or wire transfers, used to purchase digital assets, or used in transactions with online money services businesses that typically process international funds transfers.

2. A customer uses funds received from a student aid refund to quickly purchase digital assets, which the customer then rapidly transfers to another digital asset wallet for no business or apparent lawful purpose.

3. Multiple unrelated students use the same account for the deposit of federal student aid refunds.

4. A customer's account receives multiple student aid refunds, for no business or apparent lawful purpose, especially if the stated recipients listed in the transaction reference are unrelated individuals with no known connections to the customer. These funds may then be rapidly transferred to other accounts via P2P or wire transfers, used to purchase digital assets, or used in transactions with online money services businesses that typically process international funds transfers.

5 A newly established customer account is funded solely by student aid refunds and lacks other financial activity. These funds may then be rapidly transferred, in whole or part, via P2P or wire transfers to other accounts, used to purchase digital assets, or used in transactions with online money services businesses that typically process international funds transfers.

6 A business account receives multiple student aid refunds—especially if the stated recipients listed in the transaction reference are individuals with no known connections to the customer—for no business or apparent lawful purpose. These funds may be rapidly transferred to other accounts held by business entities or used in transactions with online money services businesses that typically process international funds transfers.

7 A customer receives multiple P2P or wire transfers from accounts that recently received student aid refunds, for no business or apparent lawful purpose.

8 Multiple accounts that receive a student aid refund are accessed from the same out-of-state or international IP address or the same device.

9 Multiple accounts are created online within a short timeframe at a financial institution and receive student aid refunds on a one-to-one basis (*i.e.*, one account receives one refund). These funds, in whole or part, may be rapidly transferred to other accounts via P2P or wire transfers, used to purchase digital assets, or used in transactions with online money services businesses that typically process international funds transfers.

Information for Victims of Federal Student Aid Fraud

If you believe that someone has used your personal information to apply for Federal student aid, act quickly and use the following tips:

1. Contact Federal Student Aid and the loan servicer to let them know about the situation.
2. Contact the credit reporting agencies and freeze your account so nobody else can open new credit accounts in your name. You'll find tips and credit agency contact information on identitytheft.gov.
3. If you receive an education-related email, text, or call that you believe is a scam, contact the ED-OIG Hotline to share what you received.

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

Suspicious Activity Reporting

A financial institution is required to file a suspicious activity report (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.[28] All statutorily defined financial institutions may voluntarily report suspicious transactions under the existing suspicious activity reporting safe harbor.[29]

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.[30] Financial institutions must provide any requested documentation supporting the filing of a SAR upon request by FinCEN or an appropriate law enforcement or supervisory agency.[31] 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.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping student aid fraud. FinCEN requests that financial institutions indicate a connection between the suspicious activity being reported and the activities highlighted in this Alert by including the key term "**FIN-2026-FSAFRAUD**" in SAR field 2 (Filing Institution Note to FinCEN), as well as in the narrative. Financial institutions may highlight additional Advisory, Alert, or Notice keywords in the narrative, if applicable.

Financial institutions should select SAR Field 34(z) (Fraud – Other) and include the term "**Federal Student Aid Fraud**" in the text box, as well as any other applicable check 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.

28. *See* 31 U.S.C. § 5318(g)(1); *see also* 31 C.F.R. §§ 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, 1030.320.
29. *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.
30. *See* 31 C.F.R. §§ 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).
31. *See id.*; *see also* FinCEN, FIN-2007-G003, "Suspicious Activity Report Supporting Documentation" (June 13, 2007).

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 activity 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.[32]

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. In situations involving violations requiring immediate attention, such as ongoing money laundering schemes, a financial institution should also immediately notify, by telephone, an appropriate law enforcement authority, in addition to filing a timely SAR.[33] Immediate notification to law enforcement is especially important in situations involving suspected terrorist activity, as terrorists and terrorist organizations often rely on the international financial system to acquire funding to sustain and finance their operations and engage in acts of terrorism. Additionally, FinCEN emphasizes that any financial institution and any director, officer, employee, or agent of such institution who makes, or requires another to make any voluntary disclosure of any possible violation of law or regulation to a government agency under the BSA or its implementing regulations is protected from liability for any such disclosure.[34]

Financial institutions wanting to report suspicious transactions that may potentially relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).[35]

Other Relevant BSA Reporting Requirements

Financial institutions and other entities or persons may also have other relevant BSA reporting requirements to provide information in connection with the subject of this Alert. These include obligations related to the Currency Transaction Report (CTR),[36] Report of Cash Payments Over $10,000 Received in a Trade or Business (Form 8300),[37] Report of Foreign Bank and Financial Accounts

32. *See* 31 C.F.R. §§ 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).
33. *See, e.g.*, 31 C.F.R. §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).
34. 31 U.S.C. § 5318(g)(3); *see, e.g.*, 31 C.F.R. 1020.320(f).
35. The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
36. 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 C.F.R. §§ 1010.310-313, 1020.310-313, 1021.310-313, 1022.310-313, 1023.310-313, 1024.310-313, and 1026.310-313.
37. A report filed by a trade or business that receives currency in excess of $10,000 in one transaction or two or more related transactions. The transactions are required to be reported on a joint FinCEN/Internal Revenue Service form when not otherwise required to be reported on a CTR. *See* 31 C.F.R. §§ 1010.330-331. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed $10,000.

(FBAR),[38] Report of International Transportation of Currency or Monetary Instruments (CMIR),[39] Registration of Money Services Business (RMSB),[40] and Designation of Exempt Person (DOEP).[41]

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities (FCM/IBs) are required to have appropriate risk-based procedures for conducting ongoing customer due diligence that include, but are not limited to: (i) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (ii) conducting ongoing monitoring to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.[42] Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.[43] Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons (PEPs).

Senior foreign political figures and due diligence obligations for private banking accounts

In addition to these due diligence obligations, under section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and its implementing regulations, covered financial institutions must implement due diligence programs for private banking accounts held for non-U.S. persons that are designed to detect and report any known or suspected money laundering or suspicious activity conducted through or involving such accounts.[44] Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and beneficial owners of such accounts and ascertaining whether any of these owners are senior foreign political figures, and for conducting enhanced scrutiny on accounts held by senior foreign political figures that is reasonably designed to detect and report transactions that may involve the proceeds of foreign corruption.[45]

38. 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 C.F.R. § 1010.350; FinCEN Form 114.
39. 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 C.F.R. § 1010.340.
40. A form filed to register a money services business (MSB) with FinCEN, or to renew such a registration. *See* 31 C.F.R. § 1022.380.
41. A report filed by banks to exempt certain customers from currency transaction reporting requirements. *See* 31 C.F.R. § 1010.311.
42. *See* 31 C.F.R. §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).
43. *See* 31 C.F.R. §§ 1010.230, 1010.650(e)(1) (defining "covered financial institution").
44. *See* 31 C.F.R. § 1010.620. The definition of "covered financial institution" is found in 31 C.F.R. § 1010.605(e)(1). The definition of "private banking account" is found in 31 C.F.R. § 1010.605(m). The definition of "non-U.S. person" is found in 31 C.F.R. § 1010.605(h).
45. *See* 31 C.F.R. § 1010.620(c).

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,[46] and covered financial institutions are reminded of correspondent account due diligence requirements under Section 312 of the USA PATRIOT Act (31 U.S.C. § 5318(i)) and implementing regulations.[47] As described in FinCEN Interpretive Release 2004-1, the AML/CFT program of an MSB must include risk-based policies, procedures, and controls designed to identify and minimize risks associated with foreign agents and counterparties.[48]

Information Sharing

Information sharing between and among financial institutions is critical to identifying, reporting, and preventing illicit activity, including fraud schemes targeting Federal student aid. Under the safe harbor from liability provided by section 314(b) of the USA PATRIOT Act, financial institutions may share information with other eligible financial institutions regarding activities that may involve possible terrorist activity or money laundering, including information about fraud and other specified unlawful activities.[49] FinCEN strongly encourages financial institutions to participate in this voluntary program as information sharing between and among financial institutions can assist financial institutions in managing illicit financing risks and can ultimately provide the government with highly useful information to identify and prevent financial crime. Given the transnational nature of illicit activity, FinCEN encourages U.S. financial institutions to use, and potentially expand, their processes to collect and share information with foreign financial institutions to further investigations involving cross-border activity.[50]

The section 314(b) program provides financial institutions with the flexibility and connectivity needed to counter threats and prevent illicit actors from exploiting gaps between institutions. Among other things, information sharing pursuant to section 314(b) allows financial institutions to respond to threats—activities a financial institution suspects may involve possible terrorist activity or money laundering, such as fraud and other criminal activity—that are carried out by repeat actors moving across financial institutions to evade detection.

For additional information, see FinCEN's Section 314(b) Fact Sheet.

46. *See* 31 C.F.R. §§ 1010.210, 1020.210, 1021.210, 1022.210, 1023.210, 1024.210, 1025.210, 1026.210, 1027.210, 1028.210, 1029.210, 1030.210.
47. *See* 31 C.F.R. § 1010.610.
48. *See* FinCEN, Interpretive Release 2004-1, Anti-Money Laundering Program Requirements for Money Services Businesses with Respect to Foreign Agents or Foreign Counterparties, 69 Fed. Reg. 74,439 (Dec. 14, 2004); *see also* FinCEN, FIN-2016-G001, "Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring" (Mar. 11, 2016).
49. *See* 31 C.F.R. § 1010.540; *see also* FinCEN, "Section 314(b) Fact Sheet" (June 12, 2026).
50. *See* FinCEN, FIN-2025-G001, "Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality" (Sept. 5, 2025).

FinCEN's Whistleblower Program

FinCEN maintains a whistleblower incentive program for violations of the BSA and certain national security laws such as the International Emergency Economic Powers Act (IEEPA). Individuals located in the United States or abroad who provide information may be eligible for awards if the information they provide leads to a successful enforcement action that results in monetary penalties exceeding $1,000,000 and the statutory requirements in 31 U.S.C. § 5323 are otherwise met. Under 31 U.S.C. § 5323, there are certain confidentiality protections to individuals submitting information as well as certain protections from retaliation by employers. Individuals may also choose to submit information anonymously to FinCEN, including through an attorney. FinCEN is currently accepting whistleblower tips and encourages those with knowledge of potential violations to contact FinCEN. To learn more about FinCEN's Whistleblower Program, visit https://www.fincen.gov/whistleblower-program.

The Financial Crimes Enforcement Network's Advisory Program communicates priority money laundering, terrorist financing, and other illicit finance threats and vulnerabilities to the U.S. financial system. Financial institutions may use this information to support effective, risk-based, and reasonably designed anti-money laundering and countering the financing of terrorism (AML/CFT) programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

For Further Information

FinCEN's website at www.fincen.gov contains information on how to register for FinCEN Updates. Questions or comments regarding the contents of this Alert should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

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