



FinCEN

ALERT

FIN-2026-Alert009

October 30, 2026

FinCEN Alert on Risks Associated with Foreign-Agent-Directed Transactions

Suspicious Activity Report (SAR) Filing Request:

FinCEN requests that financial institutions reference this Alert by including the key term “FIN2026FOREIGNAGENT” in SAR field 2 (Filing Institution Note to FinCEN) and the narrative.

The Department of the Treasury’s Financial Crimes Enforcement Network (FinCEN) is issuing this Alert to urge financial institutions¹ to be vigilant in detecting, identifying, and reporting suspicious activity arising from certain cross-border payments involving U.S.-based money services businesses (MSBs).

MSBs provide critically important services to underserved populations and offer a key means to transfer funds

internationally.² Treasury has consistently noted that financial institutions should assess all customers on a case-by-case basis and that no individual type of customer, including MSBs, should be considered uniformly high risk.³

However, the cross-border relationships that MSBs often maintain to make overseas money transmission possible may give rise to potential risks to the U.S. financial system. Illicit actors may exploit these cross-border arrangements—particularly settlement arrangements subject to inadequate due diligence and transaction monitoring—to move funds through the U.S. financial system and obscure the ultimate beneficiaries and the underlying purpose of transactions. In doing so, illicit actors may exploit MSBs’ cross-border relationships to further and conceal illicit activity; for example, FinCEN has identified instances where funds ultimately benefited entities with identified connections to terrorist financing. As described below, these risks may be particularly pronounced when U.S.-based MSBs implement transactions at the direction of foreign agents. Through analysis of Bank Secrecy Act (BSA) reporting, FinCEN has identified more than \$8 billion in suspicious foreign-agent-directed payments between 2021 and 2025.

1. See 31 U.S.C. § 5312(a)(2); 31 C.F.R. § 1010.100(t).

2. Notably, the United States is the world’s largest source of remittances, sending approximately \$106.5 billion in 2025. See World Bank Group, “[Personal Remittances, Paid \(Current US\\$\)](#)” (last accessed Oct. 22, 2026). A prior study assessed that MSBs conducted more than 95% of all remittance transfers. Bureau of Consumer Financial Protection, [Remittance Rule Assessment Report](#) (Oct. 2018).

3. See Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, FinCEN, National Credit Union Administration, Office of the Comptroller of the Currency, “[Joint Statement on the Risk-Based Approach to Assessing Customer Relationships and Conducting Customer Due Diligence](#)” (July 6, 2022); see also FinCEN, Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, Office of Thrift Supervision, “[Interagency Interpretive Guidance on Providing Banking Services to Money Services Businesses Operating in the United States](#)” (Apr. 26, 2005) [hereinafter “MSB Banking Guidance”].

Note: BSA reporting is merely tip and lead information, and the mere reporting of suspicious activity does not serve as proof of illegal activity. BSA reporting reflects suspicious activity that has been identified and reported by financial institutions and, therefore, should not be considered a complete representation of the scope of any particular type of suspicious activity. BSA reporting may include additional transactions and information beyond a specific transaction that may be reportable as suspicious and, accordingly, the total reportable suspicious activity amount in any report may be overly inclusive. For example, BSA reporting may reflect both completed and attempted transactions, both inbound and outbound transactions, transfers between accounts, and both legal and illicit activities associated with a particular subject. BSA reporting may also describe continuing suspicious activity, amend earlier reporting, or cover expanded networks involved in potential illicit activity and, therefore, may reflect cumulative transactions from a single filer involving the same subject.

Principal MSB-Foreign Agent Relationships

Money transmitter MSBs typically operate through a system of agents, both domestically and internationally.⁴ An “agent” is a separate business entity from the principal that the principal authorizes, through a written agreement or otherwise, to sell its instruments or, in the case of funds transmission, to sell its send-and-receive transfer services.⁵ In practice, foreign agents can allow parties outside the United States to collect U.S.-origin funds transmitted by the domestic principal MSB.

Relationships between principal MSBs and foreign agents are typically governed by agreements covering cross-border money transmission.⁶ In addition to governing cross-border money transmission on behalf of customers, these agreements may also include provisions permitting the foreign agent to direct the principal MSB to make payments not only to the foreign agent but also to third-party entities (potentially identified as suppliers or partners) on behalf of the foreign agent.⁷ Put differently, at times, U.S.-based MSB principals may receive instructions from a foreign agent to make a payment to another foreign entity with whom the foreign agent purportedly maintains a relationship.

4. 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) [hereinafter “MSB Interpretive Release”].
5. See FinCEN, [“Frequently Asked Questions: Agent Request Initiative”](#) (Apr. 27, 2011), at 1.
6. See FinCEN, [“Bank Secrecy Act/Anti-Money Laundering Examination Manual for Money Services Businesses”](#) (Dec. 2008) [hereinafter “MSB Examination Manual”], at 5.
7. See generally Financial Action Task Force, [“Guidance for a Risk-Based Approach for Money or Value Transfer Services”](#) (Feb. 2016) (“[S]ettlement may be done through wire transfers, often involving aggregated amounts, processed through the international banking system. In addition, settlement can be done through third-party payment providers. However, settlement between and among [money or value transfer services] providers and agents may also be undertaken through cash courier, net settlement or other mechanisms, without any direct wire transfer between the originator and beneficiary.” (citations omitted)).

The BSA requires all MSBs subject to the BSA to develop, implement, and maintain an effective written anti-money laundering and countering the financing of terrorism (AML/CFT) program that is reasonably designed to prevent the MSB from being used to facilitate money laundering and the financing of terrorist activities.⁸ To establish effective procedures and controls as part of that AML/CFT program, a principal MSB's program would properly include agent monitoring policies and procedures sufficient to allow the principal to understand and account for associated risks.⁹ Although principal MSBs and agents may contractually allocate responsibility for developing policies, procedures, and internal controls, both the principal and its agents remain responsible for the implementation of the AML/CFT program requirements.¹⁰ And neither the agent nor the principal can avoid liability for failing to develop, implement, and maintain an effective AML/CFT program by pointing to a contract assigning this responsibility to another party (whether the agent or principal).¹¹

Accordingly, FinCEN has previously highlighted how, to reduce exposure to agent-related risks, the principal MSB must, among other things, have procedures in place to identify agents conducting activities that lack or appear to lack commercial purpose or are otherwise not supported by verifiable documentation. In addition, the principal MSB should implement procedures for handling non-compliant agents, including agent contract terminations.¹²

Foreign-Agent-Directed Transactions

As foreign agents may differ from domestic agents in the applicable legal framework, business model, and relationship with the domestic principal MSB, foreign agents may raise different AML/CFT compliance and monitoring considerations for domestic principal MSBs.

For instance, in connection with these principal-agent relationships, both the domestic principal MSB and the foreign agent may maintain accounts with other financial institutions, such as banks, for purposes of settling accounts or managing bulk transfers.¹³ Such arrangements would allow a foreign agent to instruct a principal MSB to transfer funds to the foreign agent's account in another jurisdiction. However, as illustrated below, such arrangements may also result in the foreign agent instructing the principal MSB to transfer funds to an unrelated third party outside the United States.

8. See 31 C.F.R. § 1022.210(a).

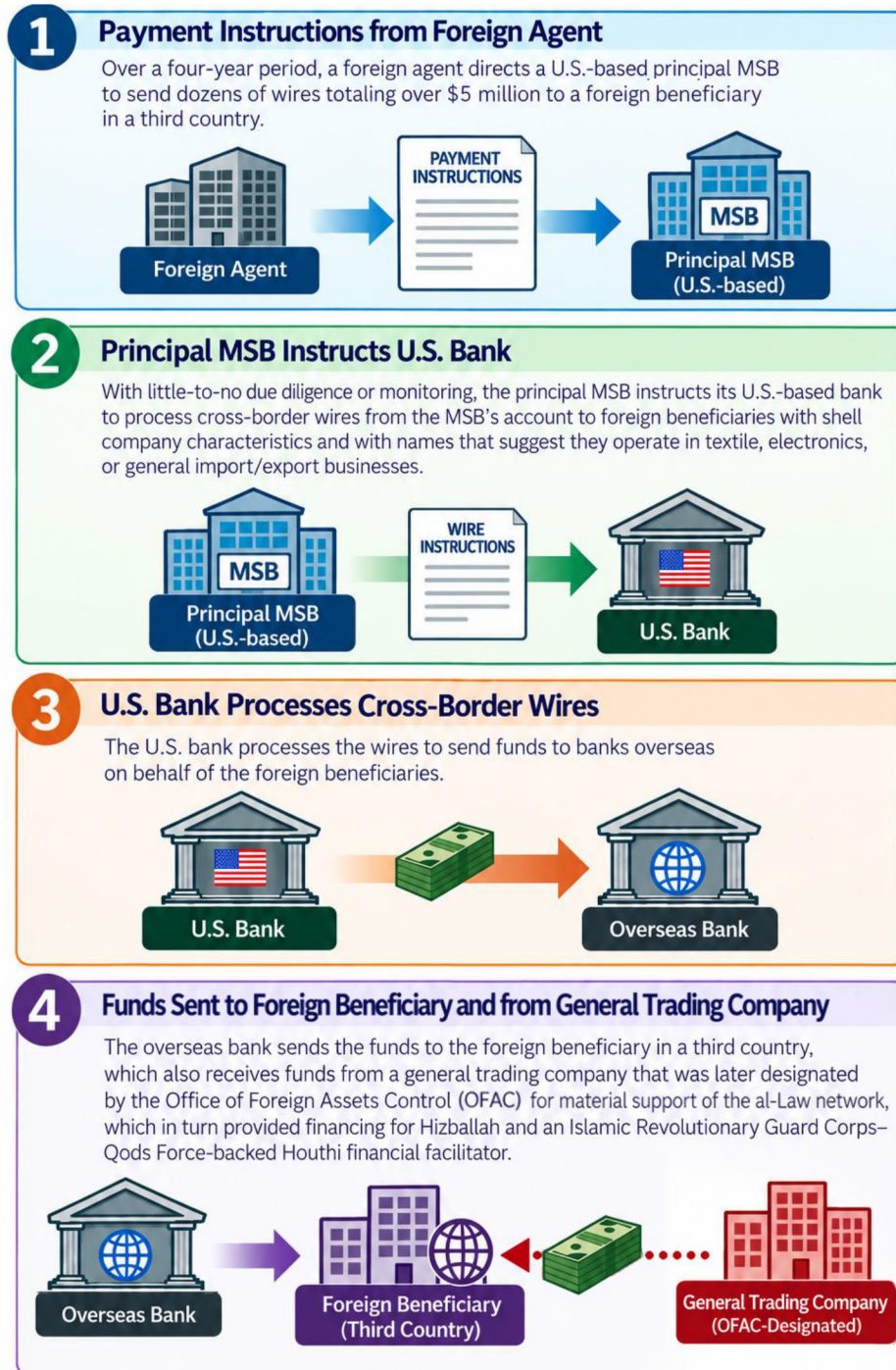
9. See MSB Interpretive Release, *supra* note 4, at 74,440–41.

10. 31 C.F.R. § 1022.210(d)(1)(iii).

11. See FinCEN, FIN-2016-G001, "[Guidance on Existing AML Program Rule Compliance Obligations for MSB Principals with Respect to Agent Monitoring](#)" (Mar. 11, 2016).

12. See *id.*

13. See MSB Banking Guidance, *supra* note 3 (noting that a money transmitter "might require [a] bank account to remit funds to its principal U.S. clearing account or may use the account to remit funds cross-border to foreign-based agents"); MSB Examination Manual, *supra* note 6, at 12–13.



As illustrated above, upon receiving the instructions, a principal MSB will often use its bank account to complete the foreign-agent-directed transactions,¹⁴ directing, for example, its bank to wire funds to a third-party recipient's overseas bank account. Although, in establishing the banking relationships underlying such transfers, the principal MSB may make representations

14. See generally MSB Examination Manual, *supra* note 6, at 12–13 (noting that, for purposes of settlement, “a money transmitter and its agent must both have access to the banking system”).

to its bank regarding the purpose and intended use of its accounts (including the nature of the transactions to be conducted, the anticipated volume and value of account activity, and the types and geographic locations of counterparties expected to send or receive funds), FinCEN’s analysis of BSA reporting suggests that the principal MSB and the banks completing these transactions may receive limited—and, in some instances, potentially contradictory—information about the nature and business of the foreign agent and the third-party recipient and about the purpose of the foreign-agent-directed transaction.¹⁵

Such transactions present a risk of exploitation by illicit actors for money laundering, terrorist financing, or other financial crime. Based on analysis of BSA reporting, FinCEN has identified several recurring patterns in reported suspicious foreign-agent-directed payment transactions.

First, FinCEN has identified potentially suspicious transactions involving transfers originated by domestic principal MSBs to certain categories of beneficiaries that do not appear to have a clear business purpose or relationship with the domestic principal MSB, including foreign exchange houses in the United Arab Emirates (UAE), Chinese commercial banks and trading companies, and numerous recipients across East Africa.

Second, the volume and timing of transactions often appeared inconsistent with the stated business model or expected levels of retail activity of the principal MSB or the foreign agent. For example, transfers to settle foreign-agent-directed payments were often in round dollar (or near-round dollar) amounts or occurred daily, inconsistent with the expected revenue patterns of a business.

Third, the recipients in these transactions may not have the expected profile of a recipient of a principal MSB-foreign agent settlement transaction (*e.g.*, wiring funds to a general trading company rather than the MSB’s foreign agent) or may not have a clear business purpose (*e.g.*, the recipient is a general trading company, a company with no web presence, or a newly created company). For instance, a foreign agent may characterize the transaction to the principal MSB as a “settlement” for goods and services provided to the foreign agent’s overseas customers and direct a U.S. money transmitter to make payments to foreign entities in third countries that appear or purport to engage in a range of commercial activities—such as importers, exporters, or other non-financial businesses—purportedly to satisfy obligations owed by the foreign agent or its customers.¹⁶

Fourth, the funds deposited into the principal MSBs’ bank accounts were frequently transferred abroad to the third-party entities through international wire transfers within hours or days of receipt.

15. See FinCEN, [“Guidance to Money Services Businesses on Obtaining and Maintaining Banking Services”](#) (Apr. 26, 2005) (noting that “[m]oney services businesses seeking to obtain or maintain account relationships with banking organizations should be prepared to provide information or explanation to their banking organizations about the risks associated with the services offered, the customer base, the markets served, and the locations of the money services business”).

16. See, *e.g.*, FinCEN, FIN-2025-A002, [“FinCEN Advisory on the Iranian Regime’s Illicit Oil Smuggling Activities, Shadow Banking Networks, and Weapons Procurement Efforts”](#) (June 6, 2025) (highlighting risks related to exchange houses, trading companies, and foreign front companies).

Finally, by directing principal MSBs to complete wires to third parties on their behalf, the foreign agents appeared to be using the principal MSBs' bank accounts as their own. Such an arrangement limited the visibility of the principal MSB's bank into the originating foreign agent, the ultimate beneficiary third parties, and the underlying transaction. Indeed, based on analysis of BSA reporting, foreign agents often provide little information or supporting documentation to principal MSBs—and by extension their banks—about the nature of the recipient, its line of business, and the purpose for such payments.¹⁷ The opacity of such transactions presents a particular risk of exploitation by transnational illicit finance networks.

Recent regulatory action in the United Kingdom further illustrates the financial crime risks associated with money remittance services. In June 2026, the United Kingdom's Financial Conduct Authority (FCA) imposed restrictions on Euro Exchange Securities UK Ltd., a firm that, as a previously authorized Electronic Money Institution, was permitted to provide money remittance and related payment services.¹⁸ Citing "significant risks of financial crime," the FCA restricted the firm's ability to provide electronic money services and sought the appointment of special administrators, which was subsequently approved by a court later that month. Although the FCA's action arose under a different regulatory framework, it underscores the importance of effective controls to mitigate the risk that payment and remittance services may be exploited for illicit financial activity.

Red Flag Indicators

FinCEN has identified the following red flags to help financial institutions detect, prevent, and report suspicious activity connected to foreign-agent-directed transactions. As no single red flag is determinative of illicit or suspicious activity, financial institutions should consider the totality of available 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 whether a behavior or transaction is suspicious.

FinCEN reminds principal MSBs that their AML/CFT programs should include appropriate risk-based oversight of agents and counterparties. Principal MSBs should assess the risks associated with foreign agent relationships, including the nature and purpose of third-party payment arrangements, the jurisdictions involved, and the types of entities receiving payments.

Red Flags for Principal MSBs



A foreign agent directs a payment (including for the purported purpose of settlement of obligations between the principal MSB and the foreign agent) to a third-party entity not covered by the agent clearing agreement.

17. See generally MSB Interpretive Release, *supra* note 4, at 74,440 (describing how, as a result of foreign agent transaction structures, "clearing banks were so far removed from the transactions that they could not trace back or screen either the intervening transactions or the individuals involved in the transactions").

18. See Financial Conduct Authority, "[FCA Opens Investigation into Euro Exchange Securities UK Ltd](#)" (Sept. 16, 2026).

-  2 A foreign agent regularly directs payments (including for the purported purpose of settling obligations between the principal MSB and the foreign agent) to third-party entities in third-country jurisdictions such as China, the UAE, Egypt, and East African countries, including Kenya, Uganda, and Djibouti.
-  3 A foreign agent provides non-descriptive, repetitive, or unsupported reasons for the payment to a third-party entity (*e.g.*, “settlement,” “services,” or “business expense”).
-  4 A foreign agent is reluctant or fails to provide appropriate documentation (*e.g.*, invoices, contracts, or orders) to the principal MSB to support payment instructions, or the foreign agent provides the documentation but it is inconsistent or otherwise contains indicia that the requested payment may not relate to legitimate provision of goods or services.
-  5 A foreign agent directs payments to third-party entities with no apparent relationship to the foreign agent (*e.g.*, a textile company, a general trading company, a company with no web presence, or a newly created company).
-  6 A foreign agent is reluctant or fails to provide evidence to confirm that it conducted appropriate due diligence on the third-party entity to which a payment is directed.
-  7 The timing, volume, or nature of the payments directed by the foreign agent is not consistent with the purported settlement arrangement or otherwise suggests that the payments do not reflect the foreign agent’s legitimate commercial transactions.
-  8 The foreign agent is unwilling or unable to provide information regarding its licensing or regulatory status, business operations, or applicable AML/CFT controls, particularly when other circumstances raise concerns about the legitimacy of its activities.
-  9 A foreign agent regularly directs payments to third-party recipients in round dollar (or near-round dollar) amounts.

Red Flags for Banks Providing Services to MSBs

-  10 A customer MSB sends payments to a foreign entity that does not have the profile of a recipient of bulk MSB funds (*e.g.*, a textile company, a general trading company, a company with no web presence, or a newly created company).
-  11 When the bank or other financial institution requests additional information about the transfer(s), the customer MSB is reluctant or fails to provide documentation (*e.g.*, invoices, contracts, or orders) to substantiate the underlying purpose of the payment.
-  12 A customer MSB sends a large payment or regular payments to a third-party entity in a jurisdiction (such as China, the UAE, Egypt, and East African countries, including Kenya, Uganda, and Djibouti) that is inconsistent with the primary population served by the MSB.
-  13 The timing, volume, or nature of the payments of a customer MSB is not consistent with a settlement arrangement or otherwise suggests that the payments do not reflect legitimate commercial transactions.

- 14** A customer MSB sends repeated foreign-agent-directed payments in round dollar (or near-round dollar) amounts.

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.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 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.

SAR Filing Instructions

SARs, and compliance with other BSA requirements, are crucial to identifying and stopping illicit actors from exploiting certain cross-border transactions originated by MSBs. 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 **"FIN2026FOREIGNAGENT"** 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.

19. 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.

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 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(c), 1030.320(c).

22. 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.²³

Financial institutions are required to file complete and accurate reports that incorporate all relevant information available. 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.²⁴

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.²⁵ 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.

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).²⁶

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),²⁷ Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300),²⁸ Report of Foreign Bank and

23. 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).

24. 31 U.S.C. § 5318(g)(3); see, e.g., 31 C.F.R. § 1020.320(f).

25. See, e.g., 31 C.F.R. §§ 1020.320(b)(3), 1022.320(b)(3), 1023.320(b)(3).

26. 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.

27. 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.

28. 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. A Form 8300 also may be filed voluntarily for any suspicious transaction, even if the total amount does not exceed \$10,000.

Financial Accounts (FBAR),²⁹ Report of International Transportation of Currency or Monetary Instruments (CMIR),³⁰ Registration of Money Services Business (RMSB),³¹ and Designation of Exempt Person (DOEP).³²

Form 8300 Filing Instructions

When filing a Form 8300 involving a suspicious transaction relevant to this Alert, FinCEN requests that the filer select **Box 1b** (“suspicious transaction”) and include the key term **“FIN2026FOREIGNAGENT”** in the **“Comments”** section of the report.

Due Diligence

Banks, brokers or dealers in securities, mutual funds, and futures commission merchants and introducing brokers in commodities 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.³³ Covered financial institutions are required to identify and verify the identity of beneficial owners of legal entity customers, subject to certain exclusions and exemptions.³⁴ Among other things, this facilitates the identification of legal entities that may be owned or controlled by foreign politically exposed persons.

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.³⁵ Covered financial institutions must establish risk-based controls and procedures for ascertaining the identities of nominal and

29. 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](#).

30. 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.

31. 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.

32. A report filed by banks to exempt certain customers from currency transaction reporting requirements. See 31 C.F.R. § 1020.315.

33. See 31 C.F.R. §§ 1020.210(a)(2)(v), 1023.210(b)(5), 1024.210(b)(6), 1026.210(b)(5).

34. See 31 C.F.R. §§ 1010.230(f), 1010.605(e)(1) (defining “covered financial institution”).

35. 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).

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.³⁶

AML/CFT program and correspondent account due diligence requirements

Financial institutions are reminded of AML/CFT program requirements,³⁷ 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.³⁸ 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.³⁹

Information Sharing

Information sharing between and among financial institutions is critical to identifying, reporting, and preventing illicit activity, including the exploitation of certain cross-border transactions originated by MSBs. 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.⁴⁰ 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.⁴¹

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.

36. See 31 C.F.R. § 1010.620(c).

37. 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.

38. See 31 C.F.R. § 1010.610.

39. See MSB Interpretive Release, *supra* note 4; 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).

40. See 31 C.F.R. § 1010.540; see also FinCEN, “[Section 314\(b\) Fact Sheet](#)” (June 12, 2026).

41. See FinCEN, FIN-2025-G001, “[Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality](#)” (Sept. 5, 2025).

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

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. 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 for 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>.

FinCEN'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 AML/CFT programs and suspicious activity monitoring systems to help generate highly useful information for law enforcement and national security agencies.

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 ois.fincen.gov/contact/.

FinCEN's mission 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.