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

Washington, D.C. 20220

FIN-2025-G001

Issued: September 5, 2025

Subject: Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), in consultation with staffs of the Office of the Comptroller of the Currency (OCC), Federal Deposit Insurance Corporation (FDIC), and National Credit Union Administration (NCUA), is issuing this guidance to encourage and promote appropriate, voluntary cross-border sharing of information between and among financial institutions, including appropriate foreign financial institutions, to help combat the threats posed by money laundering, terrorist financing, and other illicit finance activity, including from drug trafficking organizations (DTOs), foreign terrorist organizations (FTOs), and fraudsters. This guidance seeks to: (i) clarify that the Bank Secrecy Act and its implementing regulations (collectively, the "BSA") generally do not prohibit cross-border information sharing;[1] and (ii) provide examples of information that typically would not reveal the existence of a Suspicious Activity Report (SAR) and, thus, that the BSA does not prohibit sharing.

This guidance does not alter or amend any existing legal obligations under the BSA or other statutes or regulations and does not impose any new regulatory requirements or supervisory expectations.[2] Further, this guidance does not replace any previous guidance[3] and does not establish or interpret any compliance standards.

[1] The BSA and FinCEN's implementing regulations prohibit sharing a SAR or any information that would reveal the existence or non-existence of a SAR except as permitted by statute or regulation. *See, e.g.*, 31 U.S.C. § 5318(g)(2)(A); 31 C.F.R. § 1020.320(e).

[2] Section 314(b) of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act) and its implementing regulations provide a safe harbor from liability when financial institutions share information provided certain conditions are met. *See* USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001), § 314(b); 31 C.F.R. §§ 1010.540(a), (b)(5). Nothing in this guidance affects the availability or scope of this safe harbor; this guidance is limited to information that financial institutions may choose to share outside the safe harbor.

[3] *See, e.g.*, FinCEN, Board of Governors of the Federal Reserve System, FDIC, OCC, Office of Thrift Supervision, *Interagency Guidance on Sharing Suspicious Activity Reports with Head Offices and Controlling Companies* (Jan. 20, 2006), https://www.fincen.gov/sites/default/files/guidance/sarsharingguidance01122006.pdf; FinCEN, FIN-2010-G006, *Sharing Suspicious Activity Reports by Depository Institutions with Certain U.S. Affiliates* (Nov. 23, 2010), https://www.fincen.gov/resources/statutes-regulations/guidance/sharing-suspicious-activity-reports-depository-institutions; FinCEN, Section 314(b) Fact Sheet (Dec. 10, 2020), https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf.

Cross-Border Information Sharing

Robust and appropriate sharing of financial information—such as transaction records, customer and account information, and investigative materials—that would otherwise be siloed at individual financial institutions amplifies financial institutions' collective ability to detect, prevent, and mitigate illicit finance activity. Financial institutions voluntarily sharing information with each other—including, but not limited to, their foreign affiliates and financial institutions to which they offer correspondent banking services—can make the U.S. and global financial systems more resilient by enabling individual financial institutions to form a more complete picture of threats, risks, and vulnerabilities posed by money laundering, terrorist financing, and other illicit finance activity. And, by providing that more complete picture, effective cross-border information sharing enables financial institutions to enhance their anti-money laundering/countering the financing of terrorism (AML/CFT) programs to better detect and prevent illicit finance activity and produce reports that are highly useful to law enforcement and national security agencies.[4]

FinCEN is therefore issuing this guidance to further facilitate U.S. financial institutions' appropriate and voluntary cross-border sharing of information with appropriate foreign financial institutions. In determining whether to share information, financial institutions should consider their risk profile, their relationship with the foreign financial institution, and other relevant information available to the financial institution. Financial institutions should also consider any relevant obligations arising under other U.S. legal authorities (including, but not limited to, the Right to Financial Privacy Act,[5] the Gramm-Leach-Bliley Act,[6] or state laws) and, as applicable, aspects of or obligations arising under foreign law, all of which are outside the scope of this guidance.

SAR Confidentiality

The BSA prohibits the disclosure of a SAR or information that would reveal the existence or non-existence of a SAR.[7] The BSA does not otherwise prohibit sharing "[t]he underlying facts, transactions, and documents upon which a SAR is based."[8] Thus, while SARs and information that would reveal the existence or non-existence of a SAR may not be shared, other than in limited circumstances,[9] the BSA does not prohibit financial institutions from sharing—including with U.S. and foreign financial institutions—the underlying facts, transactions, and documents upon which a SAR is based.

---

[4] *See* 31 U.S.C. § 5311(1).
[5] *See* Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3697 (Nov. 10, 1978), title XI, § 1100; *codified at* 12 U.S.C. § 3401 *et seq.*
[6] *See* Gramm-Leach-Bliley Act, Pub. L. No. 106-102; 113 Stat. 1228 (Nov. 12, 1999).
[7] *See* 31 C.F.R. § 1020.320(e); FinCEN, *Confidentiality of Suspicious Activity Reports*, 75 FR 75593, 75595 (Dec. 3, 2010) [hereinafter the "2010 Rule"] ("By extension, an institution also should afford confidentiality to any document stating that a SAR has *not* been filed. Were FinCEN to allow disclosure of information when a SAR is not filed, institutions would implicitly reveal the existence of a SAR any time they were unable to produce records because a SAR was filed."); *see also* 12 C.F.R. §§ 21.11(k), 163.180(d)(12), 353.3(g), 208.62(j), 748.1(d)(5).
[8] *See, e.g.*, 31 C.F.R. § 1020.320(e)(1)(ii)(A)(2).
[9] *See, e.g.*, 31 C.F.R. § 1020.320(e)(1)(ii)(B).

Although a reasonable and prudent person familiar with the SAR filing requirement may suspect or be able to deduce from these underlying facts, transactions, and documents that a SAR was filed, the underlying information alone would not constitute information revealing the existence of a SAR for confidentiality purposes.[10]

Exemplar Underlying Facts, Transactions, and Documents

While financial institutions should consider whether to share and what to share on a case-by-case basis, below is a non-exhaustive list of exemplar underlying facts, transactions, and documents that would not typically reveal the existence of a SAR and would not fall within the prohibition on disclosure in the BSA and implementing regulations.[11] However, when sharing such information, financial institutions must take appropriate measures (*e.g.*, redaction) to ensure that information that would reveal the existence of a SAR is not shared.

1. Transaction Information

- Wire transfer/payment information associated with specific natural or legal persons, including information on counterparties, amounts, account numbers, dates, and times.

- Information on, and records of, the amounts and dates of cash deposits, withdrawals, transfers, and other related records. This may include, but is not limited to, monetary instrument logs and deposit and withdrawal slips.

- Transaction logs that indicate whether specific accountholders have transacted with individuals or entities in specific jurisdictions.

2. Customer/Account Information

- Specific customer/account owners, including beneficial ownership information, and information about those customer/account owners.

- A list of the types of products and services offered to specific customers/accountholders and information related to these products and services.

- Information on the types of businesses in which legal entity customers have told the financial institution that they engage.

- Information on occupation, sources of funds, and/or sources of wealth provided to U.S. financial institutions.

[10] 2010 Rule, at 75595 n.13 ("[I]nformation produced in the ordinary course of business may contain sufficient information that a reasonable and prudent person familiar with SAR filing requirements could use to conclude that an institution likely filed a SAR (*e.g.*, a copy of a fraudulent check, or a cash transaction log showing a clear pattern of structured deposits). Such information, alone, does not constitute information that would reveal the existence of a SAR.").

[11] *See, e.g.*, *id.*

3. Investigative or other relevant materials

- Alerts (*e.g.*, those generated by a transaction monitoring system) or specific information about the potential illicit finance typology identified.

- Transaction information and customer/account information, as described above, that is stored in an investigation file or system.

- Research conducted on a customer or transaction (*e.g.*, due diligence research and information; adverse media).

- Analytic materials (*e.g.*, those created in connection with a case or investigation)—or portions of analytic materials—that do not bear on the SAR decision process (*e.g.*, those that do not opine on whether particular activity is or is not suspicious) or otherwise imply that a SAR decision has been made.

- Cyber-related data such as IP addresses, geolocations, and/or device identification numbers.

Handling Requests for SAR Information

FinCEN reminds financial institutions of their obligation to notify FinCEN—and, as applicable, other federal regulators[12]—if the financial institution receives a subpoena or other request to disclose a SAR or information that would reveal the existence of a SAR.[13] For example, FinCEN reiterates its 2012 *SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions*: "If you or your institution becomes aware of an unauthorized disclosure of a SAR, or if your institution receives a subpoena or other request for a SAR from [anyone] other than an authorized government authority or self-regulatory organization as defined in the applicable SAR regulations, you should immediately contact FinCEN's Office of Chief Counsel at 703-905-3590."[14] Additionally, a financial institution may be required to contact its primary federal regulator, as may be applicable in a corresponding SAR rule.

Financial institutions should also consult FinCEN's prior guidance when they receive a request for production of a SAR or information that would reveal the existence of a SAR.[15]

Questions or comments regarding this guidance should be addressed to the FinCEN Regulatory Support Section by submitting an inquiry at www.fincen.gov/contact.

---

[12] *See, e.g.*, 12 C.F.R. § 21.11(k)(1).
[13] *See, e.g.*, 31 C.F.R. § 1020.320(e)(1).
[14] FinCEN, FIN-2012-A002, *SAR Confidentiality Reminder for Internal and External Counsel of Financial Institutions* (Mar. 2, 2012), at p. 2, https://www.fincen.gov/sites/default/files/advisory/FIN-2012-A002.pdf.
[15] *See, e.g.*, FinCEN, *The SAR Activity Review, Trends Tips and Issues, Issue 7, August 2004* (July 31, 2004), at p. 46, https://www.fincen.gov/sar-stats/sar-activity-review/sar-activity-review-issue-7 ("The financial institution and its lawyer should also be careful not to disclose the existence of a Suspicious Activity Report in a response to the subpoena. Rather, the privilege log or other responsive pleading should refer generically to 'nonpublic supervisory information' or something similar in nature, and not to the Suspicious Activity Report itself.").