

Opening Up Fraud Talks With Customers After SAR Guidance

By **Liz Aloï, Deborah Connor and Marc-Alain Galeazzi** (October 21, 2026, 5:41 PM EDT)

For years, many financial institutions treated silence as the safest response when a customer asked why an account had been restricted or closed, a transaction delayed or a deposit rejected. Bank Secrecy Act confidentiality rules governing suspicious activity reports are strict, and the consequences of revealing a filing are serious.

Federal regulators have now made clear, however, that the law does not require silence.

The Joint Statement

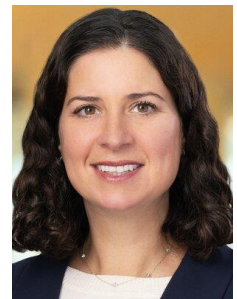
On Sept. 2, the Federal Reserve, the Federal Deposit Insurance Corp., the National Credit Union Administration, the Office of the Comptroller of the Currency and the U.S. Department of the Treasury's Financial Crimes Enforcement Network issued a joint statement clarifying how banks and credit unions can communicate with customers about suspicious or potentially fraudulent activity without violating SAR confidentiality requirements.[1]

The joint statement confirms that SAR confidentiality requirements do not preclude banks from communicating with their customers regarding potentially fraudulent transactions and other suspicious activity or account closures.

The agencies emphasized that the joint statement does not alter existing BSA legal or regulatory requirements and does not establish new supervisory expectations. That qualification is important. The agencies are not relaxing SAR confidentiality or requiring financial institutions to disclose more to customers. They are, however, clarifying the room institutions already have under existing law to communicate about the facts and transactions underling the SAR without revealing whether a SAR has been, will be or will not be filed.

For institutions that have historically adopted a highly conservative approach to customer communications, that clarification may nevertheless have meaningful practical consequences.

The Fine Print



Liz Aloï



Deborah Connor



Marc-Alain Galeazzi

The core legal principles highlighted in the joint statement are not new. The BSA prohibits disclosing a SAR itself, or information that would reveal the existence or nonexistence of a SAR. The BSA does not make the underlying facts, transactions or documents confidential merely because they formed the basis for a SAR.

The joint statement applies that distinction directly to customer communications. As the agencies explain, although a "reasonable and prudent person familiar with the SAR filing requirements" may suspect or be able to deduce from the information provided by the bank that a SAR was or may have been filed, disclosure of the underlying information alone does not reveal the existence of a SAR.

That is an important framing. The key question is not whether a knowledgeable customer might infer that suspicious activity reporting could be occurring but instead whether the institution has actually revealed the existence or nonexistence of a SAR.

The agencies provide a nonexhaustive list of communications that would not typically reveal a SAR's existence. These include:

- Requesting customer due diligence information;
- Telling a customer that a delay, limitation, restriction or closure may be related to suspected fraud or other suspicious activity;
- Telling a customer that a deposit has been rejected because of suspected fraud, including altered or counterfeit checks;
- Asking about transaction purpose or source of funds;
- Providing warnings about fraud schemes or money-mule activity;
- Communicating account maintenance or service decisions, such as declining a transaction or closing an account; and
- Asking for information about the originator or beneficiary of a funds transfer.

The clarification also extends beyond direct customer communications. The agencies reaffirm that the underlying facts, transactions and documents, where otherwise permissible, may be shared with third parties, including other financial institutions, as long as the communication does not reveal the existence of a SAR.

None of this creates a safe harbor. The agencies advise banks and credit unions to consider customer communications on a case-by-case basis and to take precautions when discussing information that could reveal the existence of a SAR. Context matters, and institutions should not simply rely on a list of approved words or phrases.

Nor does the distinction between the SAR and its underlying facts mean that everything contained in an institution's SAR investigation file may be freely disclosed. Institutions must still protect the SAR itself, the decision whether to file a SAR and information that would reveal whether a SAR exists. The practical message is therefore narrower, but still significant: SAR confidentiality does not require silence about otherwise disclosable facts simply because those facts also appear to have led to a SAR.

Why Now?

The joint statement arose from both a June 20, 2025, request for information on payments fraud and the fair banking concerns reflected in President Donald Trump's Aug. 7, 2025, executive order on guaranteeing fair banking access and preventing debanking.[2] The joint statement also fits within the federal government's broader focus on fair access to financial services.

The 2025 request issued by the Fed, FDIC and OCC elicited information about potential actions to help consumers, businesses and financial institutions mitigate the risk of payments fraud. Commenters told the agencies that frontline staff and fraud operations teams were often unsure how much they could tell a customer about the reasons behind restrictions, delays or closing related to an account.

The debanking order declares that banking decisions should be based on individualized, objective, risk-based analyses rather than constitutionally or statutorily protected beliefs or affiliations. It lays out a framework to remove the use of reputational risk from regulatory guidance documents and explicitly withdraws earlier guidance encouraging banks to assess reputational risk. It also directs the banking regulators to develop a strategy to combat politicized or unlawful debanking activities across the federal government.

The executive order has been praised by industry groups such as the Bank Policy Institute, but it is a policy priority that only works if banks can actually explain their decisions to the people affected by them. In other words, for a financial institution to demonstrate to customers with account restrictions that it is acting consistent with the executive order, it may need to say more about what activity was suspicious leading to the restriction. The joint statement gives guidance on how banks may do that.

The Shift Toward Information Sharing

The joint statement also should be understood as part of a broader FinCEN effort to clarify the boundaries of SAR confidentiality. On Sept. 5, 2025, FinCEN issued guidance on cross-border information sharing by financial institutions.[3] That guidance was designed to encourage and promote voluntary information sharing to combat money laundering and other illicit-finance threats. FinCEN clarified that the BSA and its implementing regulations generally do not prohibit financial institutions from sharing information across borders and identified categories of information that typically would not reveal the existence of a SAR, including information about customers, account owners and beneficial owners.

Taken together, the 2025 guidance and 2026 joint statement suggests a coordinated effort to address a recurring compliance problem: that institutions sometimes interpret SAR confidentiality more broadly than the regulations require and in doing so, restrict potentially useful communications that the BSA itself does not prohibit. The joint statement closes the gap between what the law permits and what compliance departments, understandably, have treated as permitted.

Takeaways

First, institutions should review their existing customer-facing scripts, call-center guidance, and closure or restriction notices. Materials that categorically state that the institution cannot discuss an account action because of regulatory requirement may reflect a broader interpretation of SAR confidentiality than the law requires.

In general, banks and credit unions should consider customer communication on a case-by-case basis and take precautions when discussing information that could reveal whether a SAR exists.

Second, frontline and fraud investigation staff should understand the distinction between describing underlying facts and revealing the existence of a SAR. That distinction may be easy to lose track of during a live conversation with a frustrated customer. Training should emphasize that the joint statement does not authorize employees to confirm or deny a SAR filing merely because they are permitted to discuss some of the underlying conduct.

Institutions also may want to document significant customer communications contemporaneously, particularly where the communication relates to suspected fraud, account restrictions or closures. Smaller compliance departments should not assume the joint statement's flexibility comes with less documentation burden; if anything, a leaner compliance function benefits most from having a short, clear internal decision tree with clear documentation for what frontline staff can say, since there may be no compliance officer immediately available to make a judgment call in real time.

Third, institutions should consider how the clarification applies to third parties and service providers. Credit unions and smaller banks in particular may rely on shared service providers, core processors, fraud-monitoring vendors or other contracted entities that interact directly with customers.

For outside and in-house counsel advising banks and credit unions, the joint statement therefore changes the practical risk analysis even though it does not change the law. It provides clearer guidance about what institutions may communicate and offers an opportunity to reconsider policies that may have treated SAR confidentiality as requiring blanket silence.

The agencies have not weakened SAR confidentiality or created a right to a customer explanation. What they have done is draw a clearer line around what SAR confidentiality never covered in the first place. For institutions that have historically stayed well back from that line, the joint statement provides an opportunity to reassess whether their customer communications and escalation procedures strike the right balance between protecting SAR confidentiality and communicating information permitted to be shared by law.

Liz Aloj is of counsel at Morrison Foerster LLP. She previously served as chief of the Special Financial Investigations Unit in the U.S. Department of Justice's Money Laundering and Asset Recovery Section.

Deborah Connor is a partner at MoFo. She previously served as chief of the Money Laundering and Asset Recovery Section at the DOJ.

Marc-Alain Galeazzi is a partner at MoFo.

The opinions expressed are those of the author(s) and do not necessarily reflect the views of their employer, its clients, or Portfolio Media Inc., or any of its or their respective affiliates. This article is for general information purposes and is not intended to be and should not be taken as legal advice.

[1] FinCEN, "FinCen, Agencies, Issue Joint Statement on Suspicious Activity Report Confidentiality Considerations Regarding Communications with Customers" (Sept. 2026), available at <https://www.fincen.gov/news/news-releases/fincen-agencies-issue-joint-statement-suspicious-activity-report-confidentiality>.

[2] Available at <https://www.whitehouse.gov/presidential-actions/2025/08/guaranteeing-fair-banking-for-all-americans/>.

[3] FinCEN, "Cross-Border Information Sharing by Financial Institutions and SAR Confidentiality," FIN-2025-G001 (Sept. 2025); see also 31 C.F.R. § 1020.320(e)(1)(ii), available at <https://www.fincen.gov/resources/statutes-regulations/guidance/cross-border-information-sharing-financial-institutions-and>.