IRS-CI

CI-FIRST

FINTAX KNOWLEDGE EXCHANGE ALERT

SUSPICIOUS ACTIVITY REPORTS (SARs):

Where Financial Institutions and IRS Criminal Investigation (IRS-CI) Connect

THE VALUE OF SARs

SARs serve as powerful tools to protect the U.S. financial system. Each SAR provides valuable insights that help IRS-CI and other agencies:

- Identify emerging threats
- Trace illicit funds
- Disrupt criminal networks

IRS-CI SAR Review Team investigations have led to the seizure of $385 million in illicit funds and assets during fiscal years 2023-2025.

IRS-CI USES SARs TO:

Generate Leads: SARs help agents track illicit funds, corroborate evidence, and prioritize cases.

Drive Investigations: SARs provide key financial intelligence that helps IRS-CI identify, develop, and support criminal cases.

Reveal Emerging Threats: Patterns in SARs expose money laundering, tax evasion, drug trafficking, fraud, and other financial crimes.

Connect the Dots: Special agents and investigative analysts use SARs to uncover relationships between individuals, businesses, and networks tied to illicit activity.

Protect the Financial System: SARs give IRS-CI the visibility to follow the money, dismantle criminal networks, and safeguard the integrity of the U.S. financial system.

WHO READS YOUR SAR?

- **SAR Review Team Coordinators**
- **Law Enforcement (Case Agent and Investigative Analyst)**
- **National Security Agencies**
- **Financial Crimes Enforcement Network (FinCEN)**
- **Office of Foreign Assets Control (OFAC)**
- **Regulators and Examiners**

DID YOU KNOW?

IRS-CI has 182 SAR Review Team Coordinators that lead or participate in SAR Review Teams in each of the 94 judicial districts.

SIX THINGS TO INCLUDE IN A SAR NARRATIVE

WHO: Identify all parties involved and their relationships.

WHAT: Describe the specific activity or transaction type.

WHEN: Include exact dates, frequency, and duration.

WHERE: Name institutions, branches, or geographic areas.

WHY: Explain why the activity appears irregular, unusual, or inconsistent with the customer's profile.

HOW: Address how the suspicious activity was conducted, such as method, pattern, or behavior.

SUSPICIOUS ACTIVITY REPORTS (SARs)

TIPS FOR WRITING USEFUL SAR NARRATIVES

Paragraph #1	**Start your narrative with a hook:** Engage your reader with a strong introduction identifying why this activity is suspicious.
Paragraph #2	**Provide background of the subjects:** Identify the subject(s) who is/are conducting the suspicious activity and provide all available information.
Paragraph #3	**Describe what took place:** Outline the suspicious activity in a logical sequence and easy-to-read format. Consider drafting a timeline.
Paragraph #4	**Summarize the key points:** Provide a clear and concise summary recapping the suspicious activity, red flags, and how it happened.
Paragraph #5	**Include details about supporting documentation:** List supporting documents available to law enforcement, and include a contact email that law enforcement can use to request the documents. This is one of the most important parts of the SAR narrative; FinCEN SAR guidance requires financial institutions to include this information.

TIP → **A concise, factual, chronological narrative helps IRS-CI connect your SAR to other data sources quickly.**

USEFUL SUPPORTING DOCUMENTATION

- **Account opening documents**
- **Beneficial Ownership forms**
- **Account statements**
- **Wire transfer forms**
- **Loan documents, including credit files**
- **High Risk Customer Review**
- **AML transaction monitoring alerts**
- **Open-source research (OSINT)**
- **314(b) responses, if applicable**
- **Video surveillance of the subject conducting the transactions**
- **Deposit items, cancelled checks, general ledgers, teller logs**

* ***Documented correspondence or outreach with the subject***

Useful Digital & Non-Traditional Identifiers

» IP addresses and timestamps
» Virtual-asset wallet addresses and transaction hashes
» Two-factor authentication logs
» Changes in contact information
» Domain names, fintech, or app usernames
» Mobile banking and mobile apps transactions records
» Email and chat handles, including chat timestamps and participants
» Device IDs, photo metadata, or geolocation
» Social media or online monikers
» Routing or settlement path data
» Linked accounts or credentials (shared IPs, devices, etc.)
» Login frequency, duration, and behavioral biometrics

Investigative Value: Metadata Matters

Metadata provides digital fingerprints that can:

- Identify linked accounts, devices, or IP addresses across institutions and subject activity.
- Reconstruct timelines to determine when funds or assets moved through multiple layers.
- Support digital forensics and attribution to specific individuals or entities.
- Corroborate SAR narratives and support subpoenas.

Combatting illicit financial activity requires collaboration between the private and public sectors.

If you have filed a SAR related to a financial threat, please contact CI-FIRST at cifirst@ci.irs.gov with the BSA ID number. ***All SAR information is confidential.***

For training opportunities or to learn more about IRS-CI and emerging threats, email cifirst@ci.irs.gov.