Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2010-A014
Issued: November 23, 2010
Subject: Maintaining the Confidentiality of Suspicious Activity Reports

---

In conjunction with updating our regulations relating to the confidentiality of Suspicious Activity Reports (SARs),[1] the Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to regulatory and law enforcement agencies, self-regulatory organizations (SROs), and financial institutions to reinforce and reiterate the requirement to preserve the confidentiality of SAR information.[2] As information contained in SARs becomes more widely used as a resource for investigations and examinations, the need to remain vigilant about protecting the confidentiality of SAR information increases. Recent media reports of possible disclosure incidents have increased concerns that SAR confidentiality requirements may not have been appropriately followed.

FinCEN, as administrator of the Bank Secrecy Act (BSA), is responsible for both safeguarding the information it collects and maintaining the integrity of the BSA records and reports, including SARs. The unauthorized disclosure of SARs could undermine ongoing and future investigations by tipping off suspects, deter financial institutions from filing SARs, and threaten the safety and security of institutions and individuals who file such reports. Further, such disclosure of SARs compromises the essential role SARs play in protecting our financial system and in preventing and detecting financial crimes and terrorist financing. The success of the SAR reporting system depends upon the financial sector's confidence that these reports will be appropriately protected.

FinCEN encourages organizations and authorities, both governmental and non-governmental, to be vigilant in ensuring SAR confidentiality is maintained. This includes making certain all employees, agents, and individuals appropriately entrusted with information in a SAR are informed of the individual obligation to maintain SAR confidentiality. This obligation applies not only to the SAR itself but also to information that would reveal the existence of the SAR. Likewise, such persons should also be informed of the consequences for failing to maintain such confidentiality, which could include civil and criminal penalties as explained herein.

---

[1] *See* 31 U.S.C. § 5318(g)(2) and 31 CFR §§ 103.15(d), 103.16(f), 103.17(e), 103.18 (e), 103.19(e), 103.20(d), and 103.21(e).

[2] The SAR confidentiality provisions clarify that both the SAR itself and any information that would reveal the existence of a SAR are confidential, and shall not be disclosed except as specifically authorized therein.

A financial institution may want to consider including such information as part of its ongoing training of all employees. Additional risk-based measures to ensure the confidentiality of SARs could include, among other appropriate security measures, limited access on a "need-to-know" basis, restricted areas for reviewing SARs, logging of access to SARs, the use of cover sheets for SARs, or supporting documentation that indicates the filing of a SAR, or electronic notices that highlight confidentiality concerns before a person may access or disseminate the information.

Similarly, law enforcement and regulatory authorities and SROs should implement robust programs to protect the confidentiality of SARs and information that would reveal the existence of a SAR. Among other things, these programs should focus on educating all users of SAR information of their responsibilities and the importance of SAR confidentiality, and should establish controls that safeguard against inappropriate use of, and access to, SAR data. The obligation to preserve the confidentiality of SARs applies equally to government officials and SROs, and SARs must remain confidential even if law enforcement, regulatory or SRO authorities obtain them directly from financial institutions.

The unauthorized disclosure of SARs is a violation of federal law.[3] Both civil and criminal penalties may be imposed for SAR disclosure violations. Violations may be enforced through civil penalties[4] of up to $100,000 for each violation and criminal penalties[5] of up to $250,000 and/or imprisonment not to exceed five years.[6] In addition, financial institutions could be liable for civil money penalties resulting from anti-money laundering program deficiencies (i.e., internal controls, training, etc.) that led to the improper SAR disclosure. Such penalties could be up to $25,000 per day for each day the violation continues.[7] FinCEN is committed to working with regulatory agencies, law enforcement, SROs, and financial institutions to take appropriate action for unauthorized disclosures of SARs. Incidents involving unauthorized SAR disclosures are investigated and appropriate action is taken for someone found to be in violation of the law.

If you or your institution becomes aware of an unauthorized disclosure of a SAR or if your institution receives a subpoena for a SAR, you should immediately contact FinCEN's Office of Chief Counsel at (703) 905-3590 as well as your primary federal regulator, as may be applicable in a corresponding SAR rule. If you have any questions regarding this Advisory, please contact FinCEN's Regulatory Helpline at (800) 949-2732.

[3] 31 U.S.C. §§ 5318(g)(2), 5321, and 5322.
[4] 31 U.S.C. § 5321 and 31 CFR § 103.57.
[5] 31 U.S.C. § 5322 and 31 CFR §103.59.
[6] Criminal penalties may increase if the violation is committed while violating another law of the United States or as part of a pattern of illegal activity. 31 U.S.C. § 5322(b) and 31 CFR § 103.59(c).
[7] 31 U.S.C. § 5321(a)(1).