WINSTON & STRAWN LLP

BLOG

FinCEN Advisory on Cyber-Crime Includes Details for Completing SARs

NOVEMBER 15, 2016

The Financial Crimes Enforcement Network (FinCEN) of the Treasury Department recently issued an advisory and a related FAQ for financial institutions on combating cyber-events and cyber-enabled crime. The stated goal of the advisory is to help reduce cyber risks for financial institutions, but it also serves as a reminder about reporting obligations and expectations such organizations have in the event of a cyber-incident.

The advisory reminds financial institutions that they may have cyber-related reporting obligations imposed by any applicable functional regulators, and that should they have an obligation to complete a Suspicious Activity Report (SAR), they should include relevant cyber information in the SARs. Under the Bank Secrecy Act, financial institutions are required to file SARs to report suspicious activity, including identity theft. It has not always been clear when a SAR should be filed in the event of a cyber incident, and the advisory attempts to clarify when in such situations a SAR filing might be required. For example, if cyber criminals gain access to a bank's systems and (in the FinCEN example) $500,000 of the customers' funds are put at risk. Or, if cyber criminals acquire sensitive customer information useful to conduct fraudulent transactions. FinCEN is particularly interested in having financial institution SARs provide the agency with information FinCEN can use to help prevent fraud or money laundering. This might include IP address information, time stamps, device identifiers, and the like. The FAQ provides detailed information about how to complete cyber-related SARs.

The advisory also encourages collaboration within financial institutions—between employees combating cyber-crime and employees combating money laundering. In the advisory FinCEN supported information sharing *within* a financial institution: anti-money laundering teams will be more effective with digital intelligence from the cybersecurity team, and cybersecurity teams will more effectively combat cyber-crime with input from the fraud experts FinCEN argues. FinCEN also supports information sharing *between* financial institutions to again more effectively combat cyber crime.

TIP: This advisory demonstrates FinCEN's hope that organizations will collaborate and share information to help combat cyber-crime, whether such information sharing is statutorily required, or provided voluntarily. This advisory reflects a trend of encouraging sharing, such as the 2015 Cybersecurity Information Sharing Act.

2 Min Read

Related Locations

Chicago

Related Topics

Financial Privacy

Related Capabilities

Intellectual Property | Privacy & Data Security | Financial Services

Related Regions

North America

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.