Department of the Treasury
Financial Crimes Enforcement Network

Advisory

FIN-2011-A016
Issued: December 19, 2011
Subject: Account Takeover Activity

The Financial Crimes Enforcement Network (FinCEN) is issuing this Advisory to assist financial institutions with identifying account takeover activity and reporting the activity through the filing of Suspicious Activity Reports (SARs).[1]

Identifying Account Takeover Activity

Cybercriminals are increasingly using sophisticated methods to obtain access to accounts, including the use of malware (malicious software), SQL injection attacks (SQLIA), spyware, Trojans, and worms.[2] These attacks aim to deliberately exploit a customer's account and, in many instances, to gain seemingly legitimate access to another customer's account. Through ongoing monitoring, financial institutions may identify inconsistencies with a customer's normal account activity that indicates illicit intrusions into a customer's account. Such irregularities might include, but are not limited to, unusual ATM activity, clustered Automated Clearing House (ACH) transactions in different geographic areas, sudden wire transfers, or changes to customer and account profiles.

Account takeover activity differs from other forms of computer intrusion, as the customer, rather than the financial institution maintaining the account, is the primary target. Computer intrusion may be defined as gaining access to a computer system of a financial institution to: a) remove, steal, procure or otherwise affect funds of the financial institution or the institution's customers; b) remove, steal, procure or otherwise affect critical information of the financial institution including customer account information; or c) damage, disable, disrupt, impair or otherwise affect critical systems of the financial institution.[3] In an account takeover, at least one of the targets is a customer holding an account at the financial institution and the ultimate goal is to remove, steal, procure or otherwise affect funds of the targeted customer.

Suspicious Activity Reporting

If a financial institution knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the financial institution involves funds derived

---

[1] In developing this Advisory, FinCEN consulted with the Federal Bureau of Investigation and the Financial Services Information Sharing and Analysis Center.
[2] For more information and resources on cybercrime techniques and updates, *see* United States Department of Justice's Computer Crime & Intellectual Property Section, http://www.cybercrime.gov/.
[3] *See* "SAR Activity Review Trends, Tips, and Issues," Issue 3, pp. 38-41 (October 2001). http://www.fincen.gov/news_room/rp/files/sar_tti_03.pdf#page=44. The definition also appears in the instructions to the SAR-DI (TD F 90-22.47).

from illegal activity or an attempt to disguise funds derived from illegal activity, is designed to evade requirements under the Bank Secrecy Act ("BSA"), or lacks a business or apparent lawful purpose, the financial institution may be required to file a SAR.[4] When completing SARs on suspected account takeover activity, financial institutions should use the term "account takeover fraud" in the narrative section of the SAR and provide a detailed description of the activity. Financial institutions may wish to take the following examples into account when filling out the Suspicious Activity Information section to further enhance the usefulness of their filings:[5]

- If the account takeover involves computer intrusion, check the box for "computer intrusion." In addition, financial institutions can check the "other" box and note "account takeover fraud" in the space provided.

- If the account takeover involved other delivery channels such as telephone banking or fraudulent activities such as social engineering, financial institutions can check the "other" box, note "account takeover fraud," and include a short description of the additional information in the space provided.

- If the account takeover involves a wire transfer, then in addition to selecting the "other" box and noting "account takeover fraud," the box for "wire transfer fraud" should be checked.

- If the account takeover involves an ACH transfer, financial institutions can check the "other" box and note "account takeover fraud – ACH."

- Account takeovers often involve unauthorized access to PINs, account numbers, and other identifying information. Financial institutions may need to check the box for "identity theft," in addition to selecting the "other" box and noting "account takeover fraud." Additional boxes should be checked if appropriate (e.g. "terrorist financing").

Questions or comments regarding the contents of this Advisory should be addressed to the FinCEN Regulatory Helpline at 800-949-2732. ***Financial institutions wanting to report suspicious transactions that may relate to terrorist activity should call the Financial Institutions Toll-Free Hotline at (866) 556-3974 (7 days a week, 24 hours a day).*** The purpose of the hotline is to expedite the delivery of this information to law enforcement. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.

---

[4] *See e.g.* 31 CFR § 1020.320.

[5] Although these suggested steps are not directly applicable to FinCEN's new SAR (OMB Control Number 1506-0065, approved July 15, 2011), when FinCEN requires financial institutions to use the new SAR financial institutions should take these suggested steps into account as indicators of the appropriate level to detail to provide when reporting suspected account takeover activity.