BEST PRACTICES TO REDUCE CORPORATE ACCOUNT TAKEOVER

FREQUENTLY ASKED QUESTIONS

Question: **What is the difference between the FFIEC Supplemental Guidance and the "Best Practices"?**

Answer: The primary difference is the focus and depth of the documents. The "Best Practices" is more comprehensive. The *FFIEC Supplement to Authentication in an Internet Banking Environment* focuses on recommending controls to properly authenticate a customer. The "Best Practices" address this as well, but were developed to focus on how to implement controls (with specific options provided) and how to specifically respond to a theft. It was structured in a format to assist the industry in quickly protecting itself against these thefts. Additionally, the focus is on controls just related to corporate accounts. The FFIEC Supplemental Guidance includes some requirements for consumer accounts.

Question: **Our financial institution does not utilize on-line corporate banking. Do we have to implement a risk management program?**

Answer: An entire corporate account takeover risk management program is not needed if on-line banking services are not offered to corporate customers. This should be documented in a risk assessment. Please be aware that the FFIEC Supplemental Guidance addresses expectations regarding BOTH corporate and retail accounts. If your financial institution offers on-line banking services to retail/consumer accountholders, then, at a minimum, action will be needed related to enhanced authentication for your on-line retail customers. If you do not provide any on-line banking services or telephone voice response systems, you will need to document this in a risk assessment.

Question: **Should we notify the California Department of Business Oversight of previous takeovers we have dealt with to add to their records?**

Answer: The California Department of Business Oversight does not need to be notified, however, a Suspicious Activity Report (SAR) should be filed with FinCEN on any incidents not previously reported. New guidelines, regarding information to provide in a SAR when identifying and reporting account takeover activity, are found in FinCEN Advisory 2011-A016 issued in December 2011.

Question: **Should institutions file Suspicious Activity Reports (SARs) if they discover what appears to be a Money Mule's account at their institution?**

Answer: Yes, if you suspect an account is receiving stolen funds, you should file a SAR. In addition, recent amendments to NACHA rules, effective January 1, 2012, may allow your institution to delay making the funds available, if you reasonably suspect that the ACH credit is not authorized.

Question: **Where is the best place to look for contact information on institutions that received money transferred from our institution during a corporate account takeover theft?**

Answer: Institutions that have been involved with these types of thefts report that one of the most frustrating aspects of trying to recover the stolen money is locating and talking to the appropriate person at the receiving institution. The California Department of Business Oversight recommends starting with the phone number of the receiving institution's ACH department that can be found using the Federal Reserve's Fed ACH Directory. You can search the directory using the routing number for the receiving institution.

Question: **Can the corporate account takeover risk assessment be added to our existing IT assessment?**

Answer: Yes, the method of assessing the risk is completely up to the institution.

Question: **When a Corporate Account Takeover theft occurs, are the wire and ACH transactions generally sent out of the country, or do they go to accounts within the United States?**

Answer: The thefts involved transactions where the funds were initially sent to money mule accounts within the United States. The money mules quickly transferred the stolen funds either to an overseas account or to another intermediate account in the United States before being transferred out of the country.

Question: **Is there a recommended timeframe for providing the Board with an outline of these thefts and the actions our institution is taking?**

Answer: No specific timeframe was designated in the "Best Practices" document since institutions vary in size and complexity. Providing the Board with at least an estimate of the number of corporate customers performing on-line transfers is recommended. Some Boards might want to review the customer education material on corporate account takeovers, since they, too, may be small business owners at risk. Multiple briefings on the implementation of an institution's risk management program are appropriate.

Question: **Is NACHA changing the rules in the event of a fraudulent event? We had an event almost 2 years ago and we started making phone calls to 38 institutions involved immediately, but it did not help because the money was already out of the mule's accounts.**

Answer: NACHA implemented a new rule on Corporate Account Takeover: Voluntary Availability Exception Option for RDFIs, which was effective January 1, 2012. This new rule provides an option for an RDFI to take advantage of a voluntary exception from the existing funds availability requirement prescribed within the Rules for an ACH credit when the RDFI reasonably suspects that the ACH credit is not authorized. The additional time might enable ODFIs and RDFIs to identify unauthorized credit entries due to corporate account takeover, and recover funds on behalf of originators. Refer to the 2012 NACHA Operating Rules & Guidelines, pages OR31 and OR36, Section 3.3, Subsection 3.3.1.1 and 3.3.1.2.

Question: **When rating customers, can institutions incorporate the BSA ratings?**

Answer: The purpose of rating (or ranking) corporate customers is simply to help identify those customers at greatest risk and then to assist the institution in determining how to implement their risk management program. Any method that works to achieve those goals is satisfactory. The “Best Practices” provides some suggested criteria for rating (or ranking) customers.

Question: **What should we tell the customer to do if they think they may have malware on their computer (i.e. they clicked on a link, etc.)?**

Answer: If the deceptive link was received through typical malware distribution methods (such as fake emails that are known to be circulating) and the malware is presumed to have been installed, the customer should be advised to contact computer/security professionals to clean and secure their computer system. Cleaning and securing a computer network (or even individual computers) can be complicated and requires detailed knowledge of the network configuration and how the computers at the business are used. The institution should also strongly consider disabling the customer's on-line access until notified by the customer that the malware has been removed. Once the malware has been removed, the customer's access credentials may be reset.