ACH Operations Bulletin #1-2017

Social Engineering Fraud Against Public-Sector and Other Entities

February 16, 2017

EXECUTIVE SUMMARY

This ACH Operations Bulletin provides information to Participating Depository Financial Institutions and their business customers about a specific type of social engineering fraud that is targeting public-sector entities. Fraudsters have used these social engineering techniques to manipulate public-sector entities into redirecting legitimate vendor payments to accounts controlled by the fraudsters. Although any business entity could be the target of this type of social engineering attack, public-sector entities seem to be specifically targeted because their contracting information is often a matter of public record.

This ACH Operations Bulletin also provides guidance for financial institutions on some steps that they and their Originators each can take to reduce their respective vulnerabilities to this type of fraud.

SOCIAL ENGINEERING FRAUD

Several recent news articles have highlighted successful social engineering fraud carried out against public-sector entities that have resulted in monetary losses. Each of these reported cases has a similar fact pattern. A public-sector agency or entity, such as a municipal government agency or a public university or college, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payments along with routing and account information. In these cases, the update did not come from the contactors themselves but from fraudsters. As described in the articles, the public entities that used the "updated" information actually sent payments to the fraudsters, resulting in losses to the public entities.

This social engineering scenario is similar to the Business Email Compromise (BEC) scenarios that were described in alerts from the Financial Services - Information Sharing and Analysis Center (FS-ISAC) and the Federal Bureau of Investigation (FBI) in 2015, and many of their recommendations are applicable to this scenario as well. The main difference is that instead of impersonating a corporate official (CEO or CFO) and ordering a payment to be made, in this scenario the fraudsters impersonate a legitimate contractor or vendor and order the change in payment information from legitimate instructions to reference a fraudulent account.

Several of the articles further suggest that the funds are being moved out of the country (China is prominently referenced). As most public-sector entities will not have the ability to initiate International ACH Transactions, other means are presumably being employed. For example,

after funds are deposited via an incoming ACH credit or wire transfer, they may be subsequently wired out of the country or otherwise withdrawn.

In a statement quoted in an article on January 20, 2017, the FBI characterized one of these cases as business email compromise, and that there is "absolutely no suspicion or indication that this fraud involved the manipulation or compromising of the Automated Clearing House banking transfer system."

PUBLIC-SECTOR ENTITIES ARE BEING TARGETED

Although any business entity could be the target of this type of social engineering attack, public-sector entities seem to be specifically targeted because their contracting information is typically a matter of public record. Fraudsters use information from such public records to more convincingly impersonate legitimate contractors.

GUIDANCE FOR FINANCIAL INSTITUTIONS AND CUSTOMERS

Financial institutions should consider alerting their business customers to this type of social engineering attack, especially those in the public sector, as well as similar types of entities such private universities and colleges, non-profits, and other nongovernmental organizations (NGOs). Financial institutions and their customers should not consider these types of social engineering attacks solely as hacking, phishing or cybercrime. Parties should know that the vectors for these attacks are not necessarily through Internet-based methods; while some come by email, others come as phone calls, faxes or letters in the mail.

As noted in the FS-ISAC alert, a method for to reduce the risk of falling victim to this scam is to authenticate any request to make a payment or change payment instructions to a contractor or vendor, and independently verify a change in payment instructions using out-of-band verification techniques, especially when the request cannot be authenticated. The phone number or other contact information used for this verification should not come from the communication requesting the change, but should instead be taken from a known and trusted contact list for that contractor or vendor.

For those entities that make forms available online for contractors to submit ACH or payment information, verification of a change in payment information should not rely solely on contact information provided in such forms. Additionally, entities should consider making such forms available only via secure means, whether online or offline. Entities should take seriously any call they receive from their financial institution questioning the legitimacy of a payment.

Receiving financial institutions may want to review procedures for identifying money mules, as a similar fact pattern may occur with this social engineering fraud. The receipt of one or more large dollar ACH credits or wire transfers into a new account, followed shortly by a withdrawal or a wire transfer order, may be indicative of fraudulent activity, depending on the totality of the circumstances.

These steps are suggestions only; each financial institution, both those that receive and those that send payment instructions, as well as each Originator, should consider the risk management practices best tailored to its individual programs and circumstances.

RESOURCES ON CURRENT FRAUD THREATS AND BUSINESS EMAIL COMPROMISE

NACHA
Current Fraud Threats Resource Center
https://www.nacha.org/content/current-fraud-threats-resource-center

FS-ISAC
Fraud Alert – Business E-mail Compromise Continues to Swindle and Defraud U.S. Businesses - June 19, 2015
https://www.fsisac.com/sites/default/files/news/BEC_Joint_Product_Final.pdf

FBI
Business E-Mail Compromise; An Emerging Global Threat - August 28, 2015
https://www.fbi.gov/news/stories/business-e-mail-compromise