Account Takeover: What You Need to Know

Sound Business Practices to Mitigate Risk

Preventing and mitigating the effects of Corporate Account Takeover, a type of identity theft in which a criminal steals a business' valid online banking credentials and then uses those credentials to initiate funds transfers out of the account, has been a top priority for risk departments over the past decade. These attacks are common due to the lucrative nature of the targets, but are seldom successful due to the regular use of sound business practices by both financial institutions and corporations to mitigate the risk. While attacks on corporate accounts remain a constant threat, criminal entities are broadening their search for targets to include consumer accounts. Lower value consumer accounts are targeted because individual accounts often do not have the same protections and levels of security that are regularly applied to business accounts.

Criminal entities are committed to exploiting vulnerabilities in corporate systems and consumer personal computing systems in order to obtain valid account information and commit fraud. Account Takeover, through stealing either a business's or consumer's valid online banking credentials, represents a risk to ACH Network participants even though the roots of this criminal activity are not in banking systems themselves. In other words, Account Takeover is about compromised credentials; it is not about a direct compromise of the ACH Network or other payment systems.

Similar methods are used by criminal entities to obtain access to legitimate banking credentials to business and consumer accounts. These methods include mimicking a financial institution's website, using malware and viruses to compromise a system to gain account access, or using social engineering to incent consumers or employees into revealing security credentials or other sensitive data. Social engineering can come in many forms and is not as easily recognizable as it once was. Fraudsters may initiate contact by email, phone calls, faxes or letters in the mail in their effort to receive sensitive information.

In each case, fraudsters exploit the vulnerabilities in an individual's or business's system to obtain security credentials that they can use to access a company or individual's accounts. The criminal can then initiate funds transfers by ACH or wire transfer to the bank accounts of associates within the U.S. (often called 'money mules') or directly overseas with wires.

NACHA's Board of Director's Policy Statement

NACHA's Board of Directors adopted a Board Policy Statement on the *Importance of Sound Business Practices to Mitigate Corporate Account Takeover.* This policy statement addresses the importance of Originating Depository Financial Institutions (ODFIs) utilizing sound business practices to prevent and mitigate the risk of Corporate Account Takeover for ACH Network participants.

ODFIs should vigilantly and proactively protect against this type of fraud in various ways, including implementing systems designed to prevent and detect attempts to access a business' banking credentials and actual unauthorized access to the business' banking accounts, and by keeping their

own customers informed about the importance of implementing their own systems and sound business practices to protect themselves. Indeed, keeping customers informed of evolving risks can be an effective method to combat criminal entities before they get access to the banking system. The types and significance of the risk to each ODFI will vary depending on the financial institution, its business and its systems and processes.

It is essential that ODFIs and other ACH participants, such as Originators and Third-Party Senders, take a risk-based approach tailored to their individual characteristics and their customers to avoid losses and liability for themselves and other ACH participants. Accordingly, each ODFI should establish and implement mechanisms aimed to prevent, detect, and mitigate risk associated with Account Takeover, and work with their customers to also take such a risk-based approach – thus acknowledging the important role of both the financial institution and the customer in preventing and detecting Account Takeover.

Each ODFI should periodically review and update such mechanisms and customer guidance in response to developments in the methods used by criminal entities to perpetrate Account Takeover and in the methods used to prevent, detect and mitigate risk associated with such fraud.

Sound Business Practices

While each financial institution should evaluate its risk profile with regard to Account Takeover and develop and implement a security plan, which includes sound business practices, to prevent and mitigate the risk of Account Takeover, such a plan should be appropriate to the unique circumstances of the financial institution's business and clientele.

Examples of sound business practices for financial institutions include:

- Requiring Originators and Third-Party Senders to incorporate minimum levels of security on their internal computer networks
- Recommending dual control for payment file initiation
- Authenticate payment requests or changes to payment instructions, and independently verify request/change using out of band authentication methods such as call backs or email or text confirmations
- Encouraging the use of value-added services like positive-pay, debit blocks, and tokens to enhance account security
- Educating business clients and consumers on prevention, detection and reporting measures; encouraging daily review of accounts
- Reviewing procedures for identifying money mules

Financial institutions *do* use sound business practices — but it is important for every financial institution to consider all sound business practices appropriate to the unique circumstances of their business and clientele.

Likewise, each consumer or business should evaluate its risk profile with regard to Account Takeover. Examples of sound business practices for businesses and consumers include:

- Use firewalls, security suites, anti-malware and anti-spyware on all computers.

- Avoid conducting financial transactions over public Wi-Fi. If public Wi-Fi must be used, connect to a secure website and use a VPN. Secure websites are those that begin with https rather than http. A VPN provides an encrypted path for your data through the internet connection.
- Use caution when clicking on links and manually type the URL when in doubt.
- Never provide password, username, authentication tools or account information when contacted. Financial institutions or corporations will not ask for this information. If in doubt, use a known contact list or publically available contact information to confirm the validity of the contact.

Additional sound business practices for businesses are:

- Dedicate one computer exclusively to online banking and cash management activity and related security efforts and do not allow workstations to be used for general web browsing.
- Initiate files using dual control — for example, file creation by one employee and file approval and release by another employee on a different computer.
- Authenticate requests to make a payment or change payment instructions by vendors, and independently verify change in payment instructions.
- Make ACH payment/information forms available only via secure means.
- Take seriously calls received from the business's financial institution questioning the legitimacy of a payment.