Corporate Account Takeover: What You Need to Know

Sound Business Practices to Mitigate Risk

Risks to payment networks are ever changing. Criminal entities are becoming increasingly sophisticated at exploiting vulnerabilities in corporate systems in order to commit fraud. Corporate Account Takeover, a type of corporate identity theft in which a criminal steals a business' 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, Corporate Account Takeover is about compromised credentials; it is not about a compromise of the wire system or ACH Network itself.

Criminal entities employ various methods to obtain access to the legitimate banking credentials from businesses, including mimicking an institution's website, using malware and viruses to compromise the business' system, or using social engineering to defraud employees into revealing security credentials or other sensitive data.

For example, a business' systems may be compromised by:

- An infected document attached to an email
- A link within an email that connects to an infected website
- Employees visiting legitimate websites – especially social networking sites – and clicking on the infected documents, videos, or photos posted there
- An employee using a flash drive that was infected by another computer

In each case, fraudsters exploit the infected system to obtain security credentials that they can use to access a company's business 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 Corporate Account Takeover, and work with their customers to also take such a risk based approach – thus acknowledging the important role of both the FI and the customer in preventing and detecting Corporate 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 Corporate 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 Corporate Account Takeover and develop and implement a security plan, which includes sound business practices, to prevent and mitigate the risk of Corporate 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
- Using out of band authentication methods such as call backs or faxed transmittals
- Encouraging the use of value-added services like positive-pay, debit blocks, and tokens to enhance account security
- Educating business clients on prevention, detection and reporting measures; encourage daily review of accounts; and build cross-department event information sharing

Many 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 business should evaluate its risk profile with regard to Corporate Account Takeover. Examples of sound business practices that businesses should consider include:

- Using firewalls, security suites, anti-malware and anti-spyware on all computers
- Dedicating one computer exclusively to online banking and cash management activity and related security efforts, such as not allowing the dedicated computer to be used in Wi-Fi hotspots, including airports or Internet cafes, and disallowing workstations to be used for general Web browsing
- Initiating files using dual control — for example, file creation by one employee and file approval and release by another employee on a different computer

Remember the Fundamental Issue

Educate all computer users. Remember the analogy: An unsecure computer is the same as an unlocked house. If you fail to lock your house, then you have a significant chance of losing your valuables.

Accurate Data is Limited

At this time, there is no accurate "publically available" industry-wide data on Corporate Account Takeover instances where the cybercrime has led to the initiation of a fraudulent ACH credit transaction or wire transfer. Measurements related to Corporate Account Takeover are complex. NACHA continues to work with several cross-industry groups to determine if there is a way to accurately report data on this risk factor.

For example, NACHA's Risk Management Advisory Group is collaborating with the American Bankers Association to develop and administer a financial institution peer survey program that includes the concept of Corporate Account Takeover. Media outlets have alluded to large dollar losses not based on accurate statistical data. Publication of inaccurate estimates does not aid either the understanding of such fraud, nor does it help to identify actions to address those instances of fraud.

Remember the 3 C's of Corporate Account Takeover

Clarity
Understanding what Corporate Account Takeover really is and how to mitigate your risk through implementing sound business practices appropriate to your organization's role in the Network.

Cooperation
Financial institutions and their business customers must work together and be vigilant to deter the risk of Corporate Account Takeover.

Communication
Follow NACHA and Regional Payments Associations communications on Corporate Account Takeover. NACHA is collaborating with cross-industry groups on communications and Regional Payment Associations on education opportunities.