NACHA Board of Directors
Policy Statement on the Importance of Sound Business Practices to Mitigate Corporate Account Takeover

(Approved October 21, 2010)

Policy Summary

Risks to payment networks are ever-changing. Cyber-thieves 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 cyber-thieves steal a business' valid online banking credentials, has recently been on the rise and represents a risk to ACH Network participants even though the roots of this criminal activity are not in banking systems themselves. Accordingly, this policy statement of the NACHA Board of Directors addresses the importance of Originating Depository Financial Institutions (ODFIs) utilizing sound business practices to prevent and mitigate the risk of Corporate Account Takeover within the ACH Network.

Policy Statement

Corporate Account Takeover is particularly pernicious because once a cyber-thief obtains a company's valid online banking credentials; the thief can use those credentials in a variety of ways. The thief may initiate funds transfers out of the compromised business' account by ACH or wire transfer to the bank account of associates within the U.S. or directly overseas. In some cases, the perpetrator may also be able to gain access to and review the business' account details, such as account balances, activities and patterns, enabling the perpetrator to mimic the legitimate users and initiate transactions undetected.

Cyber-thieves employ various methods to obtain access to the banking credentials from legitimate businesses, including mimicking a legitimate institution's website, using malware and viruses to compromise the legitimate business' system or even using social engineering to defraud employees into revealing security credentials or other sensitive data. For example, corporate systems may be compromised by (1) an infected document attached to an e-mail, (2) a link within an e-mail that connects to an infected website, (3) employees visiting legitimate websites – especially social networking sites – and clicking on the infected documents, videos or photos posted there, or (4) an employee using a flash drive that was infected by another computer. In each case, the infected system is then exploited to obtain legitimate security credentials that can be used to access a company's corporate accounts.

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 cyber-thieves 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 cyber-thieves to perpetrate Corporate Account Takeover and in the methods used to prevent, detect and mitigate risk associated with such fraud.