Sound Business Practices for Financial Institutions to Mitigate Account Takeover

I. Executive Summary

Account Takeover is a type of identity theft in which a criminal entity steals a company or individual's valid online banking credentials. Small to mid-sized businesses remain the primary target of criminals, but any business or individual account holder can fall victim to these crimes.

Attacks can be perpetrated quietly by the introduction of malware or viruses through a simple email or infected website or through social engineering. Malware or virus introduced into a computer system may remain undetected for weeks and even months as it tracks and stores 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. By introducing layered security processes and procedures, technological and otherwise, and other tightened security efforts, financial institutions, through their agreements and processes, can help protect their customers from criminals seeking to drain accounts and steal confidential information. These increased security procedures may help reduce the incidence of, and mitigate the financial losses, business risks, and reputational damage that can result from such attacks.

NACHA's Risk Management Advisory Group has developed the following sound business practices for financial institutions of all sizes to consider when reviewing and implementing security procedures to mitigate the threat of Account Takeover. The sound business practices outlined in this paper are not meant to be taken as the exclusive approaches financial institutions should implement to address the risks associated with Account Takeover, nor are they meant to be considered mandatory requirements. No single security measure alone is likely to be effective in preventing or mitigating all risks associated with Account Takeover. Similarly, some of these sound business practices may not be appropriate for all financial institutions. Accordingly, each financial institution must identify its own risks, and design and implement the appropriate security measures to prevent and mitigate the risks associated with Account Takeover.

The sound business practices for financial institutions outlined in this document are:

- Agreements & Minimum Security Procedures
- Dual Control for Payment File Initiation
- Out-of-Band Authentication and Alerts
- Enhancement of Account Security Offerings
- Exploration of Low-Tech Security Options
- Education
- Special Considerations for RDFIs

II. Sound Business Practices

Each financial institution should evaluate its risk profile with regard to Account Takeover and develop and implement a security plan, including sound business practices, to prevent and mitigate the risk of Account Takeover. Such plan should be appropriate to the unique circumstances of the financial institution's business and clientele. However, in developing such a plan, each financial institution should consider both the following sound business practices, which are recommended in most cases, and any other sound business practices determined by the financial institution regardless of whether such practices have been communicated by NACHA.

Agreements & Minimum Security Procedures

It is recommended that a financial institution that is an ODFI:

- Require Originators and Third-Party Senders to incorporate minimum levels of security on their internal computer networks. Expectations should be outlined in the ODFI's agreement with the Originator or Third-Party Sender.

- Require Third-Party Senders to communicate the financial institution's security requirements to their customers, the Originators.

- Explain in detail the financial institution's security procedure requirements to the Originator and Third-Party Sender, and document their mutual understanding of such requirements.

- Require anti-virus and security software be robust and up to date for all of the Originator's and Third-Party Sender's computer workstations and laptops that are used to conduct online banking and initiate payments.

- Require Originators and Third-Party Senders to implement appropriate restrictions on functions for computer workstations and laptops that are used to conduct online banking and to initiate payments. For example, a computer used for online banking should not be used for general web browsing, email or social media sites.

- Prohibit Originators from using 'administrator credentials' for day-to-day processing. These credentials should be reserved for administrator functions only, not file processing.

- Include a termination clause in its ACH agreements with Originators and Third-Party Senders for non-compliance with required security procedures.

- Include in its ACH agreements with Originators and Third-Party Senders the right to audit, suspend and terminate the Originator or Third-Party Sender for breach of the *NACHA*

Operating Rules.

- Include a clause in its ACH agreements with Originators and Third-Party Senders expressly allocating the risk of loss.

- Advise implementation of multi-factor and multi-channel authentication for business accounts that are permitted to initiate funds transfers. Multi-factor authentication includes at least two of the following: 1) something the person knows (user ID, PIN, password), 2) something the person has (password-generating token, USB token), and 3) something the person owns (biometrics, i.e., fingerprint scan).

- Resist making exceptions to security procedures for specific Originators or Third-Party Senders.

- Educate financial institution staff on what the financial institution requires from its Originators and Third-Party Senders related to security procedures.

Dual Control for Payment File Initiation

It is recommended that a financial institution that is an ODFI:

- Recommend payment file initiation under dual control. Dual control involves file creation by one employee with file approval and release by another employee on a different computer. Or, require dual use of tokens where a single employee creates a file, but can only release the same file by logging in a second time using a new passcode or the token.

Out-of-Band Authentication and Alerts

It is recommended that a financial institution that is an ODFI:

- Use out-of-band authentication to validate the authenticity of transactions initiated by an Originator. For example:

    - Email: Some online banking platforms can automatically trigger an email to the Originator requiring authorization to release a pending file. This email should be done on a secure platform and encryption should be considered.

    - Call backs: A service, where the ODFI contacts the Originator or vice-versa, to authenticate transfers can help detect fraudulent files.

    - Faxed transmittal registers: The Originator sends registers to the financial institution that can be used to spot fraudulent activity prior to sending the file (fax with company name, initiation time, file amount and transaction count).

- Use out-of-band alerts to warn an Originator of unusual activity. These alerts notify Originators of suspicious transactions before ACH files and wire transfers are released. Triggers may include:

    - New payees: Recipients who have never received a transfer from the Originator before.

    - IP address authentication: A file is initiated from an IP address not previously associated with the Originator.

    - New credential requests: Someone at the financial institution should be evaluating requests for new Originator credentials before issuing and permitting use of the new credentials.

Enhancement of Account Security Offerings

It is recommended that a financial institution that is an ODFI:

- Consider fraud detection and risk management services offered by the ACH Operators and online banking service providers. For example, a threshold or a cap on ACH credit origination could alert a financial institution, particularly a small institution with low average daily ACH credit origination, to irregular origination activity. Many providers also offer security options such as IP address authentication, behavioral analytics or "payment patterning" of account holders.

- Encourage Originators to use value-added services like positive pay, debit blocks, and tokens to enhance Originator's account security.

Exploration of Low-Tech Security Options

It is recommended that a financial institution that is an ODFI:

- Establish, monitor and enforce exposure limits that relate to Originators and Third-Party Senders and take appropriate action when exposure limits are exceeded. For example, files should be set to suspend if above the exposure limit.

    - Origination calendar: Consider using origination calendars that will alert a financial institution to files that are out of the normal behavior (e.g., different time of day or different amount than is typical) for the client.

    - Prenotification: Consider using prenotification for credit origination when an Originator makes changes to their origination file (e.g., adding new Receivers or account number changes).

Education

It is recommended that a financial institution that is an ODFI:

- Stay in touch with other institutions and industry sources to share information regarding suspected fraudulent activity and new threats, which can change daily.

- Educate business clients on prevention, detection and reporting measures related to cybercrimes and account takeover, and optional services offered by the ODFI that the client can use to prevent losses.

- Encourage all account holders to review their account on a daily basis.

- Build internal relationships and cross-department event information sharing.

Educate account holders about the threat of social engineering. Let customers know that the financial institution will never contact a customer requesting account information or passwords and ask them to report attempted social engineering.

Special Considerations for RDFIs

It is recommended that a financial institution that is an RDFI:

- Educate front-line staff about money mules and what to do if one is suspected or identified.
    - Who are money mules?
        - One-time mules are those people who get tricked by social engineering schemes to send money. Often after sending the money, these mules realize their error and self-report to law enforcement.
        - Career money mules make a living, or at least a substantial amount of money, by completing ACH transactions or wire transfers between bank accounts. The FBI indicates that there "are generally multiple suspicious activity reports (SARs) against these individuals and there is no way they are unaware that their activities are part of a larger illicit scheme."[1]

[1]Steven R. Chabinsky, Deputy Assistant Director, Cyber Division, FBI - 2010

- U.S. -based money mules are individuals that are actually sent to the U.S., often on work or student visas, with the purpose of moving money for cyber thieves. They have specific instructions on where to open bank accounts, what names and addresses to use, and when and where to send money.

- How can a money mule be identified?

  - Look for anomalies in deposits.

  - Compare average balances against incoming deposits.

  - Ask questions: "Is the ACH or wire transfer deposit consistent with typical account activity?" and "Does the amount of the deposit make sense for the account?" If the answer is "No" – an Account Takeover may be underway.

- What should be done when a money mule is suspected or identified?

  - Develop procedures for what to do if a money mule is suspected or identified. The procedures should include:

    - A written script for customer service staff to use when there is evidence of a money mule

    - Procedures for consistent response if an account holder tells institution staff that the account holder is a money mule

    - Documentation process of all transactions and contact with the money mule

    - Procedures for when and how to contact law enforcement.
    - Filing of a Suspicious Activity Report (SAR)