# Sound Business Practices for Third-Party Service Providers to Mitigate Account Takeover

## I. Executive Summary

Account Takeover is a type of business 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 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.

Third-Party Service Providers have a variety of roles related to the processing and handling of ACH transactions. Two roles of Third-Party Service Providers are to provide services related to the origination of ACH transactions on behalf of either Originators or ODFIs. A third role of a Third-Party Service Provider is to provide services on behalf of the RDFI. By introducing layered security processes and procedures, technological and otherwise, and other tightened security efforts, Third-Party Service Providers that provide services on behalf of Originators, ODFIs or RDFIs can 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 Third-Party Service Providers 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 Third-Party Service Providers 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 Third-Party Service Providers. Depending on its precise role, and the type of entity it is processing on behalf of, each Third-Party Service Provider must identify its own risks, and design and implement the appropriate security measures to prevent and mitigate the risks associated with Account Takeover.

## II. Sound Business Practices

Each Third-Party Service Provider 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 unique circumstances of the Third-Party Service Provider's business and clientele. However, in developing such a plan, each Third-Party Service Provider should consider the following sound business practices, which are

recommended in most cases, and any other sound business practices determined by the organization, regardless of whether such practices have been communicated by NACHA.

## Third-Party Senders Performing Services on Behalf of an Originator

A Third-Party Service Provider that performs services on behalf of an Originator is typically a Third-Party Sender. A Third-Party Sender is a type of Third-Party Service Provider that has an ACH agreement with the Originator, and the ODFI's ACH agreement is with the Third-Party Sender and not the Originator. A Third-Party Sender should: (1) educate its Originators on sound business practices, and (2) ensure that it has adequate sound business practices within its own organization. Therefore, a Third-Party Sender should ensure that the Originators it processes for receive appropriate education concerning information security practices, which may include the document, *Sound Business Practices for Companies to Mitigate Account Takeover.*

### Education

It is recommended that a Third-Party Sender performing services on behalf of an Originator:

- Stay in touch with industry sources to share information regarding suspected fraudulent activity and new threats, which can change daily.
- Work with its financial institution on prevention, detection and reporting measures related to cybercrimes and account takeover.
- Educate its Originators on sound business practices including those outlined in this document and the document, *Sound Business Practices for Companies to Mitigate Account Takeover.*

### Dual Control for Payment File Initiation

It is recommended that a Third-Party Sender performing services on behalf of an Originator:

- Initiate payment files 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 that same file by logging in a second time using a new passcode on the token.

### Agreements and Minimum Security Procedures

It is recommended that a Third-Party Sender performing services on behalf of an Originator:

- Request its financial institution to review and explain in detail the requirements of its security procedures.

- Educate its Originators about the Third-Party Sender's financial institution's requirements related to security procedures.

- Use, and require its Originators to use, multi-factor and multi-channel authentication 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).

**Exposure Limits**

It is recommended that a Third-Party Sender performing services on behalf of an Originator:

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

**Enhancement of Account Security Offerings**

It is recommended that a Third-Party Sender performing services on behalf of an Originator:

- Employ appropriate value-added services offered by its financial institution to assist in the detection of potentially fraudulent transactions. Such services may include positive pay, debit blocks, and tokens to enhance security.

**Third-Party Service Providers Performing Services on Behalf of an ODFI**

One role of Third-Party Service Providers is to provide services related to the origination of ACH transactions on behalf of ODFIs. A Third-Party Service Provider in this role should evaluate and implement, as appropriate, the sound business practices applicable as discussed in the document, *Sound Business Practices for Financial Institutions to Mitigate Account Takeover.* A Third-Party Service Provider, in this capacity, plays a vital role in ensuring that sufficient education and focus on security practices occurs as it handles ACH transaction processing on behalf of the ODFI.

**Third-Party Service Providers Performing Services on Behalf of an RDFI**

One role of Third-Party Service Providers is to provide services related to the receipt of ACH transactions on behalf of RDFIs. A Third-Party Service Provider in this role should evaluate and implement, as appropriate, sound business practices related to identifying money mules and actions related to suspected money mules as discussed in the document, *Sound Business Practices for Financial Institutions to Mitigate Account Takeover.*