**Supplementing Data Security Requirement Rule**

This change to the Nacha Operating Rules will enhance quality and improve risk management within the ACH Network by supplementing the existing account information security requirements for large-volume Originators and Third Parties. This change will be implemented in two phases.

**Details**

The existing ACH Security Framework including its data protection requirements will be supplemented to explicitly require large, non-FI Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) to protect deposit account information by rendering it unreadable when it is stored electronically.

Implementation begins with the largest Originators and TPSPs (including TPSs) and initially applies to those with ACH volume of 6 million transactions or greater annually. A second phase applies to those with ACH volume of 2 million transactions or greater annually.

**Impact**

Effective Dates:

Phase 1 – June 30, 2020 for Originators and Third Parties with ACH volume greater than 6 million in 2019

Phase 2 – June 30, 2021 for Originators and Third Parties with ACH volume greater than 2 million in 2020

Potential Impacts:

Implementation for those Originators and Third Parties that currently would not be compliant

For ODFIs, informing Originators of their direct compliance obligations

**Supplementing Data Security Requirement FAQs**

* Which parties are subject to the new Data Security Requirement to protect account numbers used for ACH purposes by rendering them unreadable when stored electronically?
	+ The new requirement applies to non-consumer Originators that are not financial institutions, and to Third-Party Senders and Third-Party Service Providers that perform any function of ACH processing on behalf of an Originator, Third-Party Sender, ODFI, RDFI, or ACH Operator.

Financial institutions are not included within the scope of the new requirement to render ACH account numbers unreadable when stored electronically because they are already subject to rigorous data security requirements imposed by their regulators.

The Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework (the NIST Framework) both have the shared objective of strengthening data security. The PCI Security Standards Council (PCI SSC) recently updated its document entitled “Mapping PCI DSS v3.2.1 to the NIST Cybersecurity Framework v1.1,” which provides industry users with guidance on data security standards that meet objectives in both PCI DSS and the NIST Framework.

* Is a Third-Party Vendor whose function is to operate a financial institution’s core processing system (i.e., DDA and savings posting systems) subject to the new data security requirements?
	+ No. A financial institution’s third-party vendor whose function is to operate the financial institution’s core processing system (i.e., DDA and savings posting system) is not subject to the new rule. **However, if that same third-party vendor also performs any function of ACH processing, such as running the FI’s ACH platform, the vendor would meet the definition of a Third-Party Service Provider under the Nacha Operating Rules and therefore would be subject to the requirements of the new rule for that function to render ACH-related account numbers unreadable while stored at rest**.
* Must all parties subject to the new data security requirements be in compliance by June 30, 2020?
	+ No. This rule focuses initially on large-volume third parties and non-financial-institution Originators and will be implemented in phases.
		- **Phase One**

Any non-financial-institution Originator whose total ACH origination volume exceeds 6 million entries in calendar year 2019 will be required to comply with this rule no later than June 30, 2020. Any Third-Party Sender or Third-Party Service Provider whose total transmission volume (that is, the aggregate volume transmitted on behalf of ALL of its clients) exceeds 6 million entries in calendar year 2019 must comply with this rule no later than June 30, 2020.

* + - **Phase Two**

Beginning in calendar year 2020, the annual volume threshold will be reduced to 2 million entries. Any non-financial-institution Originator whose total ACH origination volume exceeds 2 million entries in calendar year 2020 will be required to comply with this rule no later than June 30, 2021. Any Third-Party Sender or Third-Party Service Provider whose total transmission volume (that is, the aggregate volume transmitted on behalf of ALL of its clients) exceeds 2 million entries in calendar year 2020 must comply with this rule no later than June 30, 2021.

* How does the rule apply once fully implemented?
	+ Any non-financial-institution Originator, Third-Party Sender, or Third-Party Service Provider that meets the 2-million-entry annual origination/transmission volume threshold in calendar year 2021 or beyond will be required to comply with this rule by June 30 of the year following the calendar year in which the 2 million-entry volume threshold was met.
* When an Originator initiates entries through multiple accounts at one ODFI, or uses multiple accounts at one ODFI, or uses multiple ODFIs, how do the thresholds apply?
	+ A Non-Consumer ACH Originator that originates ACH entries through multiple settlement accounts at one ODFI, or originates ACH entries through multiple ODFIs, should consider its total, combined origination volume when determining whether it meets the 6-million/2-million-entry thresholds.
* When a TPSP or TPS initiates entries on behalf of multiple clients, is the 6M/2M entry threshold based on the TPSP/TPS’s aggregate volume of entries transmitted for all of its clients, or is it base on each Originator’s volume separately?
	+ A Third-Party Service Provider or a Third-Party Sender must consider the combined volume of entries processed for all of its various clients when determining if it meets the annual 6 million/2 million volume thresholds. These thresholds are not client-specific. TPSPs/TPSs who originate and/or transmit ACH entries through multiple settlement accounts and/or multiple financial institutions should take volume from all ACH entries they originate/transmit into consideration when determining if they exceed the thresholds.
* How does this rule impact non-financial institution Originators and Third Parties with volumes below the threshold?
	+ Non-financial-institution Originators, Third-Party Senders, and Third-Party Service Providers that do not meet these thresholds **are currently not mandated** by the Rules to render ACH account information stored electronically unreadable while at rest. Nevertheless, NACHA strongly encourages **voluntary adoption** of this data security standards as a sound business practice.
* Does the new rule to render account information unreadable apply to consumer accounts only, non-consumer accounts only, or both?
	+ Both. If an account number is used for ANY ACH payment (consumer or corporate), it must be rendered unreadable while stored electronically.
* Does the requirement to render ACH account numbers unreadable apply only to systems where transactions can be created, or does it extend to other systems within the organization?
	+ Any place where account numbers related to ACH entries are stored is in scope. This includes systems on which authorizations are obtained or stored electronically, as well as databases or systems platforms that support ACH entries. **As an example, for a Third-Party Service Provider whose client is a financial institution, these can include platforms that service ACH transaction warehousing and posting, and client information reporting systems.** For Originators and their Third-Party Service Providers, accounts payables and accounts receivables systems will be impacted, as may be other systems (for example, claims management systems for insurance companies).
* We have scanned our paper authorizations and ACH records into our database for easier storage. Does the new rule apply to the scanned documents even though the same documents in paper form would not be covered?
	+ Yes. Although the new rule does not apply to the storage of ACH account information in physical, paper form, the requirement to render the account information unreadable DOES apply if these paper authorizations or other documents containing ACH account numbers are scanned for electronic record retention and storage purposes.
* Do Nacha Operating Rules prescribe the specific manner in which data at rest must be rendered unreadable?
	+ No. The Rules are neutral as to the methods/technologies that may be used to render data unreadable while stored at rest electronically. Encryption, truncation, tokenization, destruction, or having the financial institution store, host, or tokenize the account numbers, are among options for Originators and Third-Parties to consider, but each Originator or TPSP will need to make its own business decision in consultation with its legal counsel and technology providers.
* Our electronic documents are stored on platforms that are not encrypted, but access is restricted by access controls – e.g., passwords, etc. Data is not accessible except to those with proper credentials. Does this comply with the new rule requirement?
	+ No. Although access controls such as passwords help to secure ACH-related data at rest, these do not meet the new standard. Even with the use of various physical security controls and restricted access, the electronic data at rest still must be rendered unreadable.
* If we apply PCI data security standards to all systems or platforms on which account numbers used in ACH entries reside, are we compliant with the requirements to render the information unreadable while stored electronically at rest?
	+ Yes, PCI DSS includes specific requirements related to protecting data while at rest. Utilizing one of these prescribed methods of data protection for ACH-related account numbers, in such a manner as to be compliant with the standard, should meet the commercially reasonable requirement for this Rule.
* Do we need to apply all PCI standards to our ACH-related account number to be compliant with the Supplementing Data Security Rule?
	+ No. The ACH Security Framework, first implemented in 2013, includes data security rules beyond data at rest that also utilize the commercially reasonable standard. Utilizing PCI DSS standards may be a best practice when adhering to those Rules. However, the Supplementing Data Security Rule only pertains to securing data at rest, which is currently covered by PCI DSS v3.2.1 3 (all) and 8.2.1.
* Is disk encryption considered an acceptable method to protect ACH account numbers stored electronically?
	+ Possibly. PCI considers disk encryption an acceptable protection method only if additional, prescribed physical security steps are taken. In order for disk encryption to be considered under the commercially reasonable standard, it would need to be implemented with the additional steps that would allow for meeting the PCI standard.