tokenex

ACH Data Security Compliance Guide

How to Protect ACH Data to Facilitate Safe Electronic Payments

Nacha

Table of contents

The role of Nacha

Formed in 1974, Nacha is a nonprofit association that develops, administers, and governs the Nacha Operating Rules and Guidelines, which serves as the regulatory framework for the ACH network. The operating rules for Nacha define standards and rulesets for participating in the network, and the participants in the network agree to abide by these rules and guidelines so that the ACH entries can be safely sent and received in a formalized fashion.

In this compliance guide, we'll show how Nacha's Supplementing Data Security Requirements and Fraud Detection Standards are similar to the data protection requirements of the PCI DSS and can be satisfied via the implementation of similar protective measures.

The ACH explained

As their names suggest, automated clearing houses form the foundation of the ACH network. These financial institutions called ACH Operators are responsible for transferring payments from one party to another. They are essentially intermediaries that manage transactions to ensure funds are exchanged appropriately. To accomplish this, Nacha's Operating Rules and Guidelines define and establish the roles and responsibilities of each party involved in an ACH transaction.

Parties to an ACH transaction

Depository Financial Institution (DFI)

ODFI (originating)
The financial institution that is initiating or sending the ACH entry

RDFI (receiving)
The financial institution receiving the ACH entry

Receiver

The party whose account is receiving the ACH entry

Third-Party Sender

Intermediaries that transmit data between the originator and ODFI

Originator

The organization (merchant, biller, government, etc.) or consumer that initiates the creation of an ACH entry.

Third-Party Service Provider

Parties such as TokenEx that interact with ACH data during the course of the transaction

Operator

The entities (the Federal Reserve Bank or the Electronic Payments Network) responsible for receiving and routing ACH entries from the ODFIs to the RDFIs. The operators also handle the settlement, or movement of the funds

According to Section 1.6 Security Requirements, Page OR3, these parties, excluding Receivers and non-consumer Originators, must ***"establish, implement, and update, as appropriate, security policies, procedures, and systems related to the initiation, processing, and storage of ACH transactions."***

These policies must also maintain the privacy and security of protected information (PI)—which is equivalent to personally identifiable information (PII) within the context of ACH entries—against unauthorized use and anticipated threats.

Risk and compliance

Annual audit must be performed to ensure compliance with the operating rules.*

- Failure to comply will result in a Class 2 violation
- Fines of $100,000 per month for up to three months
- After three months, escalates to a Class 3 violation
- $500,000 per month until resolved and may result in suspension of ability to process

ACH entries

Also subject to data privacy compliance (GDPR, CCPA, GDPL, etc.)

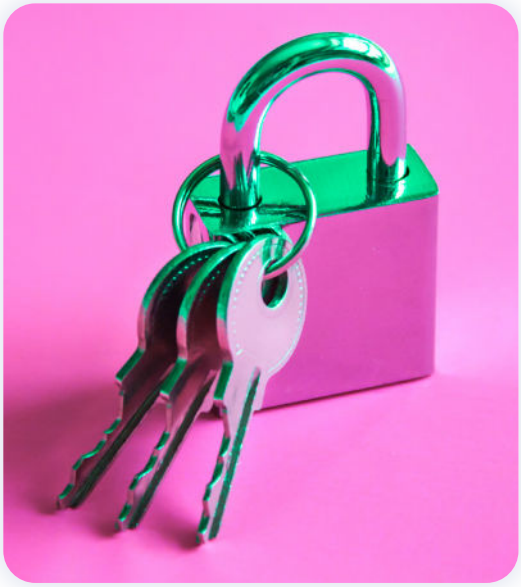
- Account numbers considered direct identifiers
- Obligation to protect personal data using pseudonymization or some mechanism to de-identify personal data

Risks of a data breach

- Financial and opportunity costs
- Nacha data breach notification requirements
- Data privacy breach notifications
- Reputational damage
- Loss of consumer trust

** Annual rule compliance audit does not apply to Receivers or Originators. WEB Originators must perform an annual security audit.*

To enforce its operating rules, Nacha requires audits of participating DFIs, Third Party Service Providers and Third Party Senders and may imposes fines for noncompliance. This keeps the network running safely and smoothly. Organizations can work with a third-party or unaffiliated internal auditor to help conduct the assessment. Completing these audits requires financial institutions and third-party service providers to reference Article One, Subsection 1.2.2 Audits of Rules Compliance.



In terms of compliance, it's important to note that the data included in an ACH entry is not always exclusively governed by Nacha. For instance, if that entry contains sensitive data such as a name or billing address, it could be subject to multiple regulatory compliance obligations for data privacy (GDPR for EU citizens, CCPA for California households, etc.). So, there likely could be overlapping data privacy obligations for protecting that information as well.

It's also important to consider overall risk: What is the risk of not being compliant or not adequately protecting sensitive personal and payment data? Predominantly, there is the financial risk with regard to fines for negligence and noncompliance, but there is also the risk of a data breach or other exposure.

287 Days

Average length of time before a breach is identified and contained.

Source: IBM 2021 Cost of a Data Breach Report

• BY THE NUMBERS •

Global breaches

$155B

Global cybersecurity spending surpassed $155 billion in 2021, up from $137 billion in 2020.

Gartner (2021)

$22B

Over 22 billion records were exposed in 2021.

Risk Based Security (2021)

$4.24M

The average cost of a breach is about $4.24 million globally and $9.05 million in the U.S.

IBM 2021 Cost of a Data Breach Report

$161

The average cost of a breached record is about $161.

IBM 2021 Cost of a Data Breach Report

The cost of compliance is an investment in your organization's future.
Protect yourself and your customers by ensuring the sensitive data in your possession is secure.

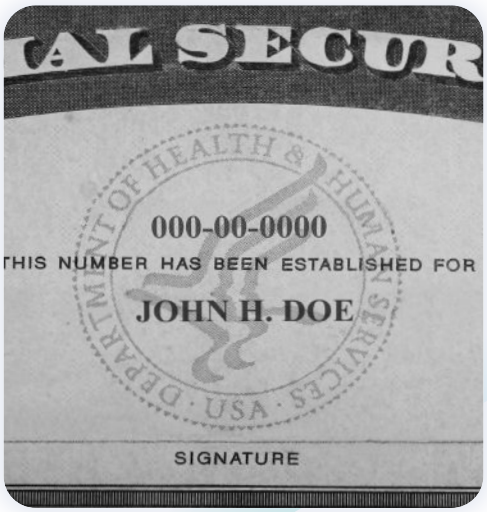
According to Nacha, a data breach is any exposure of sensitive consumer-level data. The cost of a breach can include the financial and opportunity costs it takes to remedy the issue as well as the indirect costs of reputational damage and loss of consumer trust.

Consumer-level data

Bank account and routing number

Social Security number and name

Each DFI is responsible for ensuring that its originators and third parties adopt and implement commercially reasonable policies, procedures, and systems to receive, store, transmit, and destroy consumer-level ACH data.



Operating rules and guidelines

Each year, Nacha publishes its operating rules and guidelines to ensure the ACH network is addressing the changing needs of its participants or users. All participants must review these updated regulations and meet their requirements to remain compliant.

Over the years, Nacha's Operating Rules and Guidelines have evolved to better secure and accommodate changing technology and payment types. These rules are similar in nature and language to the PCI DSS to help make it easier for organizations handling multiple types of payment data to comply with a unified set of security standards. So, the same general principles apply to protecting the confidentiality and integrity of ACH data, PII, and cardholder data (CHD).

As Nacha Rules and commercially reasonable standards continue to evolve to keep pace with changing consumer behaviors and payment technologies, it's important for organizations to remain flexible and ready to update their compliance practices and policies when necessary.

Financial institutions, originators, third-party senders, and third-party service providers are required to establish, implement, and update, as appropriate, security policies, procedures, and systems related to the initiation, processing, and storage of ACH transactions.

Section 1.6 Security Requirements

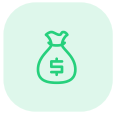
Information security requirements

These represent an expansion of security rules to require non-FI originators and third parties to protect account numbers by rendering them unreadable in electronic storage. Appropriate methods of obfuscation include hashing, encryption, tokenization, or similar technologies. This language is similar to the PCI standard around the protection of primary account numbers (PANs).

Phases of implementation

Enactment

Approved in 2018 and effective in two phases



Phase I

Requires originators of **6 million or more** annual transactions (as of 2019) to be compliant as of June 30, 2021

Phase II

Requires originators of **2 million or more** annual transactions (as of 2020) to be compliant as of June 30, 2022 or more annual transactions (as of 2020) to be compliant as of June 30, 2022

Supplementing fraud detection standards

The existing rule requires originators of WEB debits to use "commercially reasonable" fraud detection systems. A WEB debit is essentially an ecommerce or mobile transaction, so any ACH entry initiated via a desktop or mobile browser would be subject to the new fraud detection standards for those transactions. Account validation is a specific method for fraud prevention identified by the rules.

Implementation details

Fraud Prevention

Detection systems must explicitly include "account validation."

Account Validation

Originators must validate that an account is open and accepts ACH entries.

Effective Date

Originators must comply by March 19, 2021.

How to comply with Nacha rules

ACH payments are typically sent via batch processing and contain payment data similar to what is found in credit card payments, and as a result, they can be secured and desensitized by tokenization in much the same manner. In a typical payment card transaction, the primary account number and other applicable cardholder data are tokenized, whereas the bank account number and consumer-level data (such as names and Social Security numbers) are tokenized in an ACH payment.

Accept

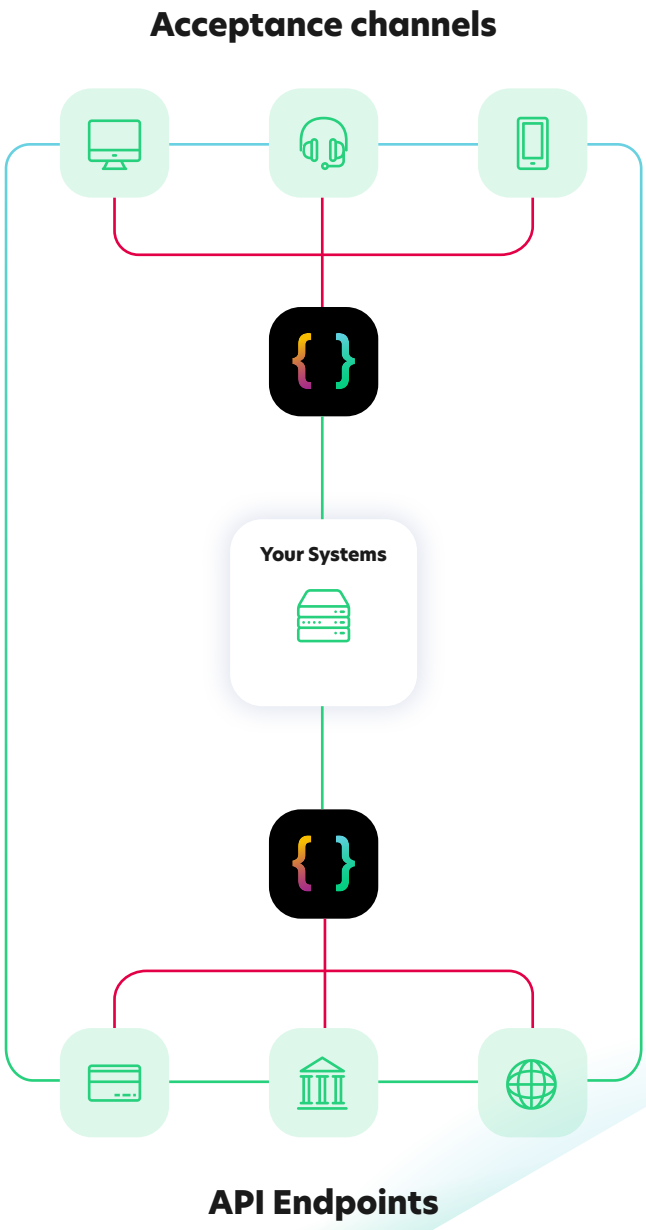
Your customers' sensitive personal and/or payment data is captured at the point of entry.

Secure (tokenization)

You receive a token for internal use while the original data is safely stored outside of your environment.

Transact

You can use our Transparent Gateway to send fully secure and desensitized data to any API endpoint.



So, although the data is different, the overall process of protecting ACH transactions is the same as the one for protecting credit card transactions. Tokenized data is obfuscated and stored offsite until the original sensitive data is needed, at which point the placeholder token will be exchanged and the ACH data returned.

Because the data is stored outside of an organization's environment, tokenization can help simplify Nacha compliance, as well as significantly reduce the risk of ACH data theft. In addition, TokenEx can work with any processor, payment gateway, or third-party provider. This capability for multiple integrations can increase the freedom and flexibility of your internal operations, fueling greater flexibility and infrastructure growth by enabling you to more easily reach new markets.

Protecting billions

Just how prevalent is the use of the ACH network?
In 2021, 29.1 billion payments valued at a total of $72.6 trillion were made.

Source: Nacha.org

{tokenex}

• AS A SOLUTION •

- Comply with Nacha data security rules.
- Enable compliance with Nacha fraud detection
- Data-centric security to support defense-in-depth
- Reduce extent and associated costs of the Nacha audit
- Simplify security by using one vendor for all data elements
- Retain flexibility and control of your data
- Accept ACH data without handling the raw account number
- Reduce risk of data theft and cost of breach notifications
- Cloud-based tokenization provider with API and batch support

Working with TokenEx enables your organization to reduce risk, simplify compliance, and streamline its operations for improved efficiency and business intelligence.

Batch use case

The ACH network typically utilizes a batch file transfer process to move ACH entries from ODFIs to RDFIs. TokenEx has a batch file solution to parse the files for tokenizing and/or detokenizing. This can enable clients to send and receive these ACH files without interacting with cleartext sensitive ACH data.

ACH file sample

```
101 021000021000000000001805150735A094101JPMORGAN CHASE         QANAMEFORCOMPANY
5220                1111111111111111111100000000PPDPayroll   MAY 30180530   1021000020000001
6320819048081234567890123456700000100001234567890123MARY JANE               1000000000000001
705PAYROLL PAYMENT FOR FIRST WEEK OF MAY                                        00010000001
822000000200081904800000000000000000000100000000000                          021000020000001
5220                1111111111111111111100000000CCDACH Pmt   JUN 12180612   1021000020000002
6320819048081234567890123456700000100001234567890123PAPER SUPPLIES          1000000000000001
705PAPER PAYMENT FOR INVOICE#34789324 ON MAY 25                                 00010000001
822000000200081904800000000000000000005000000000000                          021000020000002
900000200000100000004000163809600000000000-000000150000
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
900000200000100000004000163809600000000000-000000150000
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
```

The example above is a structured, fixed-width file with the account numbers highlighted in red.

ACH file sample

```
101 021000021000000000001805150735A094101JPMORGAN CHASE         QANAMEFORCOMPANY
5220                1111111111111111111100000000PPDPayroll   MAY 30180530   1021000020000001
6320819048088739026354728364100000100001234567890123MARY JANE               1000000000000001
705PAYROLL PAYMENT FOR FIRST WEEK OF MAY                                        00010000001
822000000200081904800000000000000000001000000000000                          021000020000001
5220                1111111111111111111100000000CCDACH Pmt   JUN 12180612   1021000020000002
6320819048088noiWhalpJisxnmQa00000100001234567890123PAPER SUPPLIES          1000000000000001
705PAPER PAYMENT FOR INVOICE#34789324 ON MAY 25                                 00010000001
822000000200081904800000000000000000005000000000000                          021000020000002
900000200000100000004000163809600000000000-000000150000
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
900000200000100000004000163809600000000000-000000150000
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999999
```

Here's that same file in a tokenized state. Once tokenized, there is no longer a raw bank account number contained within this file. This enables the secure sharing of this file with operators and other third parties. TokenEx can detokenize and pass along this information without forcing them to introduce the risk associated with ingesting or storing readable card or bank account information.

Arux.Software

The Problem

Online checkout page that accepts payment and personal data. Arux needed to reduce their risk while ensuring compliance with relevant regulatory obligations.

The Solution

By using the TokenEx iFrame to capture and tokenize payment data, Arux can provide a seamless payment experience for consumers while keeping sensitive data out of its internal systems. Arux never sees the actual number, only a TokenEx token that is submitted to its web server and then onto its PSP via the Transparent Gateway, which can be safely stored within Arux's environment to preserve analytics and improve business intelligence.

Results

- Minimized PCI scope by preventing sensitive data from entering web servers
- Protected PII and ACH data with same care as PCI
- Simplified the cost and complexity of PCI DSS and Nacha compliance
- Reduced the potential impact of a breach

How can TokenEx help my organization?

As seen in the use case above, tokenization helps your organization in more ways than one. Not only can it help you to more easily meet your requirements for Nacha and PCI DSS compliance, but it can also help ensure you're properly complying with the data protection requirements of international privacy regulations such as GDPR and CCPA.

This is because tokenization can protect any structured data set by removing sensitive values from your environment and replacing them with nonsensitive placeholders. As a result, tokenization removes the systems that were previously storing sensitive data from the scope of compliance while still maintaining the business utility of the data within them.

Additionally, we provide you with the freedom and flexibility to integrate with nearly any third party and send data to any API endpoint, enabling you to entrust your most sensitive data to security and compliance experts while promoting operational efficiency and positive business outcomes.

We understand that every organization's environment and journey to Nacha compliance is different, and we recognize that tokenization is not the only option for achieving it. However, this efficient and effective method uses proven techniques for segmentation and data minimization to isolate sensitive data, to store only what is absolutely necessary, and to protect what must be stored in a manner that virtually eliminates the risk of data theft.

To learn more about how TokenEx can help you address your unique needs surrounding security and compliance while providing the flexibility and simplicity required to promote positive business outcomes, contact us today at info@tokenex.com

Get the expertise you need.

Meet with TokenEx today to learn more about how we can help you with your payment solutions.

Connect with us