LYONS Commercial Data™

BEST PRACTICES FOR ACH COMPLIANCE

What You Need to Know to Be Ready

sales@lyonslive.com | 800-684-0388
www.lyonslive.com

BEST PRACTICES FOR ACH COMPLIANCE

Introduction

Movement of funds across electronic networks in the U.S., and sometimes abroad, is governed by NACHA, the non-profit organization dedicated to the system's efficiency and security. Entities that initiate and receive payments over the ACH network must follow NACHA's operating rules. In order to develop a "to do" list of ACH compliance, it is helpful to think of ACH payments across their entire life cycle. At each stage of this process, NACHA rules are at play. Best practices to comply with these rules ensure that customer data is secure, the details of the transaction are correct, the system is not vulnerable to attack and the risk of deliberate fraud is significantly reduced.

What's Inside

What is ACH Compliance?

With the exception of those who work inside the financial services industry, there is a general lack of knowledge about the ACH network and its importance to the national economy. ACH facilitates the movement of funds between accounts and banks, often over electronic networks. Because of this network's role in U.S. commercial transactions, it is tightly regulated.

NACHA, which stands for National Automated Clearing House Association, brings predictability and security into the system by establishing rules for ACH payments and those who initiate and receive them. These rules are regularly updated in order to respond to concerns expressed by actors involved in ACH payment processing. These updates accommodate changes in technology and emerging risks for fraud and errors.

The ACH network functions on the basis of mandatory compliance with NACHA rules. While widely accepted as fundamental to ensure the stability of the system and to prevent nefarious activity, these rules are nonetheless detailed and lengthy, and may be perceived as burdensome for some businesses. However, failure to follow NACHA regulations can result in an investigation and monetary fines. These fates can be easily avoided by sound business practices that lead to compliance in the first instance. For commercial entities who depend on ACH processing as a matter of doing business, it is essential to develop best practices for rules compliance.

NACHA achieves many different objectives. It fulfills the promise of a secure and trustworthy payment system that satisfies commercial needs for rapid transfer of funds. It also prevents fraudulent or prohibited activity, by determining all aspects of a transaction are valid. NACHA rules are substantial, but they primarily involve steps that are in fact in line with business ethics: to secure private information, prevent errors or fraud, and minimize financial liability. Adherence to NACHA rules is not the only obligation on payment originators and receivers, but it is central to their legal responsibilities.

In addition to closely following the NACHA rulebook, businesses must also take steps to preclude activities provided on behalf of companies, individuals or accounts on the Treasury Department's Office of Foreign Assets Control (OFAC) sanctions list. Many parties are listed in the OFAC database and processing a payment on their behalf — even inadvertently — can result in serious penalties. Because NACHA rules may be placed aside if following those rules would support illegality, NACHA allows for transactions to be delayed if they are sufficiently suspect after OFAC screening.

The Consequences of Non-Compliance

Because of the system's importance, NACHA imposes significant penalties for non-compliance. Violations are categorized according to severity. Class 1 Violations are liable for fines of up to $5,000 per instance; Class 2 up to $100,000 per violation per month; and Class 3 up to $500,000 per violation per month. It's important to note these are the potential penalties for non-compliance with the NACHA rules. It does not include any possible liability for failing to comply with OFAC or other regulations. The Treasury Department can impose monetary fines and jail time to enforce laws governed by OFAC.

For parties to ACH transactions, these detailed rules and large fines for non-compliance highlight the need to be diligent. As part of an interconnected network that is vulnerable to the possibility of moving fraudulent or criminally sourced funds, payment originators have a legal and moral obligation to comply with NACHA. The life cycle of a transaction involves many linked systems: it may start with a customer entering a bank account into a website, which is then transmitted to and held by the company before it initiates an ACH debit against the account as part of a larger batch. After the ACH batch is complete, the bank will return a statement that records the movement of these funds. Because of this complexity, many organizations can suffer financial liability in the event of high-level fraud, depending on where along the chain of the transaction the fraud is discovered. Even a simple error can cost an originator in fees if a payment is returned.

Compliance Best Practices

Fortunately, there are a number of steps organizations can take that shore up their internal processes, demonstrating attempts to meet the NACHA obligations of a secure and rule-based network. There are a few ways that compliance is beneficial to businesses. First, it makes their internal operations run more smoothly. Second, it helps to prevent sanction because of a procedural oversight that results in a NACHA violation. Third, it provides evidence of the intent to become NACHA compliant. In the event of audit, the company must show a willingness to implement the NACHA rules. In the event of a possible rules violation, showing procedures are in place can help aid in defense.

Overall, these elements help NACHA to function the way it should. With the right safeguards in place, parties to a transaction know who is requesting or receiving funds. The procedures aim to prevent a nefarious actor from hacking, manipulating or defrauding the system.

Multi-Factor Authentication (MFA)

At all stages of the ACH process, from customer input to releasing a payment batch, individual users have to interact with the technology. Most companies are not at the biometric level of security protocols. Most rely on passwords and security questions to verify the right person is making demands on the system, both at an inter-office and national network level.

In terms of NACHA compliance, it is an important obligation is to permit access to the system only to those who are authorized to use it. This includes commercial and institutional customers who may ask to originate ACH payments. It should not, therefore, be too easy to log on to the system. Everyone has heard that most people only use a few passwords for all of these enabled systems in their private and professional lives. This means their passwords are pretty easy to hack.

To prevent unauthorized access and to confirm the identity of all system users, implement a multi-factor authentication system. This means there are multiple levels of information a user must provide before they get in. Swiping your bank card and then entering a PIN code is an example of MFA, as is entering your bank card number online and then answering a security question. For ACH compliance, it may mean scanning a security card, answering a question, entering a passcode and using a security token if one is available.

Customer-Side Dual Control

Knowing who is interacting with the system is vital, but it is only one aspect of strong ACH security. Dual control helps to ensure that even authorized individuals are initiating a batch that does not contain errors. It also adds an additional layer of protection in the event someone's MFA elements are compromised. Under this procedure, it takes at least two individuals to initiate payments. One individual creates a batch while the second releases payments. That way, no single person can create a wire transfer or move funds without the confirmation of another. While this may seem cumbersome, it's mandatory across most organizations. It means the institution's funds are safe and no one person bears the burden of being the sole security checkpoint between payment initiation and release.

IP Restrictions

By placing limits on the number of machines that can access the ACH system, entities reduce the risk of unauthorized exposure. Technology is now smart enough to identify not only that information is transmitting electronically, over a wireless or LAN connection, but also from a computer using a unique identifier or IP address. Both home and professional machines have IP addresses that allow internet activity to be tracked and locations identified.

While restricting access to one identified machine or network connection may seem unduly inconvenient to the customer, identifying a short list of verified IP addresses can meet the needs of everyone. It is not necessary to impose on ACH users an obligation to use one designated machine at all times; a few may be

verified. Customers can therefore still opt to choose from a number of different locations while still providing financial institutions with an additional check on the validity of a proposed transaction or batch.
IP address restriction has another benefit. It may help flag any hacker activity from an off-site server or unauthorized connections to the system. Adding to this the use of SSL encryption technology and security software, discussed below, hackers have fewer routes to get into the highly sensitive and valuable store of data held by ACH processors. There are also more ways their activities can be exposed, such as seeing activity from a non-authorized IP address or from a hidden, unknown internet network.

Treasury Management Agreements

Companies transact with financial institutions for a whole list of services. If they plan to regularly use the ACH network, a bank will typically have them put the nuts and bolts of that activity, and respective responsibilities, in writing. A detailed legal agreement that explains the obligations of financial institutions and their commercial customers reinforces the need for ACH compliance. It not only defines these obligations, but also clarifies who holds liability in the case of error or violation of the rules.
A treasury management agreement is a vital tool that provides a common reference point for all parties involved in one side of ACH transactions, as well as a basis upon which disputes may be partially resolved. In addition, like other security measures, this is another way to reduce the number of individuals who may attempt to initiate an ACH payment, as a financial institution will only grant that authority to parties with whom they have a treasury management agreement in place. This means that it is simply not possible for a new company to walk into a bank and ask to start processing ACH batches without first disclosing the nature of their business, the credit risk of their organization and perhaps their individual customers and determining the level of risk liability the bank is willing to incur by entering into an ACH processing arrangement.

Over Limit Procedures

In addition to the safeguards that surround initiation of an ACH transaction, entities should develop transaction rules that go even further to prevent fraud. At the bank level, each ACH customer should be assessed for a credit risk and operate within approved transaction limits. This allows for the smooth functioning of funds transfer from an originating to receiving bank, while minimizing credit exposure in the event that fraud does occur. Banks need to place an expected range of activities on every customer in order to spot when inconsistencies or unusual transactions take place. Without understanding the normal payment patterns, these anomalies are harder to see.
Part of this process should be the development of over limit procedures, that flag and closely monitor transactions that exceed an approved limit. The transactions may still go through, but because this goes beyond the agreed upon liability threshold, banks incur a greater risk. When over-limit procedures work efficiently, the customer experiences little service interruption, while the financial institution is still in the position to identify potentially fraudulent activity and further prevent or minimize their exposure.

Third-Party Security Software

Authentication of users is vital to ACH security, but it is only one element that ensures the overall trustworthiness of the system. Third-party ACH payment originators hold private information that must be maintained in a secure environment. The NACHA rules obligate that non-public information be held within a data security framework, so it is incumbent upon businesses to take inventory of the data they hold, and the measures uses to protect it.
That includes such steps as making a list of what kinds of information they take from customers, including name, address, bank account number, credit card number, phone number, and other identifying or sensitive information. After they know what they have, they must also have step-by-step procedures to keep that information out of the wrong hands or vulnerable to exposure, either in electronic or paper form.
Using security software that provides safe storage of this data can help achieve this goal.

Encryption technology, anti-spyware, anti-malware, and system firewalls all help meet these obligations. When financial institutions communicate with their commercial clients who initiate payments, they should clarify that third-party users of the ACH network are responsible for their own customers' data security, and should not rely on the bank to make sure that information is not inadvertently or fraudulently revealed. Banks also must meet NACHA data security requirements, but those obligations are separate and apart from those held by commercial organizations.

Electronic Statement Delivery

Organizations must keep records of their ACH payments. That includes not only account information, but customer authorization to debit an account. Because of the sensitive information those records contain, their secure storage is of vital importance. By law, these records are not destroyed immediately, which means there is a trove of valuable information that poses risk to individual consumers sitting around in electronic databases or on pieces of paper that record past financial events.

Typically entities have the option to receive electronic or paper statements. Because records are held for a period of time after the ACH transfers are completed, storage systems contain identifiable data that could be used for fraudulent activity. Paper statements, even kept in locked and monitored areas, are highly vulnerable to theft. It is less risky to keep records in electronic form, safeguarded by the security protocols. Fortunately, these are the same security protocols that also make sure the transmission of that information at the time of the transaction itself is also protected.

Regularly Monitor & Reconcile Accounts

Part of the benefit of the ACH network is the rapid resolution of payments. With that quick processing time, however, comes inherent risks. In particular since the ACH recently increased its processing time by finalizing transactions within the same business day, institutions and their clients must keep a close eye on funds transfers as soon as they clear accounts.

In order to ensure system integrity and to reduce risk at the institutional level, all entities should reconcile their ACH accounts on a daily basis. This means matching the number and value of payments originated and received over the system and spotting any inconsistencies. Although same-day clearance is now in place, payment failures, anomalies or returns may take days or weeks to show up. Daily reconciliation allows for quick execution of relevant procedures to identify errors or issues as well as why they may have occurred.

Leverage Encryption & Tokenization Technology

In order to meet ACH obligations to keep data secure, it is accepted practice to use secure sockets layer (SSL) encryption technology. As users of online technology, most people recognize the difference between a site marked "http://" versus "https://," although they may not have understood that this meant the site they were accessing was using SSL technology. Perhaps in a public access area, such as a coffee shop, using an internet connection, one has been stopped from visiting certain sites because a "https://" connection was not available. This means the network connection did not meet the site's required level of security, which is perhaps frustrating for the coffee shop consumer, but good news for companies accessing the ACH network. SSL encryption creates a bound link between a computer and a server that hosts the website. Without this technology, hacker programs that rest on unsecured sites wait for a user to submit information, which is then transmitted back to the hacker. SSL encryption prevents this unauthorized transmission from happening. Any entity engaged in ACH payment origination, receipt or transmission should do so using SSL encryption. Otherwise, at any unsecured stage in the payment process, a payor's sensitive, non-public information may be compromised.

Parties subject to the ACH rules must take reasonable steps to secure non-public data and prevent its unauthorized exposure. This includes anyone with access to bank account numbers, even if they are just going “through” the organization’s systems. Indeed, with ACH, this is exactly what’s happening. From the payment originator to the bank through the ACH to the receiving financial institution, private information is moving. Any party that processes this information should implement SSL technology to keep it safe from unexpected attack.

Verify Routing Numbers

Payment originators must take steps to prevent errors in their ACH batches. This is achieved partly by verifying that the account numbers they have received from their own customers are correct. Any mistakes in the routing number could result in a failed transaction that goes back to the originator. The fees associated with account number failures can place a significant financial burden on originating businesses, so simply taking steps to verify that the routing digits provided by customers are accurate and valid is cost-effective as well as being required by the NACHA rules.

Most companies verify routing numbers with the assistance of a provider offering routing number and account verification services. Taking the opportunity to determine the validity of these codes is essential not only to follow NACHA rules, but in order for companies to provide the best possible service to their customers. While this system of pre-transfer validation goes a long way toward preventing fraud, it also saves customers the embarrassment and confusion of a failed payment. With a verification service, companies can let customers know earlier that they may need to provide alternate information.

Conduct Ongoing Employee Education

In order for a company of any size to properly comply with NACHA rules, internal procedures must be clear and easy to follow. Employees must have a thorough understanding of how the ACH works and the importance of the work they do in order to verify transactions and maintain security. These individuals doing the hands-on work are at the core of NACHA compliance, so payment originators and other regular participants in the ACH process would be well-served to fully train and inform employees about the roles they play.

Depending on the nature of the organization, there may be an initial onboarding of key pieces of information relevant to individual jobs. Day-long workshops or refresher training, especially when there is an essential update to the NACHA rules, may also be good for various organizations. An in-depth training might include such information as:

- The origin and purpose of the ACH network
- The life cycle of a typical transaction
- The NACHA rules and obligations for compliance
- The potential penalties for failing to comply with NACHA
- Best practices for originating, handling, processing and receiving ACH transactions
- Security protocols and internal procedures to uphold customer confidentiality and to meet NACHA obligations

In addition to helping individual teams understand how important their roles and responsibilities are in upholding ACH network integrity, training offers evidence that a company has taken steps toward compliance. This evidence may be necessary in the event of a procedural audit or if they are called upon to respond to a report of a potential rules violation. In general, well-trained individuals may perform better simply because they understand why they are asked to uphold the levels of security incumbent upon their positions.

Improve Efficiencies & Ensure Compliance

NACHA rules are designed to facilitate the movement of electronic payments across the United States and, increasingly, through international borders. Participants in the network have obligations to both understand their responsibilities in the NACHA rules and to adhere to them. Viewing those obligations as fundamental to not only the integrity of the ACH network, but their own ethical practice as a commercial business, can make the process of compliance easier. In order to take care of customer data, many companies already implement steps to ensure their IT systems meet or exceed industry standards of security and thoroughly review internal protocols for keeping records secure. Following these ACH best practices, therefore, also makes for sound business procedures.

Most businesses choose to partner with outside organizations who are experts in a particular piece of the ACH compliance puzzle. Their technology teams may work with contractors in integrating secure software and SSL protocols. Professional educational organizations can work with companies to develop training workshops in order to support staff who must put ACH protocols into practice. Companies can work with Lyons Commercial Data to verify bank routing and account numbers, as well as to screen potential clients against OFAC lists. By making the right outside partnerships, companies can ensure they are compliance with NACHA rules, for the benefit of their organization and its customers.