Cathay Bank

ACH training and best practices

Summary

The Automated Clearinghouse ("ACH") networks allows clearing of electronic payment from bank to bank. The ACH networks are governed by NACHA Operating Rules and Guidelines (collectively, the "NACHA Rules") which apply to all entries and data transmitted through the ACH networks.

The NACHA Rules are updated and published annually. As an ACH Originator, you are required to comply with the NACHA Rules pursuant to your ACH Origination Agreement. As an Originator, you must have access to a copy of the Rules to ensure compliance. As a new ACH customer with Cathay Bank you are provided a free subscription for the calendar year in which you acquired this service. After the first calendar year, you may access the NACHA Rules for a fee at www.wespay.org/public. You have the option to access either a printed or electronic version.

What is the ACH?

The automated clearinghouse (ACH) is a computer-based electronic network for processing transactions, usually domestic low-value payments, between participating financial institutions. It supports both credit and debit entries to accounts held at participating depository financial institution ("DFI"). The ACH network is designed to process batches of payments containing transactions.

What is NACHA?

The National Automated Clearing House Association ("NACHA") administers the NACHA Rules and oversees the ACH networks.

What are NACHA Rules?

The NACHA Rules are the foundation for every ACH payment. By defining the roles and responsibilities of DFIs and establishing clear guidelines for each ACH Network participant, the NACHA Rules ensure that millions of payments occur smoothly and easily each day.

NACHA Rules are meant to safeguard your customers' sensitive financial and non-financial data and ensure that all ACH transactions are handled smoothly and securely. Sensitive information includes things like bank account numbers and routing numbers, social security numbers, driver's license numbers, and more. If you collect and store non-public sensitive information like this, you need to comply with NACHA requirements.

What is the ACH Legal Framework?

As the Originator, you must first obtain authorization to initiate a transaction to the Receiver's account or provide notice to the Receiver that a transaction will be initiated to their account. As the Originator, you must then create a file of ACH transactions assigning a company name that is easily recognized by the Receiver. The file is then sent to your Originating DFI ("ODFI"), which is Cathay Bank. We then verify the validity of the file and, at specified times, we transmit these files to an ACH Operator. The ACH Operator receives ACH files from the ODFI, edits the file to ensure the file is formatted properly and distributes files of entries to the Receiving DFIs ("RDFIs"). Each RDFI receives files of entries from

the ACH Operator for its receiving account holders ("Receivers"). Entries are posted based upon the Settlement Date. The Receiver will receive descriptive information about the ACH transaction, e.g., via periodic statement, including such information as the settlement date, dollar amount, and payee (i.e., Originator) name.

Settlement is the actual transfer of funds between participating DFIs to settle the payment instructions contained in an ACH entry. The ACH Operators, including the Federal Reserve Banks, provide settlement services for ACH entries. The timing of settlement is based upon the Effective Entry Date indicated on the ACH file and the time of its delivery to the ACH Operator. As the Originator, you will determine the Effective Entry Date of the file you send to us. This is the date you intend the entries to post to the accounts of the Receivers (e.g., employees or customers). When the ACH Operator processes an ACH file, the Effective Entry Date is read and entries are settled based upon that date, which is known as the Settlement Date. The Effective Entry Date in most cases is the same as the Settlement Date, but it is possible that the Settlement Date could succeed the Effective Entry Date. For example, if the ACH Operator cannot settle on the Effective Entry Date due to untimely file delivery, a stale date, or a weekend or holiday, the ACH Operator will make the Settlement Date the next business day.

Below are various points to consider with respect to the ACH Legal Framework:

- An Originator is any entity or person that creates an ACH transaction.
- Entries are broadly categorized as "consumer" or "corporate."
- Federal consumer protection regulations, including Regulation E, apply to consumer Entries.
- State law, including the Uniform Commercial Code Article 4A, may apply to corporate Entries.
- The ACH Network is capable of crediting or debiting checking or savings accounts.
- Most financial institutions receive entries.
- The ACH Network is a batch system (i.e., entries are not processed in real time).

What are your responsibilities as an Originator?

As an Originator, you are required to adhere to certain rules and agreements when initiating ACH transactions. Authorization must be readily identifiable as an authorization and have clear and readily-understandable terms (including the amount or timing of debits). It should also provide that the receiver may revoke the authorization by notifying the originator in the time and manner stated in the authorization.

You should retain a copy of the authorization for two years following the termination or revocation of the authorization.

Below are various points to consider with respect to your responsibilities as an Originator:

- You must obtain authorization regardless of whether the ACH transaction being processed is a debit or credit.
- You must obtain authorization from a customer when he or she makes a one-time/recurring ACH debit.
- You must indicate very clearly to the customer that they are authorizing a one-time/recurring ACH debit.

- You must provide appropriate notice if you are changing the amount or date of a debit.
- Ensure that you cancel a subscription promptly and stop making debits if a customer asks to cancel.
- If you collect hard copies of sensitive customer data, then you must take reasonable precautions to ensure they are stored securely and only allow employee access for legitimate business purposes.
- Whether you store information electronically or in paper form, you must ensure the information is secured from the point of collection to the time of destruction. Do not store sensitive information on portable devices.
- You must take reasonable steps to ensure customers' routing numbers are valid.
- You must take steps to verify a customer's identity, without regard to whether a transaction is authorized online or by phone.
- You must ensure secure transmission and storage of sensitive data.
- You must be vigilant about possible fraud and do whatever is "commercially reasonable" to ensure the ACH transactions you initiate are not fraudulent.
- You should have a clear written policy that governs how you protect sensitive data and outlines how you transmit, access, store, and protect confidential data from various threats and unauthorized use.

Do Originators have to comply with OFAC requirements?

You are required to check payees/ACH recipients against Office of Foreign Asset Control ("OFAC") compliance checklists.

- OFAC checklists contain lists of countries, groups and individuals with which U.S. Companies are not permitted to send or receive funds.
- The Bank helps protect our clients by informing them that it is against the law to send debit or credit entries to OFAC-blocked entities.
- You may check the OFAC SDN list at https://sanctionssearch.ofac.treas.gov/.

What is a Notifications of Change (NOC)?

NOCs are created by the Receiver's financial institution to notify the originator that information in a previous transaction needs to be updated. The information must be updated or corrected before the transaction is originated again. The Bank will notify you if it receives any NOCs for any of your transactions. Some of the more common reasons for initiating NOCs are:

- Previously-valid information in an ACH entry (Direct Deposit/Direct Payment) is now outdated and needs to be changed.
- Information in an ACH entry (Direct Deposit/Direct Payment) is erroneous and needs to be corrected.
- Banks have elected to consolidate routing numbers and want originators to use a different one.

The Receiving Bank warrants that the information it provides in a notification of change which it would like updated is correct.

ACH Rules require the originator to make changes or corrections within six (6) banking days of

receiving the notification of change before sending another entry. The Bank may pass along any fines incurred based upon your non-compliance.

What are returns?

Returns are credit or debit entries initiated by an RDFI (or the ACH Operator) that return previously originated credit or debit entries to the ODFI. Returns must be initiated within the timeframes established by the NACHA Rules. Consumer unauthorized returns may be returned within 60 days of posting. Returns that are unauthorized are the company's liability, and any disputes may have to be settled outside the ACH Network. The Bank recommends that you view your account activity, including any returns, daily.

What are reversals?

Reversals are credit or debit entries that reverse an erroneous entry. Reversals may only be made under certain conditions, including wrong dollar amount, wrong account, or duplicate transaction.

What are some sound practices to promote information security?

Information security is the responsibility of the Originator. Sound practices to promote information security include, but are not limited to, the following:

- Use a dedicated computer for all business online banking transactions, as casual internet browsing can expose your computer to malware
- Use and regularly update antivirus and anti-spyware software to monitor for spyware and/or malware.
- Remove the administrative rights on company computers to protect them against certain activities, including uploads, downloads and installations.
- Use strong passwords; passwords confine system access to authorized users and may extend the amount of time it takes a hacker to access a password through an attack. (The more complex passwords are, the more difficult they are to break. You should require employees to change passwords regularly (e.g., every 30, 60, or 90 days) and forbid users to reuse old passwords.)

What are the fraud risks for ACH?

Fraud challenges all participants in the ACH Network. Originators must remain vigilant to prevent and defend against fraud risk. There are certain common fraud schemes of which you should be aware. In one fraud scheme, fraudsters hack into an Originator's computer system using compromised User IDs and passwords and originate ACH credits to "mule" accounts created for the express purpose of committing fraud. Those accounts are then emptied and abandoned. The true Originator's account (your account) is debited for the invalid origination file. The credits are usually irretrievable by the time the fraud is discovered. The originator's credentials may have been compromised by an insider within the organization or stolen through key loggers or Trojan Horse programs on the compromised computer. Due to the risk this type of fraud presents, it is essential that all computer equipment your company uses to operate treasury management and ACH Origination applications is regularly updated and patched for security vulnerabilities (including use of and updates to firewall, virus protection, anti-malware protection and anti-spam protection.)

Cathay Bank

What is website spoofing?

Website spoofing is the act of creating a fake website to mislead individuals into sharing sensitive information. Spoof websites are typically made to look exactly like a legitimate website published by a trusted organization. To prevent fraud related to website spoofing:

- Pay attention to the web address (URL) of websites. A website may look legitimate, but the URL may have a variation in spelling or use a slightly different domain name.
- If you are suspicious of a website, close it and contact the company directly.
- Do not click links on social networking sites, pop-up windows, or non-trusted websites. Links can take you to a different website than their labels indicate. Typing an address in your browser is a safer alternative.
- Only give sensitive information to websites using a secure connection. Verify the web address begins with "https://" (the "s" is for secure) rather than just "http://".
- Avoid using websites for which your browser displays certificate errors or warnings.

What is phishing?

Phishing is a method of fraud by which an attacker attempts to acquire information by masquerading as a trustworthy entity in an electronic communication. Phishing messages often direct the recipient to a spoof website. Phishing attacks are typically carried out through email, instant messaging, telephone calls, and text messages (SMS). To prevent fraud related to phishing:

- Delete email and text messages that ask you to confirm or provide sensitive information. Legitimate companies don't ask for sensitive information through email or text messages.
- Beware of visiting website addresses sent to you in an unsolicited message.
- Even if you feel the message is legitimate, type web addresses into your browser or use bookmarks instead of clicking links contained in messages.
- Try to independently verify any details given in the message directly with the company.
- Utilize anti-phishing features available in your email client and/or web browser.

You may also want to consider having one computer in your office which cannot be used to browse the internet or read e-mails and which is your sole source of access to the treasury management system. Limiting access to the computer which is used to house and transmit ACH data may help avoid accidental downloads of harmful programs/viruses that could potentially compromise your transactions. Appropriate steps should be taken within your company to ensure that all User IDs, passwords, authentication methods and any other applicable security procedures issued to your employees are protected and kept confidential. All staff should be aware of the need for proper user security, password controls and separation of duties.

As ACH Origination is a higher-risk commercial banking function, we suggest that your company perform its own internal risk assessment and controls evaluation periodically to ensure you are considering all available security options.

Does the ODFI have the right to audit and originator?

Yes. We have the right to audit your compliance with the NACHA Rules and your compliance with the origination agreement at any time. We have the right to terminate the origination agreement immediately for breach of the NACHA Rules or applicable laws.

Cathay Bank

What are file delivery deadlines and cutoff times?

All transmissions to the bank must be completed by the established Cutoff Times in order for processing to take place on the same business day. Any transmission completed and received by the bank after such Cutoff Times or on any non-business day will be processed on the following Business Day.

What you should take away from this training?

NACHA Rules extend far beyond what is outlined here. You should always follow the NACHA Rules, applicable law, and best practices for ACH transactions. For example, you should obtain proper authorization for all ACH transactions, whether they are one-time or recurring. If you are changing the charge amount or date on which the transaction occurs, you should notify customers several days in advance. And, of course, if a customer asks to cancel his/her ACH payments, you must do so as soon as the request is made.