2025 Educational

ACH ORIGINATION

Lincoln
SAVINGS BANK
Member FDIC

In an effort to keep you safe and informed, Lincoln Savings Bank offers updates and reminders regarding the ACH network and best-practices. Information provided here is not comprehensive of all changes that may be implemented, this information has been curated to identify the changes that directly impact our Originator's general use of the Nacha network. The information included herein is intended as informative only. Please consider your own internal guidance, policies, or procedures, as well as legal advice that your business has received.

Corporate Account Takeover

"Corporate Account Takeover" occurs when cybercriminals take control of a business bank account through stolen credentials and access point manipulation. There are a great number of ways these criminals can gain access to systems, but the most prevalent model stems from the presence of malware received through email or websites.

The most common source of malware is on social media sites. Cybercriminals create several videos, photos, or articles with the goal of generating interest to click through. As soon as a victim clicks on an infected link, malware is then installed on the machine and can then spread across a business's internal network. Also common are emails that appear to be from respected organizations. These emails contain links or attachments that deploy the infectious code when opened.

The malware typically installs key-logging software and can potentially alter the functionality of the user's browser. The software logs all keystrokes and potentially even token-generated passwords. A cybercriminal then retrieves the data to ascertain the user's online banking credentials.

Target: Businesses Small and Large

Cybercriminals have targeted large businesses with a greater chance of a large strike and quick loot. But the tide has changed, and businesses of all sizes and stature are at risk, even shifting the greater focus to small businesses for the following reasons:

- Many small businesses now have access to do online funds transfers, initiate ACH transactions, and potential wire activity; plus,
- Small businesses typically need more resources to provide sufficient oversight and internal controls, which leads to single-user access to all systems and approval methods. As small businesses opt for "ease of access" and lowest cost options, they typically elect to waive dual-control scenarios or purchase password-generating tokens.
- Additionally, IT departments may be minimal, or on small budgets leading to less complex firewalls and malware detection and prevention methods.

Our Commitment to Help

While there are several functions that Lincoln Savings Bank employs to help protect you from a Corporate Account Takeover event.

- Lincoln Savings Bank requires multi-factor authentication for access that requires:
  - Login Name
  - Login Password
  - Out-of-Bank Temporary Access Code (Via phone call or text)
- We continue to strongly encourage dual control for all "risky" (Funds moving to or from accounts outside

of Lincoln Savings Bank) transactions.

- Provide alerting services for authorization or processing of transactions.
- Establishing limits for the number of transactions and transactions amounts based on actual customer needs and expectations.
- Use of our back-end Risk & Fraud Analytics analysis tool to review 30+ transaction variables and inspect them against historical values to determine and flag unusual activity. Any transaction that is identified as "suspect" results in a manual phone call to the account holder to validate its authenticity before releasing.
- Restrictions on access based on IP address and Day/Hour limitations through our Corporate Banking Solution.
- Required call-back approval on all wire requests.

Sound Business Practices

Good business practices in preventing Corporate Account Takeover include:

- Utilizing Dual-Control for all online transactions.
- Use and keep all anti-virus and malware detection and prevention software up to date.
- Restrict Online banking access to within business networks and firewalls. Avoid public networks.
- Minimize computer use where Online banking is accessed. Do not use this computer for general online navigation and avoid social networks.
- Employ "safe browsing" software that prevents malware and key-logging software from running.
- Monitor and reconcile your accounts daily and be diligent in detecting anomalies.
- Use the alerts provided by Lincoln Savings Bank's online banking system to notify of transaction creation.
- Utilize out-of-bank authentication at login and also at transaction creation.
- Keep account limits as close to business needs as possible.
- To proactively prevent fraud, utilize additional fraud-prevention services like positive pay and ACH block.

Fraud and Phishing

Phishing scams are typically fraudulent emails or messages that appear to come from legitimate sources. The emails may contain malware as discussed in the "Corporate Account Takeover" section, or links to impersonated websites (phishing). The phony website appears to be a website that you may otherwise use in all facets; however, when entering login credentials, it will generally present a page that indicates the site is down or unavailable. At this point, fraudsters have already logged your credentials to the real site and can begin attempting access.

It is important to stay diligent in motoring for these types of emails to help protect against unintentionally exposing secure data. Some of the things you can look for are:

- ***Unauthenticated Email Addresses*** **-** You need to authenticate the sender's legitimacy because email addresses can be spoofed. Some Internet service providers have more robust filters than others and will check the sending IP against an authenticated IP address and domain name server. Always verify a request to change account information in person or by phone.
- ***Typos and Grammatical Mistakes*** **-** Fraudulent emails are often mass-generated- possibly even translated using software from foreign languages- and contain nonsensical grammatical flows, incorrect syntax, or use of pronouns. It is also commonplace to intentionally use incorrect spelling to bypass industry-standard spam filters
- ***Awkward Greetings*** **-** Generic greetings that are not referring directly to the recipient. May be generally stated, such as "Client."
- ***Sense of Urgency*** **-** Many phishing emails use compelling language for an immediate call to action. They will encourage you to act immediately for the sake of security or to prevent fraud or loss.
- ***Randomly Generated Numbers*** **-** Phishing emails may include account or reference numbers to try adding "legitimacy" to their message.

Credential Stuffing Attacks

Credential stuffing attacks are on the rise and are here to stay. Similar to CATO and Phishing attacks mentioned earlier, fraudsters have another of many arrows in their quiver that is being utilized more today than before.

In short, a credential stuffing attack targets websites where users are required to "authenticate" into a secure area to perform or access traditionally secure services or information. To do this, bad actors purchase, or otherwise obtain, lists of user credentials, including names, usernames, passwords, and occasionally more. They then turn around and target websites with these lists and through automated means, attempt to gain access by "blindly" throwing information against the site to see if something works.

It is important to note that you, the end user, are not generally impacted by this volume of attempts. Through our vendor partnerships, Lincoln Savings Bank has mitigating processes to handle the volume through a series of measures. However, you could still be at risk!

Information with which the fraudsters may attempt to access sites is almost always stolen from other data breaches. This means if you had data on any of the numerous sites that have been previously compromised, your information, along with the username and password used on that site, is now available to be used in these attacks. The fraudsters might get a hit if you use the same login name and password on one of those sites and your online banking.

How to Keep Yourself Safe

- Never use the same login ID and password for online banking as you use for any other site
- Keep your email address up to date with in online banking
- Utilize online banking alerts to be notified if your online access has been attempted without your knowledge. (Someone may inadvertently or directly enter your login but enter an incorrect password. This will generate an email alert to the address on your online banking profile)
- Contact LSB if anything seems suspicious

How We Help

- System monitoring
- Notifications of invalid login attempts
- You are required to enter an "out of band" authentication code if logging in from an unregistered browser. These are delivered via phone call or text message.
- For questions, to update your contact information, or for more information on how we're here to protect you, email us at TMSupport@MyLSB.com.

Links

Many phishing emails rely on external links to direct you to a spoofed website, where they will gather the information you willfully enter. Some phishing websites are blatant enough to ask you to enter account numbers, debit/credit card numbers, security codes, and PINs. By hovering over the link in an email, you can occasionally view the source code to where the link is directed, and this may be an obvious indicator of nefarious intentions.

Use of Logos, Websites, and Addresses

In an attempt to seem legitimate, phishing emails may contain authentic business logos, addresses, and phone numbers to help lower your initial skepticism of the email.

Pre-Notifications

Prior to initiating the first credit or debit entry to a Receiver's account or if account information changes, LSB strongly recommends that an Originator originate a pre-notification entry. Originators may initiate subsequent entries as soon as the third banking day following the settlement date of the prenote entry, provided the originator has yet to receive a return or COR Entry for that Prenote Entry. Suppose a return or COR entry is received. In that case, the originator must only send subsequent Entries to the receiver's account once they have remedied the reason for the Return Entry or made corrections as requested by the NOC.

Notification of Change (NOC)

A NOC is a non-dollar entry sent by a Receiving Deposit Financial Institution (RDFI) to notify the Originating Deposit Financial Institution (ODFI) (Lincoln Savings Bank) that information provided for a recipient is no longer valid. NOCs allow the RDFI to return information to the ODFI and, subsequently, the originator without returning the initiated ACH.

Upon receipt of a NOC, we shall notify the originator, who shall be required to make the requested change within six banking days of receipt, or prior to the next transmittal to the recipient, depending on which is later.

Returned Items

Returned entries may only be re-initiated if returned for insufficient funds (R01) or uncollected funds (R09) and are limited in number to two and must be initiated within 180 days of the original entry date. An entry returned for stop payment (R08) or an authorization issue may only be re-initiated if the originator has received appropriate authorization to re-initiate the payment.

When re-initiating a returned item, the words "RETRY PYMT" in all capitalized letters are required in the Company Entry Description field. Identical content is required in the following fields: Company Name, Company ID, and Amount. Modifications to other fields are permitted but only to those necessary to correct an administrative error made during processing.

We will report return information to originators within two banking days from the settlement date.

Return Reason Codes

- R07 - Authorization Revoked by Customer: The consumer receiver has revoked the authorization previously provided to the originator for this debit entry. The receiving financial institution must collect a Written Statement of Unauthorized Debit from the receiver.
- R10 - Customer advised originator is unknown to the receiver and/or Originator is Not Authorized by Receiver to Debit Receiver's Account: The Consumer Receiver does not know the originator's identity and has no relationship with the originator or has not authorized the originator to debit his account. The receiving financial institution must collect a Written Statement of Unauthorized Debit from the receiver.
- R11 - Customer advised entry not in accordance with the Terms of Authorization: The receiver has notified their financial institution that the originator and the receiver have a relationship and an authorization to debit does exist, but there is still an error in the payments such that the entries do not conform to the terms of the authorization.
- R29 - Corporate customer advised not authorized: The non-consumer receiver has notified their financial institution that the receiver has not authorized a certain transaction.

Reversals

If an originator creates erroneous ACH entries or files, corrections may be made by initiating reversing entries or files.

An erroneous entry or file is defined as:

- A duplicate of an entry previously initiated by the originator or ODFI
- Orders payment to or from receiver not intended to be credited or debited
- Orders payment in a dollar amount different than was intended
- Originated within five banking days following the settlement date of the erroneous entry

Note: We recommend that originators use an authorization agreement (credits) with their receivers that states they are authorized to debit/reverse any entries made in error. This is good business practice and will help with any disputes in the future.

Allowed Standard Entry Class (SEC) Codes

PPD - Pre-arranged Payment or Debit

- Most commonly used for direct deposit
- For business-to-consumer use only
- The written agreement must be on file with the recipient if you debit their account. Written agreement to debit a consumer must be kept on file for 2 years after termination.
- It is suggested that the written agreement is on file for credit entries, but verbal agreement is acceptable.

CCD - Cash Concentration or Disbursement

- For business-to-business use only

- It can be used for moving funds between a business' accounts at different institutions
- Used for payments or debits to other businesses
- Agreements are handled by contract authorization between companies.

Important Reminders

Entry Types by SEC Code - You cannot combine different recipient types (consumer, business) within a single batch. As noted on page 4, different SEC codes are required based on the recipient type.

Example: You cannot generate an "ACH Batch" that contains employees for weekly payroll and also businesses you are paying for invoices or other payment needs. You would need to originate one PPD batch containing all the employee transactions and one CCD batch containing all the B2B transactions.

Subsidiaries - If your online banking supports more than one legal entity, and more than one legal entity does any ACH or Wire origination, you must utilize the appropriate subsidiary when generating the transaction to ensure compliance with NACHA regulation. The subsidiary fills in the required fields such as Business Name and Company ID. Failure to do so is a breach of NACHA regulations and may result in a recipient dispute of the transaction. Failure to comply with either of these may result in the removal of origination capabilities.

Access to 2025 NACHA Rules - In addition to the NACHA Operating Rules and Guidelines you were provided initially, it is expected that you are staying up to date with the annual publication. While the rules may be purchased from a number of vendors, including directly from NACHA.org, we would be happy to provide a copy for you upon request at a discounted rate. The publication is available in digital format or as a printed book. If you would like to request pricing or to order a copy of the publication, please contact us at TMSupport@MyLSB.com

Documentation Requirements

ACH Limit Increase form - When you enter a Collection, Payment, or Payroll ACH and receive an error message "Over Your Limit," it states the ACH you are trying to originate exceeds your approved limit. We set two types of approved limits: A Daily Limit-that is a dollar amount set for the total daily amount of credits or debits, and A Monthly Limit-that is the dollar amount set for the total monthly amount of credits or debits. A month is defined as a 30-day rolling calendar. Please do not hesitate to call or email Treasury Management Support if you receive an error message. Please provide us with the type of ACH you are originating and the amount needed to accommodate your needs. That will help us in setting new limits. To complete a limit increase, we will send you a form to sign. Once that form is signed and returned, we will raise your limit so you can successfully submit your ACH.

Periodic ACH Questionnaires - This document asks for additional details about how your company uses our ACH solution. We will email the person(s) who is most often submitting ACHs through online banking on behalf of your company. The email will include a link to make it simple to complete the questionnaire online. Regulations do require that we collect a questionnaire from originators periodically.

Periodic ACH Audits - We are required to verify approvals for collections to a consumer account. We will pull two random recipients from one of your files created within the last 90 days and request that you provide us with proof of authorization for these two recipients.

If you have any questions or would like further information, please reach out to your Relationship Manager at 1-800- 588-7551