LSBPRO

2018 Educational Piece
ACHpro / CATO

In an effort to keep you safe and informed, Lincoln Savings Bank offers updates and reminders regarding the ACH network and best-practices. 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 as well.

2018 ACH Rules Changes

Phase 3 of Same Day ACH - Moving Payments Faster

Beginning March 16, 2018, RDFIs will be mandated to make funds available from same day ACH credits (such as payroll Direct Deposits) to their depositors by 5:00 PM at the RDFI's local time.

Source: NACHA.org - NACHA Operating Rules

Impact to you

If you feel you may benefit from the advanced settlement windows offered by Same Day ACH, please contact LSBpro to learn more.

E-mail: LSBproSupport@mylsb.com

Same Day ACH in Review

Phase 3 of Same Day ACH - Moving Payments Faster

The Rules enable the option for same-day ACH payments through additional ACH Network functionality, without affecting previously available ACH schedules and capabilities:

Lincoln Savings Bank is able to submit files of same-day ACH payments through two additional clearing windows provided by the ACH Operators:

- A morning submission deadline at 9:00 AM cst, with settlement occurring at 1:00 PM.
- An afternoon submission deadline at 1:00 PM cst, with settlement occurring at 5:00 PM.

- Virtually all types of ACH payments, including both credits and debits, are eligible for same-day processing. Only international transactions (IATs) and high-value transactions above $25,000 are not eligible. Eligible transactions account for approximately 99 percent of current ACH Network volume.

All RDFIs are required to receive same-day ACH payments, thereby giving ODFIs and Originators the certainty of being able to send same-day ACH payments to accounts at all RDFIs.

Source: NACHA.org - NACHA Operating Rules

$294,694,362

ACH Dollars originated by Lincoln Savings Bank Businesses in 2017

Business E-mail Compromise
Be on the Lookout!

Business e-mail compromise (BEC) is a sophisticated spin on the tried and true art form of deception. While BEC made it's first real impact in 2013, it's going as strong as ever in 2017 heading into 2018.

In it's most simplistic form, Business E-mail Compromise occurs when an impostor sends an e-mail to an employee of the company to transmit a payment, generally by wire, to some other company or individual using information included with the e-mail. What makes the BEC difficult to identify is that the fraudsters will attempt to make the e-mail address they are sending the request from as legitimate as possible, sometimes looking almost identical to your own company's e-mail. Occasionally this e-mail simply references a purchase that needs to be made Today to create a sense of urgency and skip any internal processes that may be in place to help verify transactions. Alternative, the fraudsters may have already embedded a virus-like program in your computer, or another company that monitors correspondence. Once you have verified a purchase with a legitimate company, the fraudsters will send an e-mail with instructions for payment that may include the dollar amount and recipient that you're expecting to pay, but with altered instructions that direct the funds to an account held by the thief.

In an effort to protect yourself, and your company, consider these tips:

- Create a rule to detect e-mails that identify if an e-mail is external in nature.
  - Example: If you're domain is Examplecompany.com, an e-mail received from Examp1ecompany.com would be flagged as "External" because they have swapped the letter "l" with the number "1" in an effort to deceive
- Flag e-mails where the sender and reply address are different.
- Setup an internal "out of band" verification process to approve requests. Out of band would be any communication that is different than the initial communication. In this case, where an e-mail is the initial request, verify with the e-mail sender by in-person conversation, phone call, or text message.
- Stay diligent in your processes and reviews.
- Trust your intuition, if something seems odd, or out of the norm, then follow-up with the sender before you execute.

Corporate Account Takeover

"Corporate Account Takeover" occurs when cyber criminals 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 e-mail or websites.

The most common source of malware in today's environment is through social media sites. Cyber criminals create a number of 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' internal network. Also common in the professional are e-mails that appear to be from respected organizations. These e-mails contain links or attachments that deploy the infections code when opened.

The malware typically installs key-logging software, and potentially the ability to alter the functionality of the users browser. The software logs all key strokes and potentially even token generated passwords. The data is then retrieved by a cyber criminal to ascertain the user's online banking credentials.

Target: Businesses Small and Large

Historically cyber criminals have targeted large business with the greater change of a large strike and quick loot. But the tide has changed and business of all size and stature are at risk, even shifting the greater focus to small businesses for the following reasons:

- With the advancement of Cash Management services, many small businesses now have access to do online funds transfers, initiate ACH transactions, and potentially wire activity, and;
- Small businesses typically lack the 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 the purchase of 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 things that Lincoln Savings Bank cannot do to ensure that best practices are followed in preventing Corporate Account Takeover, we do pro-actively take steps to encourage our customers to take preventative steps as well as performing behind the curtain actions to prevent fraud.

- Lincoln Savings Bank requires multi-factor authentication for access that requires:
  - Login Name
  - Login Password
  - Out of Bank Temporary Access Code (Typically via phone or text)
- Strongly encourage dual control for all "risky" (Funds moving to or from accounts outside of Lincoln Savings Bank) transactions
- Provide alerting services for authorization of "risky" transactions
- Establishing limits for number of transactions and transactions amounts based on true 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.

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 performed. 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 band authentication at login and also at transaction creation
- Keep account limits as close to business needs as possible
- Utilize additional fraud prevention services like positive pay and ACH block to pro-actively prevent fraud.

Fraud and Phishing

Phishing scams are typically fraudulent e-mails or messages that appear to come from legitimate sources. The e-mails may contain malware as discussed in the "Corporate Account Takeover" section, or may contain 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. However, 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 e-mails to help protect against unintentionally exposing securing data. Some of the things you can look for are:

Unauthenticated E-mail Addresses

Because e-mail addresses can be spoofed, you need to authenticate the legitimacy of the sender. Some Internet service providers have stronger filters than others and will check the sending IP against an authenticated IP address and domain name server.

Typos and Grammatical Mistakes

Fraudulent e-mails are often mass generated and even translated using software from foreign languages and contain nonsensical grammatical flows or incorrect syntax or use of pronouns. It is also common place 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 e-mails 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 e-mails may seem to have included account numbers or references numbers to try and add "legitimacy" to their message.

Links

Many Phishing e-mails rely on external links to direct you to a spoofed website they will gather information that you willfully enter. Some Phishing website 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 e-mail, 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 e-mails may contain authentic business logos, addresses and phone numbers to help lower your initial skepticism of the e-mail.

21,489,636,583

Total ACH Batches processed in the network -2017 per NACHA.org

5.7%

from 2016

Allowed Standard Entry Class (SEC) Codes

PPD - Pre-arranged Payment or Debit

- Most Commonly used for Direct Deposit
- For Business to Consumer use only
- Written Agreement must be on file with Recipient if you are debiting their account.
- Written Agreement suggested to be on file, but verbal ok for credit entries.

CCD - Cash Concentration or Disbursement

- For Business to Business use only
- Can be used for moving funds between a business' own accounts at different institutions
- Used for payments or debits to other businesses
- Agreements are handled by contract authorization between companies.

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, the we shall notify the Originator, who shall be required to make the requested change within 6 banking days of receipt, or prior to the next transmittal to the recipient. Which ever is later.

RETURN REASON CODES

Return Code Description
R01 Insufficient funds
R02 Account closed
R03 No account found
R04 Invalid account number
R05 Unauthorized debit using corporate SEC
R06 Returned/ODFI's request
R07 Authorization revoked by customer (non-POP, TEL, or WEB with PTC=S)
R08 Payment stopped (non-RCK)
R09 Uncollected funds
R10 Customer advises not authorized (non-RCK)
R11 Check safekeeping entry return
R12 Account sold to another DFI
R13 Invalid ACH routing number
R14 Representative Payee deceased or unable to continue in capacity
R15 Beneficiary or account holder (other than representative payee deceased)
R16 Account is frozen
R17 File record edit criteria
R20 Non-transaction account
R21 Invalid company identification
R22 Invalid individual ID number
R23 Credit entry refused by receiver
R24 Duplicate entry
R29 Corporate customer advises not authorized
R31 Permissible return entry
R33 Return of XCK entry
R37 Source document presented for payment (ARC, BOC, and POP)
R38 Stop payment - source doc (ARC and BOC)
R39 Improper source document (ARC, BOC, and POP)
R50 State law affects RCK acceptance
R51 RCK item is ineligible
R52 RCK stop payment
R53 Item and ACH entry presented for payment (RCK only)
R80 Cross-border payment coding error
R82 Invalid foreign receiving DFI ID
R83 Foreign receiving DFI unable to settle
R84 Entry not processed by Gateway Operator

*Note: This is not a complete listing of return codes. For more codes, please refer to your NACHA ACH Rules book.

RETURNED ITEMS

Returned entries may not be re-initiated unless the entry was 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 is 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 of an entry.

We will report Return information to Originators within 2 banking days from the settlement date.

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:

- is 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 then was intended
- Must be originated within 5 banking days following settlement date of the erroneous entry.

Enter REVERSAL (must be in all capitalized letters) in the description field of the Company Batch Header Record.

- Will need to build a new Batch Record
- Change the transaction codes to offset entries (i.e., debits reverse credits)
- The Effective Date should be the same date as the original entry/file date for future dated files

Notify the Receiver of the reversal by the settlement date.

In the case of an erroneous file, transmit a correcting file with the reversing file.

> 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.

Resources

Lincoln Savings Bank

www.mylsb.com/business

Support

E-mail: ***LSBproSupport@mylsb.com***
Phone: ***515-777-7940***

NACHA

www.NACHA.org

Jon Parker, AAP
1st VP Business Banking and Services
jon.parker@mylsb.com

Jon has been in the banking industry for over a decade, and with Lincoln Savings Bank for four years. He currently oversee our Treasury Management Department as well as Business Banking and Online Services. He received his "Accredidated ACH Professional" designation in 2017.