LSBPRO

2020 Educational
ACHpro

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.

2020 ACH Rules Changes

Same-Day ACH (SDA) - Increased Entry Limits

Effective March 20, 2020

Beginning March 20, the limit on Same-Day ACH entries, both credit and debit will increase from $25,000 to $100,000.

Source: Nacha.org - Nacha Operating Rules

Impact to you

Please note that prevailing limits on your account will persist. Should you have a need to increase your limits for use, please contact your Treasury Management Officer, or LSBproSupport for assistance.

E-mail: LSBproSupport@mylsb.com

Repurposed Return Code - R11

Effective April 1, 2020

In an effort to provide useful return information, Nacha has updated the Name and purpose of R10, and completely repurposed R11.

R10 -

- Previously - "Customer advises unauthorized, improper, ineligible, or part of an incomplete transaction"
- Now - "Customer advises originator is not known to receiver and/or is not authorized by received to debit receiver's account"

R11 -

- Previously - "Check truncation entry return"
- Now - "Customer advises entry not in accordance with the terms of the authorization"

Source: Nacha.org - Nacha Operating Rules

$618,709,444

ACH Dollars originated by Lincoln Savings Bank Businesses in 2019
25% Increase from 2018

Repurposed Return Code - R11 (Continued)

Impact to you

Previously, when a recipients' account was presented with an ACH entry that they didn't recognize, authorize, or was in an amount or date that was not agreed upon, the only option was to return the transaction as an R10. This forced the originator to cease all entries and the only path forward for corrective entry was to contact the recipient outside of the ACH system to obtain a new authorization.

With the re-purposing of the R11 trancode, a customer is able to report to their financial institution that while the Originator is known, and the transaction is not as expected for some reason. If the transaction is returned with the R11, then the originator is granted the ability to fix the transaction and re-initiate without the need to seek a new authorization. This provides a simpler and more streamlined process for making corrections that fall within this realm. Note - the re-initiated entry must be made within 60 days of the R11 receipt.

To assist in the process, if we receive an "R11" return for a transaction that you've originated, we will notify you with the reason as provided within the addenda information to make corrections on, similar to how you may be notified of a "Notice of Change".

Here is an example of when each code may be used.

R10 -

- Receiver does not know Originator
- Receiver has no relationship with Originator
- Receiver has not authorized Originator to debit account

R11 -

- Debit Entry for an incorrect amount
- Debit Entry was debited earlier than authorized
- Debit Entry is part of an incomplete transaction
- Debit Entry was improperly re-initiated

Important

Receiving an "R11" return will count as an "unauthorized return" for purposes of Nacha threshold management.

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 are e-mails that appear to be from respected organizations. These e-mails contain links or attachments that deploy the infectious code when opened.

The malware typically installs key-logging software, and potentially the ability to alter the functionality of the user's 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 chance 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 potential wire activity; plus,
- 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 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 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. Any transaction that is identified as "suspect" results in a manual phone call to the account holder to validate it's 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.
- 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. 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 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- possibly even translated using software from foreign languages- and contain nonsensical grammatical flows or 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 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

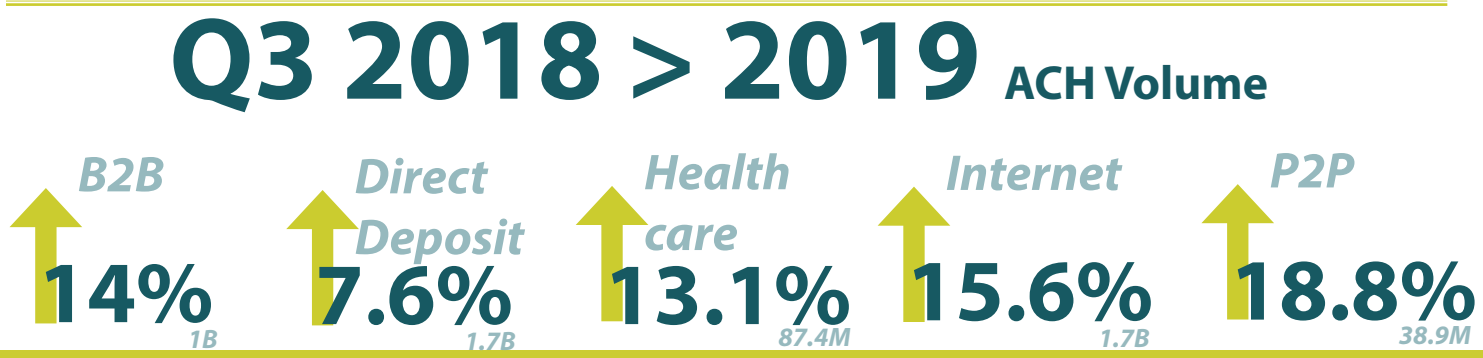
Phishing e-mails may seem to have included account numbers or reference numbers to try and add "legitimacy" to their message.

Links

Many Phishing e-mails rely on external links to direct you to a spoofed website, where 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.



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, 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.

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)
R08 Payment stopped (non-RCK)
R09 Uncollected funds
R10Customer advises, unauthorized, improper, ineligible, or part of an incomplete transaction (non-RCK)
R11 Customer advises originator is not known to receiver and/or is not authorized by received to debit receiver's account
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 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.

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 then was intended
- originated within five 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.

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 arrow 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 which include name, usernames, passwords, and occasionally more. They then turn around and target website 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. Lincoln Savings Bank through our vendor partnerships have mitigating processes in place 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 are 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. If you happened to use the same login name and password on one of those sites, AND your online banking, then the fraudsters may get a hit.

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 e-mail address up to date within 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 you login, but enter an incorrect password. This will generate an e-mail 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
- 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, e-mail us at lsbprosupport@mylsb.com

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 of the employee transactions, and one CCD batch containing all of the B2B transactions.

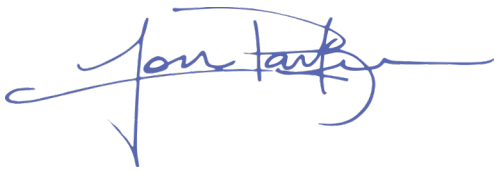
Subsidiaries

If your online banking supports more than one legal entity, and more than one legal entity does any type of 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 removal of origination capabilities.

Access to 2020 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 the printed book. If you would like to request pricing, or to order a copy of the publication, please contact us at LSBprosupport@mylsb.com.



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 six years. He currently oversees our Treasury Management Department as well as Business Banking and Online Services.