FIRST NATIONAL BANK OF HUTCHINSON

Fall 2019

WHAT ARE NOCS AND WHAT AM I SUPPOSED TO DO ABOUT THEM?

NACHA Requirements for Responding to an NOC

What is an NOC?

NOCs (Notifications of Change) are any posted Entries or Prenotification Entries that contain invalid or erroneous information and should be changed.

How will I know I have an NOC?

We as the Originating Depository Financial Institution (ODFI) must provide you, the Originator, the NOC within **two banking days** of the Settlement Date of the NOC we have received. We will send this to you via whatever means has been agreed to (e.g., secure email, mail, fax).

What do I do when I receive an NOC?

As the Originator, you must then make the changes specified in the NOC within **six banking days** of receipt of the NOC information **or prior to initiating another Entry to the Receiver's account**, whichever is later.

For monthly or bi-weekly recurring payments, this means you must correct prior to transmitting the next entry. However, for weekly recurring payments, it may take two payment cycles (i.e., within 6 banking days) before the correction is made. In either case, you may choose to verify corrected information with your Receiver before updating the payment information.

What happens if I don't make the changes?

An overview of the Rules Enforcement process explains that potential fines related to non-response to NOCs begin at $1,000.

When a NOC is not corrected, the following steps can be taken by the Receiving Depository Financial Institution:

1. Financial institutions may report an alleged violation of the *Rules* to the National Automated Clearing House Association (NACHA) within 90 days of the occurrence by completing and submitting a signed Report of Possible *ACH Rules* Violation form, along with documentation supporting the claim.
2. Each Report is evaluated by NACHA. A Notice of Possible *ACH Rules* Violation will be sent for a first-time infraction explaining the sited *Rules* violation and possibility that fines may be imposed if the violation is not corrected.
3. The financial institution must respond to the Notice within 10 banking days of receipt and either (1) acknowledge the violation and intent to correct the problem by a specified date, or (2) provide a statement, along with supporting documentation, of why the institution doesn't believe a *Rules* infraction occurred.
4. If NACHA receives a complete and timely response, no additional action will be taken unless (1) NACHA believes the timeframe for resolution is excessive, or (2) NACHA receives an additional *Rules* violation report. In these situations, NACHA will forward the case to the *ACH Rules* Enforcement Panel for evaluation and possible assessment of a fine or penalty.

So, the next time you receive an NOC, follow these simple requirements to correct your files so they have the most current account information.

If you have any questions, please don't hesitate to ask us. We're here to help!

Contacting ACH Support

Contacting ACH Support at The First is easy! We have a new ACH Coordinator, Sarah Winkler, who is excited to begin assisting you. Sarah has previously worked in Customer Support and we appreciate your patience as she continues to learn her new position. It is important to note that if Sarah is ever away from her desk you may speak with any member of our **Customer Support** team by calling **620.663.1521**. You will always get an immediate response and they can help you with risk and fraud overrides and user login issues. They are friendly, knowledgeable, and always available**!** Also, if needed, they can forward your call to another member of the ACH team or to Sarah's voicemail.

You may also email **ACHSupport@fnbhutch.bank** at any time, and any one of our ACH experts will be able to respond!

New Wire Fraud Scam Sends Paychecks to Criminal Accounts

Around two or three times per month, KVC Health Systems, a midsize nonprofit agency for child welfare based in Kansas City, receives phishing emails from criminals with the goal of rerouting an employee's paycheck via direct deposit.

The emails look legitimate at first, as though they come from the CEO, CFO or payroll director.

The scammer is trying to convince human resources personnel to change the bank account and routing information the employee uses to have paychecks direct-deposited. Once routed to the criminal's account, the company is on the hook for replacing the stolen funds and the employee faces the inconvenience of a late paycheck.

It's a new version of wire fraud scams that have devastated businesses in recent years, and a more focused version of a series of payroll fraud crimes that the IRS warned late last year were on the rise. The fraud is growing, experts said, because it easily bypasses many existing technical controls, and the small sums stolen are inoffensive enough that they can be folded into the cost of doing business.

"The fake emails defy many existing controls for malicious communications," said Erik Nyberg, director of information technology at KVC. "They are usually well written, cordial and lack the misspellings, grammar mistakes and exclamation points that would trigger many popular email filters that search for spam or phishing attempts.

"They might just say, 'I need to update my direct deposit information,'" said Nyberg. "Or they start with, 'Hey, do you have a second?' and if that target person responds, then they go from there." KVC has had a few near misses, Nyberg said, but has not transferred any paychecks to scammers.

A New Scam with a Convincing Pitch

The scam has only emerged in the past month, according to Adrien Gendre, chief solutions architect at email security company Vade Secure.

Many companies "have put processes in place to validate big wire transfers, so now [criminals] want to stay under the radar. It's a new approach, and every day we have more customers reporting it," he said.

Gendre said a dozen Vade companies have reported attempts to change direct deposit information.

The scam not only bypasses some email controls, but it also bypasses warnings companies may have already issued to their employees about wire fraud, because scammers aren't asking for money or an invoice transfer—they're simply asking to change a bank account number.

The fraudsters typically impersonate the company's higher-value employees, like the CFO or CEO, Nyberg said. The emails are usually brief, polite and lightly urgent, and often ask HR personnel to change the direct deposit information quickly, "before the next paycheck."

Others try to discourage the target from calling, by writing "I am going into a meeting now."

The spoofing doesn't require the criminal to hack into anyone's email account, as it often does with bigger-ticket wire fraud. The scammers generate the fake emails with free services like Gmail—the scammer simply opens a new Gmail account and fills in the employee's name—which allows them to get around tools meant to detect hacking attempts on employee email, Nyberg explained. Employees may not notice, either because they are working quickly and they

see SCAM on page 3

SCAM continued from page 2

don't notice the full email address, or they are working on a mobile device where only the person's name is displayed in the "from" field, he said.

Why would scammers target a nonprofit? Nyberg said he expects that the organization may be attractive in part because of its genial culture: "The nature of our work is helpful, people who are very literally here to help other people. They might also believe that our training isn't as rigorous as a Fortune 500 company," he said.

Despite the relatively low dollar figure associated with this scam—thousands of dollars compared with hundreds of thousands in a typical wire scam—Gendre said it's so cheap to execute that he expects it to become more attractive for criminals.

"They have found a way to automate it, which means you can scale it. You may not make $100,000 in one hit, but you may be able to make 20 hits staying in one company and be able to make your return [on investment]."

How to Combat the Scam

To fight the threat, Nyberg said the organization has focused on training people on a simple truth: "The CEO is never going to email you out of the blue and ask you for any deposit changes. And, if you have any sliver of a doubt, call the person who is making the request."

Gendre said his company has used "natural language processing," which analyzes the language used in incoming emails to test for "urgency," then flagging those emails as potentially suspicious, especially if they come from a new email address.

Nyberg also said they've asked executives to avoid using their personal emails when sending messages to staff. The company has also tweaked its email filters to pick up on common hallmarks of the request.

Source: CNBC

Non-Processing Days for 2020

2020 Observed Holidays

New Year's Day	Wednesday, January 1
Martin Luther King, Jr. Day*	Monday, January 20
Presidents' Day	Monday, February 17
Memorial Day	Monday, May 25
Independence Day	Saturday, July 4
Labor Day	Monday, September 7
Columbus Day*	Monday, October 12
Veterans Day*	Wednesday, November 11
Thanksgiving Day	Thursday, November 26
Christmas Eve (Closed at noon)	Thursday, December 24
Christmas Day	Friday, December 25

*The Hutchinson Dillons location will be open

2019 RECAP OF ACH RULE CHANGES

The 2019 edition of the NACHA Operating Rules & Guidelines contains changes related to the following amendment:

Expanding Same Day ACH: Faster Funds Availability (effective September 20, 2019)

The Faster Funds Availability rule will provide faster funds availability for many ACH credits. Funds from Same Day ACH credits processed in the first same day processing window will be made available to the Receiver for withdrawal by 1:30 p.m., RDFI local time. Funds from all non-Same Day ACH credits (regardless of SEC Code) that are made available to the RDFI by 5:00 p.m., RDFI local time, on the banking day before Settlement Date will be available to the Receiver for withdrawal by 9:00 a.m., RDFI local time, on Settlement Date.

Same Day ACH Dollar Limit Increase (effective March 20, 2020)

The Same Day ACH Dollar Limit Increase rule will increase the per-transaction dollar limit from $25,000 to $100,000. At implementation, both Same Day ACH credits and Same Day ACH debits will be eligible for same day processing up to $100,000 per transaction.

New Same Day ACH Processing Window (effective September 18, 2020)

The New Same Day ACH Processing Window rule will create a new processing window that will enable ODFIs and their customers to originate same day transactions for an additional two hours each banking day. The new window will allow Same Day ACH files to be submitted to the ACH Operators until 4:45 p.m. ET (1:45 p.m. PT). RDFIs will receive files from this third window by 5:30 p.m. ET (2:30 p.m. PT), with interbank settlement occurring at 6:00 p.m. ET (3:00 p.m. PT). RDFIs will need to make funds available for credits processed in the new window by the end of their processing for that Settlement Date. All credits and debits, and all returns, will be eligible to be processed in the new Same Day ACH window, with the exception of International ACH Transactions (IATs), Automated Enrollment Entries (ENRs), and forward entries in excess of the per-transaction dollar limit.

ACH Processing Times

A friendly reminder that our processing deadline is:

4:30 p.m. for ACH files and 3:00 p.m. for Wire Transfers

Our processing times are automated and cannot be over-ridden.
Any files after the cut-off will be processed on the next business day.

Please note that on **Christmas Eve** we will be accepting ACH files only until **12:00 p.m.**