



PAYMENTS INSIDER

e-Newsletter

FALL 2019

DO "ACH RULES" AUDIT REQUIREMENTS IMPACT YOUR BUSINESS?

by **Larry Matteson**, AAP, APRP, CCM, Vice President, Risk & Third-Party Programs

If your company transmits ACH credits or debits through your financial institution, you are considered an ACH Originator and the NACHA Operating Rules (ACH Rules) audit requirements ultimately impact you, even if you aren't required to conduct an audit of your own. Let's look at what the Rules say so you can be mindful of your responsibilities and help ensure the security and integrity of transactions being sent through the ACH Network. But, before we get started, let's define what it means to be an Originator.

If your company requests payment to be made for its electric bill through your electric supplier's website or call center, you are not considered an Originator in that transaction-the electric company is the Originator and your company is the Receiver of the debit. However, if this situation were reversed and you contacted your financial institution to send an ACH credit to the electric company to pay your bill, then you would be the Originator-the electric company would be the Receiver of the credit payment. Clear as mud? Basically, if your company utilizes your financial institution to send bill payments, payroll files, debits to collect payment from your clients or any other type of debit or credit entry through the ACH Network, you are an Originator.

If your company is an Originator, the ACH Rules (Subsection 2.2.2, f) require that your financial institution

enters into an ACH Origination Agreement with you that covers, among other items, the institution's right to audit your company's compliance with that agreement and the ACH Rules. This means that your financial institution can request documentation from your company or even request an onsite visit to verify you are compliant with the Rules.

While this may sound intimidating, playing by the Rules actually helps to protect your company from both monetary and reputational risk that can easily be avoided. It is in the best interest of you and your financial institution to do periodic checks to make sure that you are protecting yourself and your company's clients by keeping proper documentation, storing information securely and adhering to time restrictions and other requirements. If you are unsure about which rules apply to your company, you should reach out to your financial institution.

Some Originators may also be required to have their own separate ACH Rules Compliance Audit conducted, similar to the audit your financial institution is required to conduct (ACH Rules Subsection 1.2.2). However, this only applies to Originators that also qualify as a Third-Party Sender or Third Party Service Provider. A Third-Party Sender is an intermediary between an Originator and the financial institution sending the entries into the ACH Network. The financial institution doesn't have a relationship with the Originator in this situation, while the Third Party Sender does.

If your company sends ACH debits or credits to your financial institution on behalf of another company, you may be a Third Party Sender. For example, if your company handles payroll files for local businesses and sends Direct Deposit payments to your financial institution for ABC Grocery and Local Hardware, you are a Third-Party Sender. If this is true, your company is in the best position to ensure that your Originators' (ABC Grocery and Local Hardware) ACH transactions meet all the requirements of the Rules and any applicable regulations or other legal responsibilities. If you are a Third-Party Sender, you have all the responsibilities of an ODFI as far as origination is concerned, and therefore, must perform an annual audit. If you think you might be a Third-Party Sender, but you aren't sure, contact your financial institution.

A Third-Party Sender can conduct its own audit or contract another party. Whoever performs the audit should be familiar with the ACH Network and the ACH Rules and ensure the audit addresses the topics included in ACH Rules Supplement #1-2019. The results of the audit, including any inadequacies, should be documented in a formal report and reviewed by senior management of the Third-Party Sender.

see **AUDIT** on page 2



AUDIT continued from page 1

Recent ACH Rules changes allow covered parties to perform a risk-based audit instead of the prescribed audits performed in previous years, which is good news for Third-Party Senders. If a Third-Party Sender has little or no risk in a particular area, they do not need to expend a great deal of time and energy addressing that risk. For example, if a payroll processor does nothing but issue Direct Deposit credits, its Return risk is very low, so less time may be spent auditing Returns.

It should also be noted that NACHA (the ACH Network Administrator) randomly selects participating financial institutions, Third-Party Senders and Third-Party Service Providers to request proof that an annual ACH Rules Compliance Audit has been conducted. Not conducting an ACH Rules Compliance Audit annually is a violation of the Rules and participants could be subject to fines or other actions as described in

Appendix 10 of the Rules.

EPCOR's audit staff has conducted many Third-Party Sender audits and is ready to help your organization identify weaknesses and mitigate risk. If you do need to conduct an ACH Rules Compliance Audit, you can schedule one by calling 800.500.0100 or via email at mcmserve@epcor.org.



YOUR BUSINESS — IS — OUR BUSINESS

Useful products, helpful people and easy online solutions make Business Banking better.

 **Platte Valley Bank**
A Platte Valley Company

 **Mountain Valley Bank**

NEW WIRE FRAUD SCAM SENDS PAYCHECK 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

[see SCAM on page 3](#)

SCAM continued from page 2

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 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

SAME DAY ACH HELPS PAYROLL AT COMPANIES BIG AND SMALL

"Same Day ACH gives payroll professionals a number of options for meeting their needs," said Michael Herd, Senior Vice President of the ACH Network administration at NACHA, which administers the ACH Network. "When they have missed deadlines or emergencies, they can use Same Day ACH to make payments faster."

Since debuting in September 2016, Same Day ACH has taken off. The fourth quarter of 2018 saw more than 51 million same-day debits and credits worth \$44.6 billion. It was the first quarter in which the number of Same Day ACH payments passed the 50 million mark.

Plus, enhancements are on the way. The current \$25,000-per-transaction limit for Same Day ACH climbs to \$100,000 in March 2020. A third processing window for same-day transactions is also coming, but has been

postponed for six months and cannot go into effect until the Federal Reserve Board of Governors (Fed Board) approves the initiative.

"We're making it even better because we know payroll professionals need to have later hours for Same Day ACH," Herd said. "They'll have more time to get their payrolls processed."

Same Day ACH is not just for big firms in glass towers. In fact, the smallest of companies are some of its biggest beneficiaries.

Small Business, Big Worries

Wave Financial caters to what Les Whiting termed "the small end of small business"

"We build a number of different financial services specifically tailored for what we call 'micro-businesses' These are true small businesses," said Whiting, Senior Vice President, Financial Services, at Toronto-based Wave Financial. "They're designers, they're contractors. They wear all the hats."

While small businesses are often thought of as having ten employees or fewer, Whiting said "the vast majority" of their customers "have one, two or three employees." And this can lead to a big problem.

"Arguably, the smaller you are, you typically have greater challenges with cash flow," Whiting said. "The faster you can get money to where you need it to be, the better off you are."

That's where Same Day ACH factors in. "With Same Day ACH, it all comes down

see PAYROLL on page 4



BUSINESS BANKING

HOW YOU WANT
WHEN YOU WANT
WHERE YOU WANT

www.pvbank.com • online anytime • www.bankmvp.com

PAYROLL continued from page 3



to speed," Whiting said. "If I can run a payroll today to pay my employees tomorrow, that's much better than if I have to run it three or four days before."

While it might not be as much of a factor for salaried employees, Whiting noted, "as soon as you start to get into hourly workers, seasonal workers, compressing those windows is super crucial. And, frankly, the longer they can hold onto cash in their business, the more it's going to help them with cash flow."

Wave Financial recently launched a product enabling customers to take advances on invoices they have already generated but haven't collected.

"We've made it very simple for them in three or four clicks to be able to get access to capital," Whiting said.

And when it's in their customers' accounts later that day?

"That's a pretty magical experience that without Same Day ACH, in some situations, we would be looking at getting funds into accounts in two days," he said. "That makes a world of difference in the experience that our customers will have."

Beyond the Payroll

For businesses of all sizes, there's more work to be done than just on payday. This includes reimbursing staff for travel and other expenses, which

Herd called "another great way to use Same Day ACH" - getting money to folks faster. "Employees will love if many payroll departments also handle sending tax withholdings to federal, state and local government agencies, as well as remitting deductions for items such as health and life insurance.

"Same Day ACH can be a way to make sure you don't miss a deadline, or to get the money there faster if you do," Herd said.

But just as you wouldn't wait to come down with the flu before getting a flu shot, Herd said the time to look into Same Day ACH is now. "You might never know you need Same Day ACH until you wake up in the morning with a problem," he said. "If you haven't set it up and tested it in advance, you might not have access to it. So, the time to prepare is before you need it."

The first question to ask is whether your bank or service provider offers the service.

"If your bank hasn't talked to you about Same Day ACH, don't wait until you have an emergency," he said.

Then again, if you're paying employees with paper checks, Herd sees another place to start.

"For those companies that still hand out paychecks, they need to use any kind of direct deposit," he said. "It's the way more than 90% of Americans get paid. Any direct deposit is better than no direct deposit."



Source: NACHA for American Payroll Associations' PAYTECH magazine

FIVE TIPS FOR IMPLEMENTING SANCTIONS SCREENING

OFAC screening is part of doing business for U.S. companies who transact with international customers. The process ensures compliance with U.S. law and protects the interests of the company by avoiding fines and unintentional contact with blocked parties.

Despite its importance, there are few guidebooks on how to do comprehensive and efficient OFAC screening. Companies are largely left to themselves, to both search publicly available information and interpret how the law applies to them. Thankfully, there are some easy-to-implement strategies that improve OFAC screening procedures to reduce the risk to companies.

Tip #1: Know OFAC Compliance Involves Many Different Laws

Although the Know Your Customer guidelines are a relatively recent initiative, the U.S. government has put restrictions on trade and economic activity since the 1800s. OFAC compliance is in fact following U.S. Treasury laws that apply to many different countries, individuals and companies in order to support U.S. interests. OFAC barriers are in place to stop a range of activities, including terrorism, drug trafficking, money laundering and more. Because of the scope of these rules, it is wise not to assume that a new customer will not fall on the specially designated nationals (SDN) list and to always perform due diligence.

Tip #2: Get Informed of Updates

The SDN list is not a static, unchanging document. It is updated on a regular basis, so your new or existing customer may fall under its gambit without warning. It is a good idea to stay abreast of the latest version of the SDN so you can take appropriate action in case you are barred from doing business with a certain party. You can sign up to receive email updates from the U.S. Treasury and receive alerts when the list is revised.

Tip #3: Use an Automated OFAC Screening System

Many companies rely on a manual system to check for OFAC compliance. Unfortunately, this fails many companies who do not have the capacity to thoroughly ensure they are not doing business with blocked parties. Companies that operate with integrity and value transparency may find they inadvertently run afoul of U.S. Treasury law. To fully protect your company, it is best to use an automated system. Fortunately, you can adopt one that works seamlessly with your existing procedures.

Tip #4: Beware of False Positives

One drawback of manual, and some automatic, OFAC sanctions screening systems is the potential for false positives. Many of your valued customers could have a name similar to, or the same as, a party on the SDN list. In order to prevent a challenging situation where you refuse to do business with a legitimate customer, consider a system with a computerized algorithm that identifies false positives based on such misleading cues as initials and acronyms.

Tip #5: Run a Self-Audit

As a business owner who transacts with international parties, OFAC screening is your obligation. You may have to demonstrate your compliance. Keep accurate and detailed records of how your screening process works to fulfill your due diligence. Details about who you screened, when you screened them and the results of your screening should be kept on file.

OFAC sanction screening is required by U.S. law. Doing so efficiently and accurately helps your business by allowing you to grow your customer base without worry. By automating your screening practices and staying up-to-date with changes to the law, you can ensure compliance without unreasonable constraints on your time.

Source: Lyons Commercial Data



THREE STRATEGIES FOR SMALL BUSINESSES TO FIGHT FRAUD

Despite advances in technology, fraud continues to be a major pain point in our modern society. Throughout the years, there have been many examples of the devastating consequences of fraud and how it affects small businesses. According to a recent study from the multinational professional service company, PricewaterhouseCoopers, nearly 50% of businesses around the world have been a victim of different types of fraud or economic crime.

There are many strategies that scammers use to separate you from your hard-earned savings. Aside from common frauds like identity theft, wire scams and cloned debit cards, check and Automated Clearing House fraud have been on the rise in the last few years. According to the latest report from the Federal Reserve, the combined value of ACH and check fraud rose from \$6.10 billion in 2012 to \$8.34 billion in 2015.

Small businesses are a prime target

Small businesses can be especially vulnerable to fraud. The Association of Certified Fraud Examiners reports that 30% of fraud cases occur in small businesses (those with fewer than 100 employees) and 60% of small-business fraud victims don't recover any of their losses. Fortunately, these risks can be managed.

Following are three fraud prevention strategies that small businesses should consider implementing:

1. General strategies

- Get a locking mailbox and sign up for accounts with all mail service providers. One study from the U.S. Secret Service showed that the top two methods of non-technological identity theft were mail theft and rerouting of mail.

see FRAUD on page 6



FRAUD continued from page 5

Through creating a secure account, you will make it harder for someone to impersonate you and reroute your mail.

- Sign up for electronic delivery of financial statements and bills. Unsecured letters from your financial institution or vendors provide information thieves can use to compromise your accounts.
- Obtain an identity theft protection service. This service alerts you when your personal information is being used in ways that generally don't show up on your credit report. These services can help you act immediately if your personal information is ever compromised.

2. Work with employees to help prevent fraud

- Create strong internal procedures that are easy to understand and implement. Although a suspected case of internal fraud may require confidentiality, a case of external fraud can be more straightforward. For example, if a cashier suspects a customer is using a stolen credit card, they should immediately notify a manager.
- Warn employees about types of



fraud to watch out for, which commonly include:

- New account fraud: Setting up accounts based on stolen identity or personal information.
- Credit card fraud: Using credit cards without authorization.
- Check fraud: Using checks without authorization or utilizing fake checks.
- Identity theft: Using another individual's personal or financial information without his or her consent.
- Separate duties with checks and balances. Having more than one employee handle payroll, make deposits and reconcile bank statements provides oversight and acts as a fraud deterrent.

3. Implement automated fraud prevention technology

- Finally, your business can add another layer of protection through a sophisticated, automated system like Positive Pay from your financial institution. Positive Pay helps businesses identify and report fraudulent and unauthorized payments by verifying transactions before completing payment.
- Positive Pay uses a secure conduit to send the bank a daily list of authorized checks. After a transaction is submitted to the bank for payment, the system automatically compares it against the list. If an item is on record as having issues or has been altered, the system detects the mismatch and halts payment.

Banks Are a Valuable Ally Against Fraud

Despite the prevalence of fraud, you can help reduce your risk by implementing proven strategies and working with a financial institution that can support you. Financial institutions have experience with fraud management and want to help you manage risk in your business.

Source: East Idaho Business Journal

THANK YOU

for choosing us to be your partners in banking.



Platte Valley Bank
A Platte Valley Company



Mountain Valley Bank