FIRSTAR BANK. epcor

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE THIS ISSUE

No News Is Good News with ACH... But What If There's Bad News? ..... pg. 1
Pumpkin Spice Up Your Payments Education for 2023! ..... pg. 1
6 Reasons Why Businesses Need to Upgrade Their Payment Systems ..... pg. 3
Fighting the Cybersecurity Fraudsters Going Bump in the Night ..... pg. 4
Business Fraud Prevention Tool ..... pg. 4
What Kinds of BNPL Options Are Available to Merchants? ..... pg. 5
How Fast is Fast Enough? ..... pg. 6
Have You Audited Your WEB Debit Security Standards Lately? ..... pg. 7
5 Reasons Why It's Crazy for Businesses to Write Checks ..... pg. 8
What Do Third-Party Senders Need to Know About OFAC? ..... pg. 9

No News Is Good News with ACH... But What If There's Bad News?

by Shelly Sipple, AAP, APRP, NCP, Senior Director, Certifications & Continuing Education, EPCOR

The COVID-19 pandemic forced businesses and consumers alike to drastically change how they make payments. Contactless payment methods, like ACH, have grown significantly over the past several years. In fact, ACH payment processing in 2022 has accelerated and is outpacing activity from a year ago. Perhaps your business has also increased its usage of ACH payments in recent years.

Initiating ACH payments is simple - sign up for ACH origination services with your financial institution; obtain authorizations from employees, consumers or businesses to credit or debit their accounts; create your file of ACH entries, then upload it to your financial institution for processing into the ACH Network. From there, it's "automagically" posted to the recipient's account. But is that always the case?

The ACH Network operates on a "no news is good news" principle. That is, receiving financial institutions may post payments based solely on the account number contained within the entry. Therefore, your company will not receive any confirmation regarding payment processing and may assume all went as expected. However, you will be alerted if there is bad news; that is, when there are issues processing the payment. In these situations, receiving financial institutions may send a Notification of Change (NOC) related to the payment or return the entry.

So, how do you respond to this bad news? It depends on whether an NOC is received, or the payment has been returned.

Receipt of a Notification of Change (NOC)

If the receiving institution can determine whose account the payment should be posted to, they will process it and send an NOC to your financial institution identifying erroneous information (e.g., wrong account number) and provide corrected data. Your financial institution will communicate this to you within two business days of receipt (e.g., phone call, secure email). Once notified, you

see NEWS on page 2

Pumpkin Spice Up Your Payments Education for 2023!

by Madison Howard, Manager, Member Communications, EPCOR

It's that time of year again—the weather is changing, the holidays are approaching and the year is quickly coming to an end. This is the time of year when many organizations begin looking ahead to the new year, make budget plans and set new goals. Plus, with many organizations seeing vital staff members approaching retirement, it's imperitive to educate less tenured staff to take their place.

see SPICE on page 2

NEWS continued from page 1

must make the specified change(s) related to a recurring payment within six business days of receipt or prior to initiating another entry, whichever is later. You may choose to confirm corrected data with the payment recipient first; however, this does not change the timeframe in which to make the update.

Receipt of a Return Entry

If the receiving institution returns the payment, they will identify the reason for the return. Information related to returned payments will also be communicated to you by your financial institution as outlined in your origination agreement. There are several valid return reasons, and appropriate action should be taken depending on the reason. Let's look at the most common return reasons along with your next steps.

- Administrative returns are entries that cannot be posted due to an invalid account number, account closure or the inability to locate the account. You should contact the recipient to obtain new account information before reinitiating the payment.
- Debit entries may be returned for insufficient funds. You may attempt to collect by reinitiating the payment up to two times. Consider timing payments on a payday to increase your chances of collecting. You may also ask your financial institution if they offer a service whereby reinitiating the payment is done automatically on your behalf.
- Recipients may request a debit payment be stopped by their financial institution. For these returned payments, contact the recipient to determine the reason for the stopped payment and only reprocess if authorized to do so.
- Debit entries may be disputed by the recipient because the payment was not processed according to the terms of the authorization (e.g., wrong dollar amount, debit date earlier than agreed upon). You should review the authorization and initiate a new entry to correct the underlying error.
- A debit payment may also be returned because the recipient claims it was not authorized. If you did not obtain authorization before sending the debit, then you must do so prior to initiating a new entry. However, if authorization was in place, you must resolve the issue directly with the recipient.

So, the bad news isn't all that bad if you know how to handle it! Reach out to your financial institution if you have any questions related to ACH payment processing. They are, after all, your payments experts!

You can also visit EPCOR's Corporate User Webpage at epcor.org/corporateuser for more helpful resources and information.

SPICE continued from page 1

The best way to be successful is to have the right tools and education. So, **grab your lattes and let's look at some ways to pumpkin SPICE up your payments education for your staff and clients!**

ACH Rules

What better way to ensure compliance with the *ACH Rules* than to provide access to the *ACH Rules*? Consider reaching out to your financial institution if you need a copy, or additional copies.

NEW *ACH Quick Reference Guide for Corporate Users*

This year EPCOR rolled out a brand-new resource called the *ACH Quick Reference Guide for Corporate Users*. This Guide is a quick summary of all the *Rules* ACH Originators need to know and covers general rules, ODFI/Originator requirements, prerequisites and warranties, as well as a review of all the processes such as returns, NOCs, prenotes and more!

Did You Know... Informational Videos

These quick and free animated videos explain payments topics in just a few short minutes! The fun format and easy-to-understand language make these videos perfect for passing along important information to staff and clients. Recent topics include cryptocurrency 101, cryptocurrency scams, preparing for the digital payments shift, ACH file holders and more. These videos are available on EPCOR's website, LinkedIn and YouTube channel.

Payments Insider

Payments Insider (which you're reading now) is a semi-annual e-newsletter designed to inform businesses of all sizes of recent payment systems developments. This newsletter is distributed in the months of April and October. Our April edition also includes a special *ACH Rules Update for Corporate Originators*. The latest copy of this newsletter is always available on the Corporate User Webpage.

Corporate User Webpage

This webpage contains end-user resources, information on upcoming *ACH Rules* changes and much more. And, we're constantly adding new resources and taking suggestions from page visitors. Visit the webpage at epcor.org/corporateuser.

If you have any questions or aren't sure what resource is right for you or your organization, reach out to your financial institution.

6 Reasons Why Businesses Need to Upgrade Their Payment Systems

by Allen Brown, The Southern Maryland Chronicle

The following article originally appeared on April 17, 2022, on SouthernMarylandChronicle.com.

Have you been using the same outdated payment system for years? It's obvious that payment systems are necessary for doing business. However, many companies are still using outdated payment systems that are no longer effective. Outdated payment systems are often unreliable and can cause many problems for businesses. This is because they're not able to keep up with the latest technology, and they cannot process payments as quickly or efficiently as newer systems. There are several reasons why businesses need to upgrade their payment systems. Here are just a few.

Increased Security

One of the most important reasons to upgrade your payment system is increased security. Outdated payment systems are often not as secure as newer ones. This is because they cannot keep up with the latest security measures. Some have been neglected by their creators and haven't been updated in years. This leaves them vulnerable to attacks by hackers who are always looking for new ways to steal information.

Newer payment systems use state-of-the-art security features to help protect your business from fraud and other security threats. It is essential to look for a payment system that offers modern features such as fraud detection, data encryption and authentication. For instance, these Top 10 POS software solutions provide advanced security features to help keep your business safe. These features can go a long way in protecting your business from security threats.

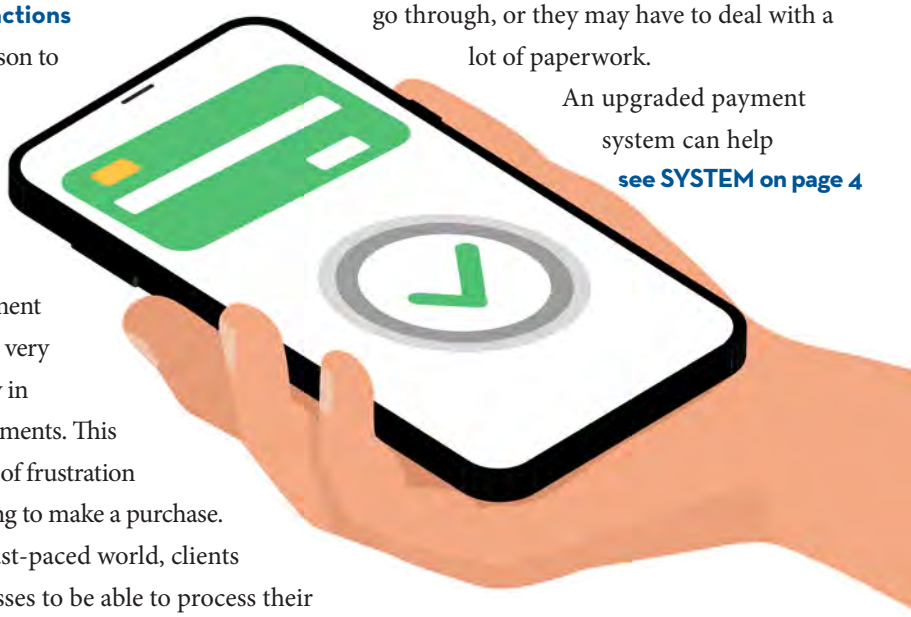
Faster Transactions

Another reason to upgrade your payment system is for faster transactions. Outdated payment systems can be very slow, especially in processing payments. This can cause a lot of frustration for clients trying to make a purchase.

In today's fast-paced world, clients expect businesses to be able to process their payments quickly and efficiently. They don't want to wait in line for a long time or fill out a lot of paperwork. Newer payment systems are designed to be fast and efficient. They can process payments quickly, so clients can get what they need and move on with their day.

Improved Client Experience

Everyone nowadays is looking for a good client experience. They want to do business with companies that offer a positive and convenient experience. If your payment system is outdated, it could negatively impact the experience. This is because clients may have to wait a long time for their payments to go through, or they may have to deal with a lot of paperwork.



An upgraded payment system can help

see SYSTEM on page 4

SYSTEM continued from page 3

improve the experience. This is because it can make transactions faster and easier. Clients will appreciate being able to get what they need quickly and without any hassle. In turn, this can help increase client satisfaction and loyalty.

Better Integration

If you're using an outdated payment system, it may not be compatible with other business systems. This can cause many problems and make it challenging to get the information you need.

Newer payment systems are designed to be compatible with other systems. This means that you'll be able to integrate them into your existing system easily. This can save you a lot of time and money in the long run. For instance, you won't have to hire someone to manually input data into your system.

Lower Costs

Many businesses think that upgrading their payment system will be expensive. However, this is not always the case. It can save you money in the long run. This is because newer payment systems are often more efficient than older ones. They're able to process payments quickly and accurately. This can save you a lot of time and money that you would otherwise waste on manual processing.

In addition, newer payment systems often come with lower transaction fees. This can save you a lot of money, especially if your business processes many payments. You will be paying less than you would with an older system. This reduces the overall business costs and makes your business enjoy a higher ROI.

Increased Efficiency

If your business is still using an older payment system, likely, it's not very efficient. This can cause many problems, such as long lines and slow transactions. Inefficiencies can cost your business a lot of money in the long run. They can also cause a lot of frustration for clients who have to deal with them.

A newer payment system can help increase your business's efficiency. This is because it can make transactions faster and easier. Clients will appreciate being able to get what they need quickly and without any hassle. In turn, this can help increase overall satisfaction and loyalty.

There are many reasons why businesses need to upgrade their payment systems. Outdated systems can be slow, insecure and expensive. Newer payment systems offer several benefits that can help improve your business. These include faster transactions, improved client experience, better integration and lower costs. If you're still using an older payment system, it's time to upgrade to a newer one. Your business will be better off in the long run.

Source: The Southern Maryland Chronicle

Fighting the Cybersecurity Fraudsters Going Bump in the Night

by Madison Howard, Manager, Member Communications, EPCOR

Happy spooky season! If you're like me, thoughts of the fall season, comfy sweaters and scary movies are so exciting. But Freddy Krueger and the Sanderson Sisters aren't the only spooky beings to think about lurking in the shadows.

Fraudsters are always on the prowl, searching for ways to take advantage of the cybersecurity weaknesses of your organization. These fraudsters are truly monsters—which is why it makes sense that Cybersecurity Awareness Month is held in October, the epitome of the spooky season, each year.

While there's surely always something strange lurking in the cybersecurity shadows, you yourself can be a ghost (fraud) buster by implementing these cybersecurity tips and sharing them forward.

- **Ditch your recycled passwords.** With so many services and accounts accessible online that contain personal information, a strong password is often the only thing standing between your data and a fraudster. And, with data breaches being an unfortunately common event, it is vital to utilize new passwords and change them regularly. A strong password should contain a minimum of twelve characters (though more is better) and should not be easily guessable.
- **Use two-factor or multi-factor authentication.** While the extra step(s)

see BUMP on page 5

Business Fraud Prevention Tool

Small businesses assume scammers will only target the big corporates, but fraud losses have proven that scammers will target any size business. Businesses of all sizes need to stay vigilant when it comes to fraud. Really, it is the smaller businesses that need to be more alert as 1/3 of these businesses experience at least one fraud attempt annually! Putting effective fraud prevention measures in place and proper employee education is crucial for any size business to combat fraud. Education and vigilance are where fraud prevention begins.

Visit epcor.org/corporateuser for helpful free resources, including our NEW one-page, easily-digestible business fraud prevention document which provides ways to prevent payments fraud in your business.

BUMP continued from page 4

may seem annoying, having an extra layer of protection is vital. This way, if you do fall victim to a phishing attack or data breach, you have an extra roadblock in the way of a fraudster attempting to make use of your compromised credentials.

- **Keep your software up to date.** Software vendors often update their products and issue patches when vulnerabilities are discovered. Sometimes these vulnerabilities are severe, with some cases being as alarming as enabling malicious third parties to completely control someone's computer without their knowledge. It's very common for fraudsters to scan the Internet for machines that are utilizing older versions of software that contain exploitable vulnerabilities. Keep an eye out for available updates and enable automatic software updates if you are able.
- **Use antivirus software.** There are many programs available to protect your computer from malicious code infecting your computer. This includes malware that's arrived via infected email attachments, malicious links in email messages and so-called "drive-by downloads" – automatic downloads initiated by compromised websites. Consider installing antivirus software on your electronic devices.
- **Slow down!** We're all busy and trying to get things marked off our to-do list as fast as possible. But slowing down before you open an email, or thinking twice before you click on a link, could be the difference between a close call and a massive data breach.

Staying up to date on the latest happenings in the fraud space can help you stop fraud at the door.

Source: BTB Security, Virtu

What Kinds of BNPL Options Are Available to Merchants?

by Srii Srinivasan, Founder & CEO, Chargeback Gurus

The following excerpt originally appeared on April 6, 2022, via an article titled Buy Now, Pay Later: What Merchants Need to Watch Out For on ChargebackGurus.com.

Merchants looking to adopt a buy now, pay later (BNPL) solution from a third-party provider should be aware of the two main types of plans they might encounter: merchant transaction fee loans and shopper interest loans.

With merchant transaction fee loans, a loan is provided to the consumer at the point of sale. No interest is charged to the consumer if they make their payments on time. Instead, the merchant is charged a transaction fee.

Merchants typically pay the BNPL provider between 2% and 8% of the purchase amount, and in some cases a small per-transaction fee. Providers typically don't disclose their pricing upfront, so merchants interested in pursuing a relationship with a BNPL provider should expect to go through a process of registering an account and submitting business information to receive a quote.

While the fees a merchant pays to buy now pay later services might seem steep, these services can bring in consumers and encourage purchases that might not otherwise be made, especially when the offered installment plans don't charge interest.

BNPL services can be particularly valuable for merchants who sell goods or services that come with a hefty price tag, as the option to pay nothing up front can help hold onto consumers who might otherwise be driven away by sticker shock. Different BNPL providers have claimed increases in average order value ranging from 40% to 85% for merchants who partner with them.

With shopper interest loans, no fees are charged to the merchant, but the consumer pays interest as part of their installment plan. This makes BNPL a more attractive option for merchants, but a less attractive option for their clients, reducing some of the benefits of offering it.

Offering BNPL options can be particularly valuable during the holiday season when consumers increase their spending, buying gifts for friends and loved ones. Many consumers are highly conscious of the extra strain put on their accounts during the holidays, and the option to reduce the immediate pressure by spreading the payments out over several months can be very attractive.

To learn more about BNPL, including fraud trends, risks, how this service affects chargebacks and more, click here to read the full article.

Source: ChargebackGurus.com

How Fast is Fast Enough?

by Ashton Vandivert, Manager, Emerging Payments, EPCOR

Is "fast, faster, fastest" really equivalent to "good, better, best?" That's the industry buzz, anyway… but how fast is truly fast enough? And once speed is determined, what are the pros and cons?

First, let's dig into the big debate: fast vs. faster vs. fastest, or instant. What do these categories mean and how are they different?

When it comes to payments that are "fast," think of the more traditional payment methods such as cards, wires and ACH. One could also argue that checks could potentially fall into this category after the onset of Check 21. However, as the financial ecosystem has evolved, the speed of these options has been questioned. Are these methods fast enough to meet demands in the current landscape?

Enter "faster" payments. Going beyond the traditional payment methods listed above, this classification of "faster" is a hot debate. The Federal Reserve defines faster payments as electronic payment services that provide funds to the payee within seconds or up to a few hours of initiation by the payer. This includes instant payment services like RTP® and FedNow℠, Same Day ACH, push-to-card and digital wallet payment apps.

With all the different options available, it can be hard to tell which payment system to choose and why. Let's look at Same Day ACH, RTP® and FedNow℠ side by side, along with some pros and cons of each.

Pros	Cons
Cash flow management	Lacking full participation
Improved efficiency	Initial investment
Strategic opportunity	Irrevocable

Network Characteristics			
Characteristic	**Same Day ACH**	**RTP**	**FedNow℠ Service**
Originators/Senders & Receivers	Businesses & consumers	Businesses & consumers	Businesses & consumers
Operating Hours	3 processing windows Monday – Friday (excludes Federal holidays)	24/7/365	24/7/365
Transaction Types	Debits & Credits	Credits only	Credits only
Dollar Limit per Transaction	$1,000,000	$1,000,000	$500,000
FI Access to Network	Direct connection or via Third-Party Service Provider (TPSP)	Direct connection or via TPSP	Direct connection or via TPSP
Settlement	Net settlement 3 times daily	Real-time gross settlement	Real-time gross settlement

Faster payment solutions provide multiple benefits. The list is much longer than this, but here is a reflection over a few pros including better cash flow, improved efficiency and the fact that it's a strategic opportunity.

Due to the speed and transparency of faster payments, there are advantages in the overall cash flow management process. Same Day ACH provides same-day funds availability within hours, and RTP® and FedNow℠ will provide it within seconds due to their always-on 24x7x365 functionality. This can help to assist in liquidity and asset management needs for many small businesses, corporations and financial institutions.

Faster payments are also automated using straight-through processing, or STP. This eliminates the need for slow, manual processing and in turn, can lead to streamlined efficiencies and increased cost savings.

see FASTER on page 7

FASTER continued from page 6

Most importantly, faster payments are a future-facing solution. Designed with evolving needs and demands in mind, Same Day ACH, RTP® and FedNow℠ have the potential to provide a competitive edge. It is because of this potential that these payment options are strategic opportunities to be considered.

As with any other payment system, there are a few aspects of faster payments that could be perceived as disadvantages.

The first disadvantage of faster payment systems RTP® and FedNow℠ is that they are not yet a universal solution offered by all financial institutions. Currently, the RTP® Network reaches only 61% of U.S. demand deposit accounts and FedNow℠ is not launching until mid-2023. However, this will continue to improve as adoption rates increase.

The second disadvantage of faster payments is the upfront investment cost. New business ventures often come with a high price tag during the initial phases of launch, so faster payment implementation calls for early budgeting.

The final "disadvantage," depending on how you look at it, is the irrevocable nature of payments that are sent through the RTP® Network or FedNow℠ Service. Because of this payment finality, there is little to no room for erroneous entries. Instant payments enable immediate, final settlement to the payee, which is the key element of instant payments.

When it comes time to evaluate overall strategic opportunities, faster payments are without a doubt something to be considered. By comparing the options and weighing the pros and cons, you will have much of what you need in order to make a well-rounded decision. Reach out to your financial institution to learn more about your available options.

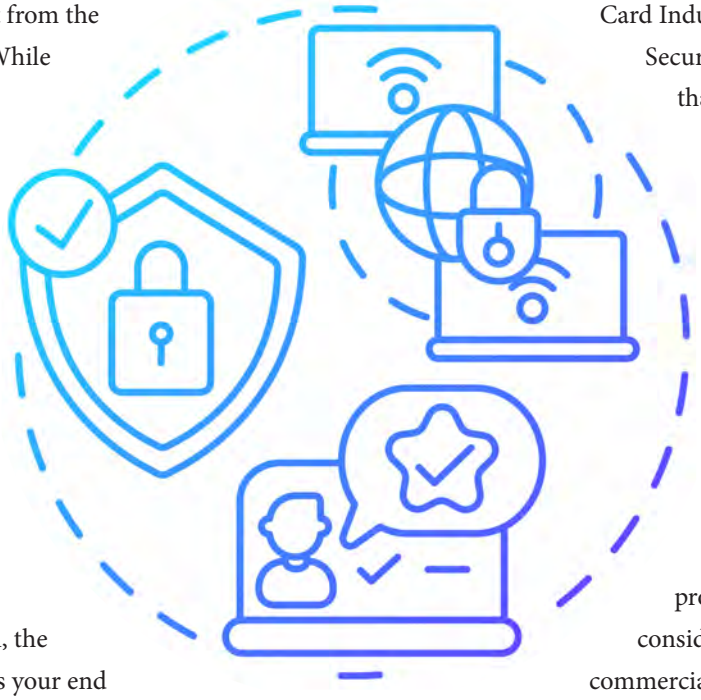
Have You Audited Your WEB Debit Security Standards Lately?

by Jennifer Kline, AAP, APRP, NCP, Director, Audit Services

As far as the *ACH Rules* go, compliance obligations are shouldered by the financial institutions that participate in the ACH Network. And, if your company sends and receives ACH transactions, your part of maintaining those compliance obligations are relayed via your agreement with your financial institution. However, there are a few *Rules* for companies (aka Originators) who originate ACH WEB Debit transactions that are specifically called out and Originators are held responsible for under the *ACH Rules*.

In particular, Originators, Third-Party Service Providers (TPSPs) and Third-Party Senders (TPSs) that offer WEB origination services are required to conduct or have conducted an annual security audit of WEB Debit Entries under *Subsection 2.5.17.3* of the *ACH Rules*.

As the EPCOR advisory team conducts audits for financial institutions and third-parties, we find this *Rule* often boils down to a couple key questions related to the WEB Debit security audit. One, what is an acceptable and commercially reasonable security audit report for the origination of WEB Debit Entries? And two, should the ODFI or TPS obtain proof of the completion of the annual security audit from the Originator? While it may sound like we are starting backwards with the final outcome of the audit (the audit report) it is actually a great place to start. After all, the audit report is your end goal and proof that you have met this *Rule* requirement. And, there may be a shortcut to meeting the requirement *if* your company accepts online card payments.



If your company accepts card payments online, you may have already conducted a PCI-DSS audit of compliance that shows your organization's data security standards to protect cardholder account data. PCI-DSS is the Payment Card Industry Data Security Standards that have been in use for a long time. When these same standards are applied in the same manner to ACH transactions, ACH security processes are considered to be a commercially reasonable method for ACH data security. So, if you are an ACH Originator that sends WEB Debit Entries and processes card payments online, and the same security

see SECURITY on page 8

SECURITY continued from page 7

standards apply to both ACH and card transactions and processes, your business may already have online data security standards in place that meet the Rule requirement. In this case, your company can rely on a PCI-DSS audit compliance report *if* the review includes ACH financial information and systems and verifies the ACH financial information, also known as 'Protected Information' as stated in *Subsection 8.80*.

If your company does not accept card payments, then you cannot assume you are meeting the data security standards as required in *Subsection 2.5.17.3* and must conduct a security audit. Again, under the *ACH Rules*, all Originators of WEB Debit Entries are required to conduct, or have conducted on its behalf, annual audits to ensure that the financial information it obtains from the Receiver is protected by security practices and procedures. As you conduct your audit, you must ensure that those practices and procedures meet the requirements of *Subsection 2.5.17.3*, which include at a minimum, adequate levels of:

a. Physical security to protect against theft, tampering or damage;
b. Personnel and access controls to protect against unauthorized access and use; and
c. Network security to ensure secure capture, storage and distribution.

Additionally, requirements for WEB Debit Entries also include:

- the use of fraudulent detection systems that use a "commercially reasonable fraudulent transaction detection system" which includes "account validation" to screen WEB Debit Entries for fraud. This requirement applies to the first use of an account number and subsequent changes to the account number;
- authentication methods to verify a Receiver's identity; and
- verification of Routing Numbers used in the transaction.

For more information on your annual audit of the WEB Debit Entries look to the Guidelines section of the *ACH Rules*, *Chapter 48 – Internet Initiated/Mobile Entries (WEB), Risk Management*, which offers an example scope for an independent audit. This section includes additional context, details and examples around the requirements of *Subsection 2.5.17.3* and is quite helpful. Ultimately, the audit should utilize a commercially reasonable, generally accepted security compliance program for the Originator's annual WEB Debit security audit. Additional types of security audits of WEB Debit Entries could include, but are not limited to, SSAE-16, SOC 1 or SOC 2 audits.

Once your review is completed you should keep a copy of your report on file so that you can verify your compliance with the Rule as requested by your financial institution or Nacha upon request.

5 Reasons Why It's Crazy for Businesses to Write Checks

by Rob Unger, Senior Director, Product Management & Strategic Initiatives, Nacha

The following article originally appeared on March 21, 2021 on Nacha.org.

Remember the "Jetsons" cartoon when George Jetson took his dog Astro out for a walk on the space treadmill? Yikes! He got sucked up into a never-ending, out-of-control spin cycle, screaming, "Jane, stop this crazy thing!"

Similarly, many businesses are stuck on the check-writing treadmill, and the spin cycle is cranking out an unfathomable 20 million commercial checks each day. Businesses, stop this crazy check thing!

Here are five reasons why it's crazy for businesses to write checks:

1. Fraudsters love checks more than any other payment type. There is a lot of information printed on checks, and businesses write a lot of checks, so checks are an easy target for forgery and theft. Checks continue to be the primary target of payment fraud, according to the Association of Financial Professionals, citing that 81% of respondents to their latest Payments Fraud survey reported being targeted—or experiencing—actual check fraud attempts. (*Spoiler alert—ACH payments have the lowest fraud rate.*)
2. If you experience check fraud or make a mistake (like pay an incorrect payee or amount) on a check payment, say "bye-bye" to your funds if that check gets cashed; you have no administrative recourse to reclaim funds. (*Spoiler alert—you have protections against unauthorized ACH withdraws to your bank account and there are opportunities to get your money back in the event you make an incorrect ACH payment.*)
3. Checks cost your company more than any other payment type by far but check printers never send a "thank you" note for funding them and paying more than needed. (*Spoiler alert—ACH is a much lower payment cost option.*)

see CHECKS on page 9

CHECKS continued from page 8

4. Have you ever had to make a rush or an emergency payment? Delivering that check by expedited service or courier costs a good chunk of change, and expedited delivery services don't send "thank you" notes either! (*Spoiler alert—you can make a rush payment today using Same Day ACH at a fraction of the cost of expedited delivery services.*)
5. Managing cash flow is a critical function, but in today's low interest environment, and with the option for check receivers to image checks for quicker settlement, there is really no float benefit, like in the good old days. And wouldn't you like to know precisely when that check will clear to help manage your cash position? (*Spoiler alert—ACH payments give better insight into cash flow, providing precise payment settlement times.*)
6. Bonus reason why it's crazy for businesses to write checks: in the wake of COVID-19 and changes to protocols, many businesses are working remotely and issuing checks has been even more difficult. In Nacha's 2020 Industry Survey, businesses resorted to creative check issuing, like "drive-by" check approvals to maintain proper distancing. Another business had to shut down the office after a technician serviced a malfunctioning check printer because the tech later discovered he had COVID-19. (*Spoiler alert—businesses with established ACH payment programs have fared much better during the pandemic.*)

As the hints suggest, ACH payments provide clear benefits compared to check payments. If your company currently does not send ACH payments to vendors/suppliers, you can contact your financial institution for recommendations on how to get started with sending ACH payments.

Or you can allow your trusted vendor/supplier to pull the funds from your account, where you don't have to do anything except provide the company routing and account number. Consumers are very familiar with the various names' companies call this option (e.g., Direct Payment, Auto Pay, Simple Pay, Easy Pay, Sure Pay, Recurring Debit, etc.).

Now, I hear from a lot of B2B accounts payable types, who say that's fine for consumers, but their companies are uncomfortable with allowing the company bank accounts to be debited for invoice payments. But that's what a check does! And checks are crazy (see above).

ACH Resources

Nacha has numerous resources to help businesses better understand the benefits and best practices for ACH payments:

- ACH in the Community – Learn the benefits of ACH for businesses, nonprofits and religious organizations.
- Quick Start Guide – A tool for your business to learn how to pay or get paid electronically using ACH.

If you're interested in ACH, work with your financial institution to explore your available options.

Source: Nacha

What Do Third-Party Senders Need to Know About OFAC?

by Matthew T. Wade, AAP, CPA, Senior Manager, Advisory Services

As a Third-Party Sender (TPS) you may be asking, "Why do I need to be concerned about OFAC?" Or perhaps you might ask, "What does OFAC stand for anyway?" Assuming you are familiar with the acronym, you may ask, "OFAC only pertains to financial institutions, right?" Let's see if we can answer those questions for you and any others you may have.

OFAC is the Office of Foreign Assets Control and is a division of the U.S. Department of the Treasury. OFAC administers and enforces economic and trade sanctions against targeted foreign countries and regimes, and against terrorists and other individuals based on U.S. foreign policy and national security concerns. Among other things, OFAC imposes controls on financial transactions and assets of such designated parties under U.S. jurisdiction. While many OFAC policies and efforts focus on the financial banking industry, its policies and powers are not limited to financial institutions only. In fact, ALL U.S. citizens, companies located in the U.S., overseas branches of U.S. companies and, in some cases, overseas subsidiaries of U.S. companies fall under OFAC jurisdiction.

If you revisit the ACH Origination Agreement you have with your Originating Depository Financial Institution (ODFI),

see OFAC on page 10

OFAC continued from page 9

you may not find any explicit reference to OFAC. However, there is a good chance that somewhere in that agreement you, as a TPS, have agreed to comply with all U.S. laws. Those U.S. laws could be referring to a wide range of legislations and regulations, but assuredly, OFAC is included in the list, even if those requirements have not been specifically communicated to you by your ODFI. Many ODFIs expect their TPSs to contribute to the financial institution's OFAC program. Therefore, it is imperative that TPSs be aware of their responsibilities and their obligations related to OFAC compliance.

One common misconception is that OFAC only applies to international transactions or foreign entities or individuals. But in fact, OFAC sanctions can and sometimes do apply to U.S. citizens and companies as well. **TPSs need to have policies and procedures in place to develop their own OFAC program, whether required by their ODFI or not.** TPSs need to ensure they do not process or facilitate financial transactions for parties targeted by OFAC and that the proper action is taken when such transactions are presented. To make that assurance, the TPS needs to periodically scan its client base, and all parties to the transactions it processes, against OFAC's Specially Designated Nationals (SDN) list. The SDN list is a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. The list is updated frequently and is available to the public via the U.S. Department of the Treasury website. A strong OFAC program should incorporate periodic scans of the TPS's client base against the list. This can be done manually on a per-transaction basis, but there are also several automated programs available for companies to use. Your ODFI may also agree to provide this service to you or on the TPS's behalf.

Once a program is established which incorporates scans of the SDN list, the TPS should have procedures for the evaluation of "hits" and "matches" to the list, and the organization should be able to determine the difference between the two. A hit is where certain information, or strings of characters in the information, compares favorably to a name on the SDN list. A hit could be a common surname matching individuals on the SDN list. A match is of greater quality and could be where the entire name accurately corresponds to an entry on the SDN list. With a match, there should be additional procedures to determine the validity of the match. At this point, the TPS should work with their ODFI to take the appropriate course of action.

If a valid match to a name on the SDN list has been confirmed, the TPS will need to follow OFAC procedures which could include blocking/freezing the transaction, rejecting the transaction, blocking access to funds, performing proper reporting obligations and/or discontinuing the relationship. Even with a strong program in place, consultation with your ODFI and OFAC is highly recommended before taking any of these actions.

Hopefully, this answers some questions you have about OFAC and what it means to your organization and your participation in the ACH Network. While there is no formal requirement, having written OFAC policies and procedures is highly recommended. Another component of a strong OFAC program is the designation of an individual that is primarily responsible for the program. Finally, it is recommended that you partner with, and seek guidance from, your ODFI in developing an appropriate OFAC program for your organization.

If you have further questions about OFAC, don't hesitate to reach out to your financial institution. If you are unsure if your current OFAC policy and procedures align with the current OFAC requirements and would like a deeper dive, contact EPCOR's Consulting/Advisory team at advisoryservices@epcor.org! In addition to providing a comprehensive review, we can provide guidance to help you mitigate risk and improve your ACH, wire and RDC processes.

Electronic Payments Core of Knowledge

EPCOR is a not-for-profit payments association which provides payments expertise through education, advice and member representation. EPCOR assists banks, credit unions, thrifts and affiliated organizations in maintaining compliance, reducing risk and enhancing the overall operational efficiency of the payment systems. Through our affiliation with industry partners and other associations, EPCOR fosters and promotes improvement of the payments systems which are in the best interest of our members.
For more information on EPCOR, visit www.epcor.org.

The Nacha Direct Member mark signifies that through their individual direct memberships in Nacha, Payments Associations are specially recognized and licensed providers of ACH education, publications and advocacy.

www.epcor.org
2345 Grand Blvd., Ste. 1700, Kansas City, MO 64108
800.500.0100 | 816.474.5630 | fax: 816.471.7665