CROSSFIRST BANK®

Treasury Notes

WINTER 2022

Inside this Issue

Meaningful Modernization of ACH Authorizations

by Marcy Cauthon, AAP, APRP, NCP, Director, On-Demand Education, EPCOR

On September 17, 2021, Nacha implemented various *ACH Rules* amendments designed to improve and simplify the ACH user experience by facilitating the adoption of new technologies and channels for the authorization and initiation of ACH payments. Nacha, the rule-making body governing the ACH Network, is hopeful that these amendments will reduce barriers to use the Network, provide clarity and increase consistency around certain ACH authorization processes and reduce certain administrative burdens related to ACH authorizations.

Standing Authorizations

Currently, authorizations for consumer ACH debits encompass recurring and single payments.

Recurring payments occur at regular intervals for the same or similar amount, with no additional action required by the consumer to initiate the payment (i.e. utility bill). A single entry is a one-time payment and can be between parties that have no previous relationship (i.e. online purchase) or between parties that can have a relationship, but the payment is not recurring (i.e. a single payment on a credit card account).

Previously, businesses that originated ACH payments and wanted to use a different model for ongoing commerce did not have specific rules for payments falling somewhere in between the definitions for recurring and single entries. By defining a Standing Authorization, this *Rule* will fill the gap between single and recurring payments and enable businesses and consumers to make more flexible payment arrangements for relationships that are ongoing in nature. For example, I give my insurance company a standing authorization and then they send me a text when the bill is due. When I receive the text, I authorize yes or no to pay the bill via the text message.

The Standing Authorizations *Rule* defines a standing authorization as an advance authorization by a consumer of future debits at various intervals. Under a Standing Authorization, future debits would be initiated by the consumer through further actions. This will allow for Originators to obtain Standing Authorizations in writing or orally.

Subsequent Entries are defined as individual payments, which are initiated based on a Standing Authorization. Subsequent Entries may be initiated in any manner identified in the Standing Authorization. Originators intending to make use of the Standing Authorization/Subsequent Entry framework should appropriately reference the subsequent entries in their authorizations. So, Originators need to specify whether the authorization relates to a single entry, multiple entries or subsequent entries initiated under the terms of a standing authorization.

Originators do have some flexibility in the use of consumer Standard Entry Class (SEC) Codes for individual Subsequent Entries. Originators will be able to use the TEL or WEB SEC Codes for Subsequent Entries, when those entries are initiated by either a telephone call or via the Internet/wireless network, respectively, regardless of how the Standing Authorization was obtained. In these cases, the Originator will not need to meet the authorization requirements of TEL or WEB but will need to meet the risk management and security requirements associated with those

see MEANINGFUL on page 2

MEANINGFUL continued from page 1

SEC Codes.

So, Originators utilizing this flexibility framework should understand the elements of the TEL and WEB rules that apply to their subsequent entries, based upon the consumer's affirmative action to initiate the subsequent entry via a telephone call, internet or wireless network.

An Originator has the option to identify an entry as having been originated under the terms of a Recurring, Single-Entry or Standing Authorization. The standard code values will be "R" for Recurring, "S" for Single-Entry and "ST" for Standing Authorization. An Originator may choose to include these values in the Payment Type Code Field of a TEL or WEB entry or the Discretionary Data Field of a PPD entry. To accommodate this option, the *Rule* will remove the existing requirement that TEL and WEB entries must be identified as either Recurring or Single Entries and will instead designate the Payment Type Code as an optional field. However, Originators may continue to use the Payment Type Code field to include any codes that are meaningful to them, including "R," "S" or "ST."

Oral Authorizations

The Oral Authorizations *Rule* now defines and allows Oral Authorizations as a valid authorization method for consumer debits distinct from a telephone call. Enabling the broader use of Oral Authorizations will allow businesses to adopt ACH payments in transactional settings that make use of verbal interactions and voice-related technologies. For example, I give Amazon a standing authorization. I realize I need ink cartridges for my home computer and say, "Hey Alexa, order a color print cartridge from Amazon." The *Rule* change did not change how existing TEL transactions are used and authorized.

Any oral authorization obtained via any channel will need to meet the requirement of an Oral Authorization. An Oral Authorization obtained over the Internet that is not a telephone call must meet the risk and security requirements that currently apply to Internet-Initiated/Mobile (WEB) Entries and utilize the WEB Standard Entry Class Code. The new *Rule* allows for Standing Authorizations to be obtained orally and for Subsequent Entries initiated under a Standing Authorization to be initiated through voice commands, instructions or affirmations.

Originators may choose to use the expanded applicability of Oral Authorizations but are not required to do so. Originators that want to use Oral Authorizations will need to modify or add to their authorization practices and language to ensure they meet all the requirements for Oral Authorizations. Originators may also find that their digital storage needs will be impacted by using Oral Authorizations.

Proof of Authorizations

An Originator is required to provide proof of authorization to its ODFI in such time that the ODFI can respond to an RDFI request for proof of authorization (within ten banking days). Some ODFIs and Originators report that a "pain point" occurs when they provide proofs of authorization, but then debits are still returned as unauthorized. To avoid this issue, some ODFIs and Originators would prefer to agree to accept the return of the debit rather than expend the time and resources necessary to provide proof of authorization.

The Alternative to Proof of Authorization *Rule* reduces the administrative burden on ODFIs and their Originators for providing proof of authorization requested by an RDFI. By allowing an alternative, the *Rule* is intended to help reduce the costs and time needed to resolve some exceptions in which proof of authorization is requested. However, if the RDFI still needs proof of authorization, the ODFI and its Originator must provide the proof of authorization within ten days of the RDFI's subsequent request. Originators and ODFIs that want to take advantage of the *Rule* may need to modify their business processes.

If you would like to learn more about these new rules, reach out to your CrossFirst Treasury Banker.

Standing Authorization/Subsequent Entry Grid

Standing Authorization Received Via:	Originator Receives Subsequent Entries Instructions Via:	SEC Code of Subsequent Entry
In writing	Internet or Wireless Network	PPD or WEB
	Telephone (orally over the phone)	PPD or TEL
Internet or Wireless Network	Internet or Wireless Network	WEB
	Telephone (orally over the phone)	TEL
Mobile/Telephone	Internet or Wireless Network	WEB
	Telephone (orally over the phone)	TEL

Let's Get Digital

by Allison Bramblett, Treasury Management Officer, The Farmers Bank

Over the last few years, digital payments have become very popular; even more so during the COVID-19 pandemic, as many stores have added a contactless payment option to avoid the spreading of germs. If you haven't tried contactless yet, I highly recommend it on both a business and personal level!

Although I must confess, there was a time in my life where I wasn't as enthusiastic about digital payments, and I thought checks were the way to go. When I opened my first bank account, the Customer Service Representative asked if I wanted checks. I was so excited to have my very own! I couldn't wait to personalize the background, symbols and even add a quote in the by-line. I really thought I was cool.

It wasn't too long after when I started realizing electronic and digital payments were the better, faster and most convenient way to handle my finances. I was a young adult and could barely take care of myself, let alone take care of mailing in payments on time, remembering to pay back friends and not losing what cash I did have in my possession. And when I knew there was an option to pay my friends and family quickly and digitally? Sign. Me. Up.

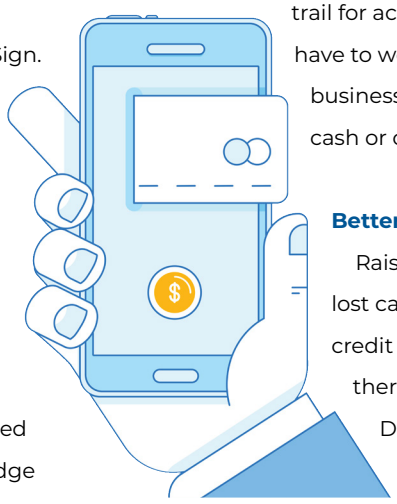
Fast forward to a couple of years ago, when I needed some work done on my home and the business only accepted cash or checks. I then had to pull out those checks I received nearly 15 years ago, wipe off the collected dust and ask that they not judge my checks, which most definitely have the personality of a 21-year-old (check out the image of my old check for a glance into my young adult self!). Of course, they didn't care, they were just happy I paid.

Nowadays, I will always utilize a digital/contactless payment before pulling out my wallet to pay with a physical card. And, I've seen some amazing results from companies utilizing digital payments. So, why should your organization choose to use a digital payment method over any other payment method?

Convenience

We can all agree there is plenty to remember and do daily in our lives. The capabilities technology gives us now is the convenience we're looking for to simplify some of those tasks. With digital payments, you have the capabilities of leaving your home or office with only your phone in hand, and you potentially have everything needed to get through your day. Gas stations, grocery stores and more have some form of contactless payment system, and it's as easy as hovering your phone over the card reader and within seconds the sale is finished.

From a business perspective, the conveniences of digital payments are endless. With digital payments, your processes are more automated, there's an additional paper trail for accounting and you don't have to worry about potentially losing business clients who don't carry cash or checks on hand.



Better Security & Less Fraud

Raise your hand if you've ever lost cash, a checkbook or a debit/credit card? I'm willing to bet there are some raised hands. Digital payments allow us to leave that worry behind. Once your card number has been added to your digital wallet, you can keep your physical card in a safe and secure place. There are also layers of biometric authentication, encryption and tokenization in place to secure any purchases made digitally.

If you use cash for your purchases, there's a higher risk of those funds being lost or stolen. On the flip side, if you're a merchant that accepts the consumer cash as payment, you must consider the possibility of accepting counterfeit bills. And, having large amounts of cash sitting around could put your organization at risk for a robbery.

Cost & Time Savings

Using a digital payment method provides your organization the opportunity to save on the cost of checks and the time spent making trips to your financial institution. There's also time saved in completing business transactions. Utilizing cash means waiting for change back, or even waiting on the card reader to recognize a chip card. Contactless payment allows for a quick and effortless way to complete the purchase.

These are just some of the bigger benefits of utilizing a digital payment method. I could go on and on with more examples, not just for the consumer, but for merchants and businesses as well.

Forbes recently reported the digital payments market is set to grow globally at 19.4% CAGR between 2021 and 2028, so now is the time to increase your usage of digital payments and stay in line with the growing market! It's important to balance what your clients want with what is best for your organization. Reach out to your CrossFirst Treasury Banker to discuss what is right for your organization.

Don't Get Smoked with Counterfeit Check Scams

by Cheri Fahrbach, Senior Vice President and Manager, Retail Banking, First National Bank and Marcy Cauthon, AAP, APRP, NCP, Director, On-Demand Education, EPCOR

Picture this—a gentleman has extensive smoke damage to his home due to an electrical fire. This information was posted on social media and shortly thereafter, he began receiving messages from a woman who appeared compassionate about his situation and willing to lend an ear. After sending one photo of herself and a brief Skype phone call, money became a point of conversation.

The woman claimed to have funds due to her from an estate that her "uncle," was helping her access. In the end, the man sent $5,000 to help this woman for attorney fees, thinking he was assisting her in collecting her inheritance so she could fly overseas to see him.

Just his luck—the woman had a friend in construction, so she offered to provide funds to the man in the amount of $60,000 for home repairs. He was dealing with extensive smoke damage, after all. He was instructed to open an IRA, then do an early withdrawal and take a cashier's check for $47,000 to the woman's friend's financial institution, which he did. In the end, because the teller at the financial institution of first deposit put a hold on the funds, the man and the financial institution were spared losing $47,000.

Believe it or not, situations like this involving counterfeit checks and similar frauds are all too common. Typically, a person will receive a check from a scammer for a variety of reasons. They're told they are a sweepstakes winner, or they have received overpayment for online purchases, or it's pay from an online job, to name a few. The victims are then told to use part of the funds to pay some sort of fee, taxes, charges or other costs associated with the scam to a third party and assured they can keep most of the check for the monetary cost of the transaction. Days later, the victim discovers the check bounced at the financial institution and they are now liable for the full amount of the fraudulent check, including any money they returned to the scammer or spent themselves.

It's important to stay vigilant when fighting these types of fraudulent situations. Here are some tips for you, or for you to share with your employees and clients, to avoid counterfeit check scams:

- Do not accept a check from someone you do not know.
- Do not wire or send money to people you do not know.
- Never cash a check you are not expecting.
- Always verify a check's validity before depositing.
- Never provide any personal identifying information.
- If you receive a fraudulent check, shred the check and discard.

These scams work because fake checks generally look just like real checks, even to financial institution employees. They are often printed with the names and addresses of legitimate financial institutions and it can take weeks for an organization to realize the check is fake. Many scammers demand that victims send money through money transfer services, like Western Union or MoneyGram, or buy gift cards and send them the PIN numbers. Once the money is wired, or scammers have the gift card PINs, it is like giving someone cash. It's almost impossible to get it back.

If you suspect a check is fraudulent, it's best to proceed with caution and reach out to CrossFirst Bank for assistance on next steps.

Source: Federal Trade Commission

Focus on Fraud: A Look at Ransomware

by Jim Smith, CTP, Vice President - Treasury Management Services, Union Bank & Trust Company

No matter how many precautions you take to secure your company's data, you can't help but wonder if it's ever enough. If you're familiar with the evolving cyber scams, you know that education is key to helping protect your company against fraud.

Ransomware scams can be very costly and debilitating if you lose all your data or are threatened with a release of sensitive information. So, you may be asking: what is ransomware, where does it come from and how do you reduce the risk of this attack? Let's talk about it.

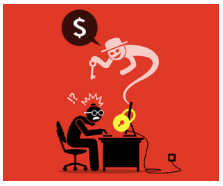
What is Ransomware?

Ransomware is a form of malicious software, or malware, that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data. With the rapid shift to remote work by millions of Americans, and a dramatic surge in phishing scams and fake websites, we are all at increased risk of ransomware attacks—individuals and businesses alike.

While we tend to see reports of these incidents among government and critical infrastructure organizations, this type of cybercrime can (and does) happen to any type of business or individual. Anyone connected to the internet with data stored on their device or network is at risk.

During a ransomware attack, you would likely receive messages telling you that your data has been encrypted, and demanding you pay a fee to regain access. You would then be given instructions on how to pay the fee to receive the decryption key. This "ransom" can range from a small amount to thousands or even millions of dollars, depending on the value of the data. It's usually demanded in the form of Bitcoin or other types of anonymous cryptocurrency. The cybercriminals may threaten to sell or leak this stolen data if you don't pay the ransom. They may threaten to publicly name you (or cyber-shame you) as a secondary form of extortion. The attack may also involve deleting system backups, making it even more difficult to restore your data.

Some victims pay to recover their files with no guarantee the files can be retrieved.



Your stolen data may even be sold on the dark web. Recovery, when it happens, can be a difficult process that may require the services of a data recovery specialist. This process can severely impact business processes, and leave organizations without crucial operational data and with a fractured reputation.

Protecting Yourself and Your Business

So, how do these attacks occur? And how can you prevent one from happening? This moneymaking scheme can be initiated through deceptive links in an email, instant message or a website designed to install malware. The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following precautions to protect yourself against the threat of ransomware:

- Update software and operating systems with the latest patches. Outdated applications and operating systems are the target of most attacks.
- Never click on links or open attachments in unsolicited emails.
- Back up data on a regular basis. Keep it on a separate device and store it offline.
- Follow safe practices when using devices that connect to the Internet. Read Good Security Habits for additional details.

CISA also recommends organizations employ the following best practices:

- CISA released a guide for parents, teachers and school administrators that provides information to prevent or mitigate malicious cyber actors from targeting K-12 educational institutions, leading to ransomware attacks, theft of data and the disruption of learning services.
- Restrict users' permissions to install and run software applications and apply the principle of "least privilege" to all systems and services. Restricting these privileges may prevent malware from running or limit its capability to spread through a network.
- Use application allowlisting to allow only approved programs to run on a network.
- Enable strong spam filters to prevent phishing emails from reaching end users and authenticate inbound email to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

We also recommend reading CISA's article in its entirety and downloading whatever related resources you may find helpful.

Source: CISA