Alliance Bank epcor Electronic Payments Core of Knowledge

PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

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

see MEANINGFUL on page 2

Education for ACH Originators

by Jen Kirk, AAP, Vice President, Education, EPCOR

If you are a business that originates ACH payments, the *ACH Rules* likely feel overwhelming. However, it's extremely important that you, as an Originator, understand and abide by the *ACH Rules*.

Luckily, there are several ways you can understand your responsibilities without breaking much of a sweat. Here are some of the resources EPCOR's payments experts have created for businesses like yours, to make *ACH Rules* compliance a little easier.

ACH Rules

Keeping the *ACH Rules* at your Originating fingertips is a great way to make sure you have access to the information you need for on-the-spot decision making. The *Rules* are available in a paper copy, App version or Online version. We also have *ACH Quick Reference Cards for Corporate Users* to help Originators find quick information on ACH Returns, Dishonored Returns, Standard Entry

see ORIGINATORS on page 3

MEANINGFUL continued from page 1

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 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 financial institution.

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

ORIGINATORS continued from page 1

Class (SEC) codes, Transaction codes and Notifications of Change (NOC).

ACH Quick Reference Guide for Corporate Users

Next year, we're rolling out a brand-new resource we're calling the *ACH Quick Reference Guide for Corporate Users*. This Guide is a quick summary of all the *ACH Rules* that ACH Originators need to know, and covers general rules, ODFI/Originator requirements, pre-requisites and warranties, as well as a review of all the processes such as returns, NOCs, prenotes and more! This new resource will be available for as low as $30 and will be available in both print and electronic versions. We can't wait to hear what you think!

Payments Insider

This semi-annual e-newsletter (which you're reading right now!) is designed to inform businesses of all sizes of recent payment systems developments and is distributed in the months of April and October. The EPCOR team meets and cues in our Cash & Treasury Management Committee, comprised of EPCOR members, to determine what corporate payments users need to know about current payment systems changes and challenges. All articles are written from the corporate user's perspective.

Annual ACH Rules Update for Corporate Users

Each year, our training team puts together this handy document that outlines ONLY the *ACH Rules* changes that pertain to corporate users in the coming year. We break those changes down in easy-to-understand language and explain their impact on corporate users—from their perspective. This update is part of our April edition of *Payments Insider* each year.

Did You Know... Informational Videos

Many of the topics covered in our *Did You Know...* informational videos are perfect for corporate users. Recent topics include the third Same Day ACH window, new WEB debit standards, money mules and pandemic scams, tips for avoiding bad checks and more! Each video is short, sweet and to the point to make the message easy to understand and remember.

Corporate User Webpage

I saved the best for last! If you haven't checked out our new Corporate User Webpage, you won't want to wait much longer. The idea for this page and everything on it came from members of our Cash & Treasury Management Committee, comprised of EPCOR members. The page includes links and information for all the corporate user resources listed in this article and more, including:

- Upcoming *ACH Rules* Changes
- *Payments Insider* Newsletter for Corporate Users (Includes *Annual ACH Rules Update for Corporate Users*)
- *Did You Know...* Short Informational Videos
- Check Fraud Spotting Tool
- Nacha Operations Bulletins
- Tips for Handling NOCs
- Frequently Asked Corporate User Questions & Answers
- Quick Reference Guides and Cards
- Audit and Risk Assessment Workbooks
- Corporate User Education

Be sure to take advantage of the resources above and remember, your financial institution is there to help.

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

see DIGITAL on page 5

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 with 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.

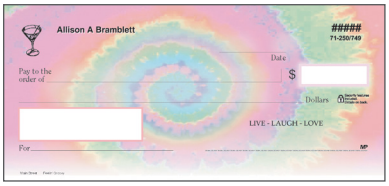
These scams work because fake checks generally look just like real checks, even to financial institution employees. They are often printed with the names and addresses of legitimate financial institutions and it can take weeks for an organization to realize the check is fake. Many scammers demand that 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 your financial institution for assistance on next steps.

Source: Federal Trade Commission

DIGITAL continued from page 3

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

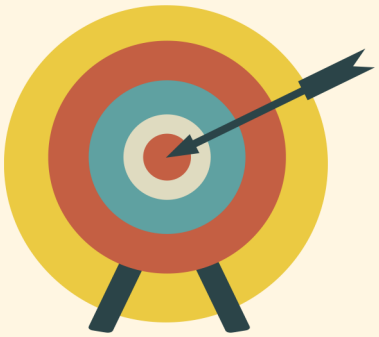
Using a digital payment method provides your organization the opportunity to save on the cost of checks and the time spent making trips to your financial institution. There's also time saved in completing business transactions. Utilizing cash means waiting for change back, or even waiting on the card 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. You might want to think about Buy Now, Pay Later (BNPL) or other digital offerings. Reach out to your financial institution to discuss what is right for your organization.

Plan Now to Advance Your Payments Goals for 2022!

- Start accepting new payments types
- Better understand payments rules and regulations
- Create payment policies and procedures
- Evaluate payments risk or efficiency
- Increase recognition through payments accreditation



If you are thinking of conquering ANY payments challenge, reach out to EPCOR (800.500.0100 or memserve@epcor.org) to find out how we can help!

Payment Systems Update

Are you ready for *ACH Rules* changes coming in the new year?

Find out what you NEED-TO-KNOW at EPCOR's 2022 *Payment Systems Update* seminar!

Watch epcor.org for details.

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.

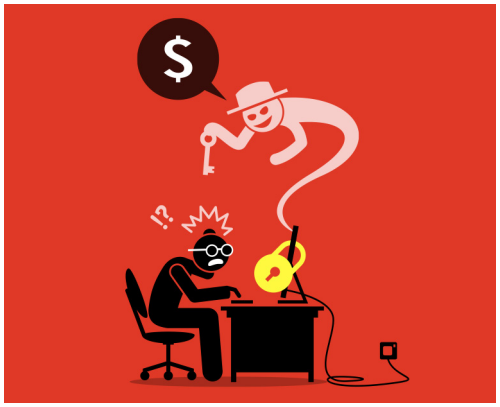
What is Ransomware?

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.

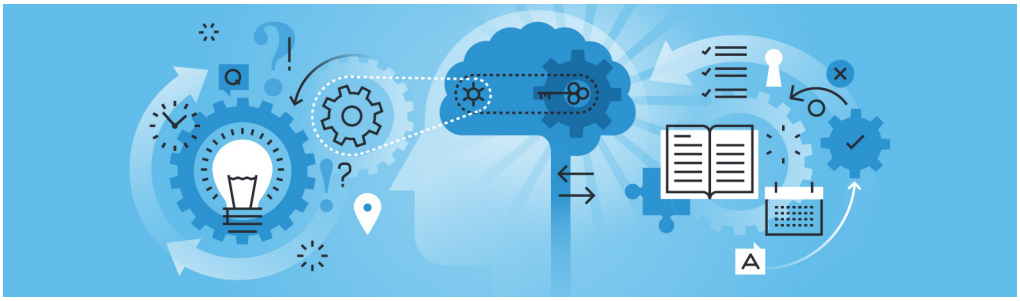
We also recommend reading CISA's article in its entirety and downloading whatever related resources you may find helpful.

Source: CISA

Four Faster Payment Methods for Businesses and How Each One Can Benefit Your Brand

The following article originally appeared on January 21 on RedBridgedTA.com.

Over the last few years, the number of corporates and financial institutions seeking faster payment methods in the U.S. has spiked. COVID-19 has pushed many corporates further in this direction,



and it has highlighted the need for quick, contactless payment methods. With branch closures and employees working from home, companies are looking for faster, safer and more convenient ways to make payments. As a result, the popularity of Same-Day ACH, Real-Time payments (RTP), mobile payments, Zelle transactions and other types of electronic payments have grown rapidly.

Same-Day ACH

Corporates familiar with ACH payments know that they are electronic bank-to-bank funds transfers processed through the Automated Clearing House network. These payments have different settlement times, depending on the premium the corporate is willing to pay. Because it has the fastest settlement times, Same-Day ACH is the most expensive payment type. However, despite its higher price, Same-Day ACH has clear benefits that could entice a company to use them more frequently.

Same-Day ACH's primary benefit is the speed at which the payment is settled. As the name says, the settlement occurs the same day. This is great for corporates that are under a time constraint when it comes to making payments. On the receivables side, Same-Day ACH could be a great alternative for card acceptance because businesses would not have to pay other fees like interchange or assessment fees.

Beyond the higher price tag, same-day settlement can also be a disadvantage. For example, it can put pressure on a payroll team to have all the files sent and settled the same day. Any issues with the file or its contents could cause a delay in payment.

Real-Time Payments

The RTP® Network was launched in November 2017. At first, financial institutions and corporates were slow to adopt this new technology because it required significant updates to internal systems and processes to enable the payments. However, as organizations started to understand the many benefits of implementing this new payment type, both the number of financial institutions and the number of transactions sent over the network increased substantially.

Benefits of sending and receiving payments through the RTP Network:

see FASTER on page 8

FASTER continued from page 7

1. RTPs can be made and received from existing accounts, so there is no need to open new accounts.
2. Corporates can send and receive money 24/7, with immediate availability of funds received.
3. If there is an outstanding invoice to your company, you can send a "request for payment" via the network.
4. Being able to send and receive money instantaneously keeps corporates more in control of their cash flow and working capital needs.
5. Once the payment is sent over the network, the payer cannot recall or cancel the payment. This provides the payee settlement finality.
6. The network only "pushes" money, which mitigates fraud such as someone being able to pull money from an account.

Real-Time payments also assist with straight-through processing and automated reconciliation. Reconciliation can be a large pain point for many corporates. Each payment sent through the network is accompanied by enriched data, which makes it easy to match a payment to a specific invoice and allows corporates to dedicate less time to receivables reconciliation.

Mobile Payments

Many global and domestic financial institutions have mobile banking solutions. This gives companies the ability to authorize payments from their mobile phones. Corporates have slowly been shifting to mobile banking over the past few years, and over the last year, financial institutions have seen an increase in the use of this solution due to the pandemic. Mobile banking allows employees to send payments from any location, and with a large percentage of employees working from home, this is a new convenience.

Mobile banking solutions are very secure with passcodes, touch ID capabilities and tokenization. Tokenization safeguards the payee's account details so when a transaction is sent, the actual account number is not shared. Not only do the mobile banking solutions let corporates make payments on the go, but they also can provide visibility of real-time balances across accounts and cash positioning. As financial institutions continue to see interest in this solution, the innovation and capabilities will expand.

Zelle®

Zelle is one of the newer payment methods being widely used by small businesses and consumers. Zelle payments can be made directly between two consumer accounts with the use of an email or mobile phone number. Consumers have been the primary users of Zelle payments, but businesses are slowly starting to adopt this technology as well. So far, the transaction path for business-related transactions has mostly been business to consumer; however, it is only a matter of time before there is more consumer-to-business traffic.

One of the advantages of this payment option is the fact that account numbers are not exchanged between the parties. Transactions are quick and easy, and they can be sent and received either online or through a mobile banking application. Zelle transactions are best used when the sender has to make a quick, low-dollar amount transaction.

Fraud implications should be considered with Zelle payments. The fact that only an email address or mobile phone number is used is both its biggest advantage and biggest disadvantage. If, for example, the sender accidentally misspells the receiver's email or types the wrong phone number, they could potentially lose their money. Currently, there is no way to "undo" a payment. Once the payment is submitted, the sender cannot cancel it, unless the receiver has not yet been registered with Zelle. Another thing to consider is that this might be more difficult for larger companies to use, because linking an account to an employee's mobile phone number or email could be risky. Although these concerns have yet to be completely resolved, it is expected that financial institutions will find a way to address them soon.

Transaction Limit by Payment Type

Payment Type	Limit
Same-Day ACH	• $100,000 per transaction • Increased from $25,000 in March 2020
Real-Time Payments	• $100,000
Mobile Payments	• Varies depending on the financial institution and the type of account. Ususally tied to the account's limits.
Zelle	• Varies depending on the financial institution and the type of account. • Daily limits range from $500 to $5,000 • Monthly limits range from $5,000 to $40,000

Federal Reserve Bank Instant Payment Resources

Consumers and businesses are moving toward technologically advanced payment practices that better align with their ever-evolving wants and needs. The COVID-19 pandemic and associated economic downturn have resulted in a rapid increase in faster payments use, and a growing demand for a certain type of faster payments called instant payments. The Federal Reserve article *How Can Faster Payments Benefit Me?* gives a full picture of how individuals, businesses and financial institutions might benefit from

see FASTER on page 9

FASTER continued from page 8

adopting faster payments, including instant payments, for a variety of transactions. Consumers benefit from increased flexibility and transparency into payment status, businesses benefit from improved cash flow and money management and financial institutions benefit from new solutions that enable them to better serve their clients.

While many can benefit from instant payments, as with any type of payment, the potential for fraud exists. But, some characteristics of instant payments may increase fraud concerns. Read the Federal Reserve article *Fraud and Instant Payments: The Basics* to learn about various types of fraud involving payments, the particular challenges posed by the unique characteristics of instant payments and ways to protect your organization and clients against instant payments-related fraud.

Are instant payments just another payment option for businesses, or are they an opportunity for transformation? In many cases, instant payments can drive efficiencies, minimizing or even eliminating the costly, manual payment processes that many businesses experience today.

Major corporations and large businesses have already made significant investments in systems that enable them to automate some of their payments processing by using existing payment rails and electronic data interchange (EDI) messaging tools. In fact, an estimated 25% of the 25 billion invoices exchanged annually in the United States use these tools. Lacking the resources to make the same investments, however, some smaller and midsize businesses may be less able to automate their payment processes.

Instant payments can provide the much-needed opportunity for smaller businesses to expand their payment processing capabilities and possibly see a real, beneficial change in this landscape by eliminating some of its current complexities. However, it will take the entire ecosystem, including financial institutions, accounting software providers and business partners, to enable instant payments and streamline the process from end to end. In addition, it's particularly important for businesses to understand and plan for what's involved in making this happen. The following links talk a little bit more about what the Federal Reserve Bank is doing to address these issues:

- *Instant Payments and B2C: Opportunity for Efficiencies and Modernization*
- *Instant Payments: What Could They Mean for How We Do Business?*
- *Study Reveals Pandemic is Spurring Business Demand for Faster Payments*

Source: RedBridgedTA.com.

Get Ready for Instant Payments: Focus on Relieving Pain Points and Creating Value

The following article originally appeared on FRBServices.org.

Whether they're utilities, insurance companies, lenders or healthcare providers, all billers have at least one thing in common, namely, accounts receivable (A/R) processes that, on occasion, go awry. Payment snafus can force organizations to devote significant resources, usually staff time, to resolve them. If these issues occur frequently, it could be time to rethink the underlying payment process to reduce their likelihood.

Instant payments provide an opportunity to resolve, or at least mitigate, a variety of payments-related pain points. The scenarios described below could assist in developing a vision for the A/R benefits in the return on investment (ROI) equation for instant payments.

Late Payments and Service Shutoffs: C2B Scenario

An electric utility or mortgage lender's client sends a check that is delayed in the mail and becomes subject to a late payment penalty. This may lead to an angry client calling the biller's customer service or A/R department to complain and ask for a waiver of the penalty. Up to 18% of client calls to companies are bill-related, and handling such calls costs on average $8, in addition to the potential for client ill will. Encouraging clients to use instant payments, even on the payment due date, can reduce the incidence of late

see INSTANT on page 10

INSTANT continued from page 9

payments and the need to handle a costly call from a dissatisfied client.

In addition, instant payments are especially useful to the utility company when a client's account is so delinquent that they must make an immediate payment to avoid a costly service shutoff. Compared with other payment options that the client might use, instant payments eliminate the possibility of the payment being returned. Instant payments also can provide immediate confirmation of payment and thereby potentially reduce the volume of client calls to the biller's A/R department to check on payment status.

Returned Payments: C2B Scenario

In any given billing cycle, some payments get reversed, or charged back, due to insufficient funds in the client's checking account, over-the-limit card account balance, card expiration or account closure. Offering instant payments as an option to clients could reduce the incidence of returned payments because they are irrevocable "push" payments, and clients can take advantage of them only when they have the funds to do so. In addition, instant payments can give billers an important tool to support the collection process. By including a scannable QR code that contains a Request for Payment (RFP) in collection communications, a mobile network service provider, for example, could offer clients a way to use their mobile banking app to initiate an instant payment to resolve the obligation immediately and with certainty.

Autopay Aversion: C2B Scenario

To reduce late payments and automate payments processing and client account posting, many lenders, insurance companies and utilities, among others, encourage clients to sign up for automatic recurring ACH or card payments. Almost always, however, some part of the client base is unwilling to do so; in fact, a study by Aite found that only 35% of consumer bill payments are set up to be paid on a recurring basis. This is due to a variety of factors, including consumers' desire for more control over the timing of their payments and their cash flow. In addition, some have concerns about having their financial institution account number stored in the biller's database.

For these clients, billers could update A/R systems to include in their client billing statement a QR code or URL linking to an RFP message that the client could scan or click to initiate an instant payment. Clients would control the timing of the payment, and they wouldn't need to provide payment card or checking account information to the biller. And the biller could see a reduction in returned payments relative to all other payment options they offer, as well as reduced handling costs.

Posting Errors: B2B Scenario

A close cousin to late payment pain points are payments that are posted incorrectly. These situations arise primarily because the client hasn't provided accurate or complete remittance information with the payment.

Consider a commercial client's payment for telecommunication services that lacks the needed remittance details. This payment leaves the A/R department of the communications services provider guessing about which account and which invoice(s) to credit. If the wrong account or wrong invoice is credited, the A/R department may end up reinvoicing and possibly charging that client late fees or denying an early payment discount. This could lead to a poor client experience.

Compounding the error, the client's accounts payable (A/P) department may pay the duplicate invoice, resulting in overpayment issues that need to be resolved as well. Reaching resolution entails costly staff time for both the biller and the client.

Billers can reduce the incidence of, and costs associated with, incomplete or missing remittance information by sending clients an RFP message via an instant payments service such as the FedNow℠ Service. This message could include account number and certain invoice details, enabling the automatic inclusion of the necessary remittance information when the client makes the corresponding instant payment.

Using instant payments to send an e-invoice is also potentially beneficial to the commercial client. It enables the client to upload the invoice into their A/P system and automatically schedule their payment to take advantage of any early payment discounts or pay on the due date to maximize working capital and liquidity.

Time to Focus on Pain Relief?

These payment scenarios only scratch the surface of the pain points encountered by billers and their clients alike. Even so, they can help stimulate thinking about how instant payments could provide tangible cost-saving benefits, notably reduced staff time spent resolving posting errors, returned payments and client complaints, while improving customer service.

Taking advantage of the pain point relief instant payments can offer will require billers, as well as others involved in supporting end-to-end payments processing, to update a variety of systems and processes. Work with key partners, including financial institutions, vendors and key clients to determine the ROI and get ready.

Source: FRBServices.org

Alliance Bank

epcor®

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.

Nacha® Direct Member

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