



PAYMENTS INSIDER

The inside scoop on payments for businesses of all sizes

INSIDE: ACH Rules Update for Corporate Originators	pg. 1
Penny for Your Thoughts—Where are the Coins?	pg. 1
5 Signs it's Time to Consider Electronic Payment Options AND 5 Options to Consider	pg. 1
Money Mules & Pandemic Scams	pg. 2
How Well Do You Really "Know Your Client?"	pg. 3

COVID-19's Impact on Payments Usage	pg. 4
I Went to Prison for SBA Loan Fraud: 7 Things to Know When Taking COVID-19 Relief Money	pg. 5
Protecting Small Businesses from Fraud	pg. 7

ACH Rules Update for Corporate Originators

As an Originator of ACH entries, it is important to stay current with the *ACH Rules*, including how updates and changes might impact your business. In case you missed it in our April edition, read through our [2020 ACH Rules Update for Corporate Originators](#) to discover some important changes coming in 2021 and beyond. Also, did you know you can influence the *ACH Rules* by participating in Nacha's Requests for Comment and Requests for Information? Contact your financial institution to learn more. 🌱

NEW RESOURCE CENTER COMING SOON!

EPCOR is in the process of launching a Business Payments Resource web page. This page will be a resource for business/corporate account holders to receive information from our various payment channels. This page will also have an FAQ section to address common questions you deal with daily. Stay tuned for our page launch, coming in 2021!

5 Signs it's Time to Consider Electronic Payment Options AND 5 Options to Consider

by Amy Donaghue, AAP, APRP, NCP,
Director, Advisory Services – Risk & Third-Party Services, EPCOR

Is it time to consider electronic payments? If you've experienced any of the five warning signs below, it might be time for your company to make the move!

1. You've turned clients away who didn't have cash on hand.
2. Donations or sales have plummeted during the pandemic.
3. You're running out of coins to make change.
4. It's getting harder to make runs to your financial institution.
5. Your clients are asking for it!

see OPTIONS on page 2

Penny for Your Thoughts—Where are the Coins?

by Brian Laverdure, AAP, Director,
Emerging Payments Education, EPCOR

"Hey, do you have change for a dollar?" The once simple act of breaking a dollar has become increasingly difficult due to disruptions in the regular supply and distribution of coins. Is there a coin shortage? Not exactly, because the United States has plenty of cash and coins

floating around. However, many businesses cannot access an adequate amount of coins to service their clients. So, what is going on?



The Root of the Problem According to reports from the Federal Reserve Bank of Atlanta, the United States has

approximately \$47.8 billion in coin currently in circulation. On top of that

see PENNY on page 3

OPTIONS continued from page 1

The COVID-19 pandemic has challenged the way we live, including how we make and receive payments. Luckily for small businesses, there are more options than ever to send and receive money. Long gone are the days when accepting debit and credit cards were the most common (and often expensive) payment alternatives. And, your financial institution is the perfect partner to help you find the payment alternative(s) that best fits your company's way of doing business and budget. Here are just a few payment alternatives financial institutions have reported helping companies like yours implement since the world changed drastically this spring:

- **ACH Credit Push/Pull:** Did you know you can accept payments from your clients and pay your vendors electronically – without using a card or check? ACH stands for Automated Clearing House and the name says it all. By using simple account information, you can send and receive payments electronically without ever having to touch a physical form of payment. Additionally, your financial institution may offer the ability to

process ACH payment activity the same day the receiver's information is obtained. Everything happens behind the scenes without anyone having to go to their financial institution or your place of business. It's also a great way to accept donations or payments online. Both small and large businesses can also use the end-of-day data file (sometimes including images of the payments) typically provided with lockbox processing for straight through processing and cash forecasting.

- **Remote Deposit Capture:** If you can't envision life without paper checks, then Remote Deposit Capture can at the least save you endless trips to your financial institution to make deposits. This handy check processing method is available in a variety of formats that can include hardware provided by your financial institution that reads information from the checks. Or, it may be as simple as taking photos with your phone! No more trying to sneak away before closing time to make a run to your financial institution or trying to securely transport bags full of checks.

- **Lockbox Processing:** If you handle large volumes of mail payments sent to your place of business, handling those items during the pandemic while adhering to social distancing and other restrictions may become burdensome. Lockbox processing is similar to Remote Deposit Capture, but instead of the payments coming to you they are sent to a special post office box and processed by a third-party. Image technology like that used in Remote Deposit Capture is utilized to read payment information to expedite payment processing, reduce errors and ensure funds are deposited into your accounts as early as possible.
- **Card and Wire Payments:** Sneaking two in here, but they are classics for a reason. If the cost or hassle of handling card and wire payments has deterred you in the past, it may be time to look again. New technology and integration with payment apps now provide new ways to utilize these payments types and minimize some of the traditional risks.

If you are interested in exploring new payment options, please reach out to your financial institution. 📞

Money Mules & Pandemic Scams

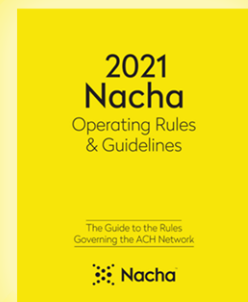
Did You Know...

Fraudsters will stop at nothing to steal money. And guess who is left holding the bag? You, the "money mule!" EPCOR's recent *Did You Know* video breaks down how this common type of fraud takes place and how to prevent it in a quick, easy-to-digest format. Watch on YouTube and then share it forward with your co-workers and loved ones. If you have clients



who need to hear this message, reach out to EPCOR Member Support (800.500.0100 or memserve@epcor.org) about hosting the video on your company's website. 📺

Order Your Digital Copy of the 2021 ACH Rules



Ensure compliance by making sure you are using the most current *Rules* available. Access your digital copy on your desktop or via an app on your mobile device! Contact Member Support at memserve@epcor.org to place your order!

PENNY continued from page 1

existing supply, the [Federal Reserve also announced](#) that the U.S. Mint is running at full capacity and it will produce 1.65 billion coins per month for the rest of the year. So... Where is it all then? Well, a lot of it is sitting in piggy banks or stuck between couch cushions across the nation! In normal times, many Americans take their coin collections to financial institutions to deposit or perhaps to a coin-counter at a grocery store to turn into cash or gift cards. Once deposited, these coins can circulate throughout the economy, as businesses pick up change orders and use coins in everyday commerce. Unfortunately, the ongoing pandemic has brought everything to a grinding halt since many Americans are limiting their trips outside to reduce their potential exposure to the virus. Thus, the cumulative effect of so many individuals choosing to keep coins at home, in wallets and piggy banks, is a nationwide disruption in the regular circulation and supply.

How Are Businesses Responding to the Shortage?

For some, the shortage may have pushed businesses away from being “cash-only” to quickly adopting credit or debit cards. For others, however, there may be less of an impact due to an earlier digital payment push, perhaps at the beginning of the coronavirus lockdown in late February and early March. But what will happen to these new digital or contactless payment experiences as the pandemic continues? Will we see people return to old ways, like cash, once conditions improve? Or, will the pandemic forever alter the landscape of electronic payments and produce a new generation of Americans with

little, or perhaps no, experience with cash and coins? Only time will tell!

How is the Industry Responding?

[The Federal Reserve convened the U.S. Coin Task Force](#) in July to bring together leading experts from financial institutions, merchants, coin machine operators and other related groups to provide insights on possible ways to improve distribution and supply. The task force issued a [preliminary report on July 31](#) in which it committed to producing materials to educate consumers about coin circulation and recommend best practices for financial institutions to encourage account holders to bring in coins. [One bank in Wisconsin](#) even initiated a special program offering a \$5 incentive for every \$100 in coins deposited by its account holders!

What Can Your Business Do Now?

Although we cannot look into a crystal ball to seek exactly what payments will look like after the pandemic, it is a safe bet that digital payments will be important. The shift from paper to digital began long before the virus hit, and the underlying causes of that shift, like easily accessible smart phone technology, will continue to push innovation forward. Businesses should continue to position themselves for success today and in the future by knowing what makes the most sense for their clients and implementing the right digital products for their specific needs. And, if you aren't sure of your options are or what makes the most sense for your company specifically, reach out to your financial institution for guidance and recommendations. 🟢

How Well Do You Really “Know Your Client?”

by Karen Nearing, AAP, APRP, CAMS, CRCM, NCP, Director, Compliance Education, EPCOR

Has the pandemic changed your business model? Have the shelter-in-place orders changed traditional ways clients interact with you? Has technology enabled a new wave of clients to find your business?

New clients can be exciting and promising for the future of your business. However, we also must be cognizant that fraudsters are using the pandemic to defraud businesses as well as consumers. As we look at these new opportunities, we must also figure out the risk in engaging with this new entity. How do I know who my client is and what is his/her intention?

Fraudsters use the internet to find information about people and either manipulate the information to suit their needs or conveniently update the information to make it appear as if the information conforms to the request. This manipulation

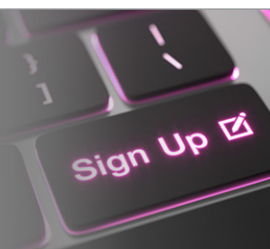


see CLIENT on page 4

Explore EPCOR Membership

For ongoing access to payments-related guidance, resources and information, consider becoming an EPCOR member.

Explore your options by calling 800.500.0100 or visiting epcor.org.



CLIENT continued from page 3

of information has led to a new type of identity theft called Synthetic Identity Fraud. This type of fraud enables current and manipulated information to become part of what appears to be a legitimate or “real identity.” This new type of fraud enables the fraudsters to bypass certain verification services, such as credit verification services, because red flags aren’t raised, and the fraudster’s synthetic identity is assumed to be that of a real client based on the criteria.

In addition to automated processes of getting to “Know Your Client,” here are some questions to ask as you build new relationships to help avoid the reputational and credit risk of accepting synthetic identities as clients:

- Does the order make sense?
- Does the client live within my typical market?
- Is the order consistent with other orders I receive?
- Can I reach them on the phone?
- Have I reached out to them to confirm the order?
- Will payment be made in advance and how is the payment being made?
- Is the name and address on the payment the same as the order?

In addition to the questions above, be sure to validate any information provided by reaching out to your clients on the phone directly. Don’t just email, pick up the phone and call to confirm. Be sure you’re the one calling them, don’t let them call you. Also, don’t forward or reply to emails, start a new email string to avoid a potentially compromised email address. And, don’t rely on easily accessible personal information.

Fraudsters know how valuable your goods and services are and will do just about anything to get your trade secrets without legitimately paying for them. Trust your instincts and do not be afraid to cancel orders that do not make sense or are risky to your livelihood. A new client or a new order may not be worth it in the long run. 🟢

COVID-19’s Impact on Payments Usage

by **Brian Laverdure, AAP, Director,
Emerging Payments Education, EPCOR**

How has COVID-19 impacted the way people use payments?

That’s a great question and I will answer it with another: when is the last time you made a cash payment? With the rapid spread of the novel coronavirus in late February and early March, cash—and even any sort of in-person transactions—suddenly became difficult, if not impossible, due to social distancing measures that shuttered businesses.

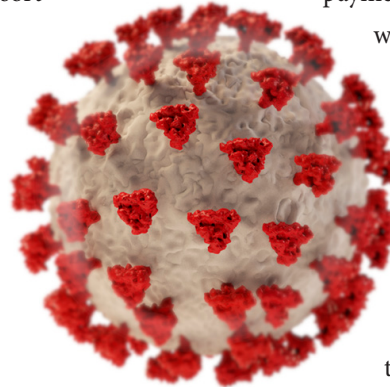
As economies around the United States are reopening and adjusting to their “new normal,” many businesses are shying away from accepting cash in favor of contactless or mobile payments that may help limit interactions that could spread the virus. We do not yet know the full long-term impacts of the coronavirus on payments, but it is important to look at what has happened in the past few months to see how swiftly payment behaviors changed for a glimpse at what the future of payments holds.

Right now, we know that interest in and usage of contactless and mobile payments are surging around the United States! Recently, Mastercard released its first-quarter results indicating card-not-present and

contactless payments surged by 40%. PayPal also reported that it added 20.2 million new accounts, bringing the company’s total volume of accounts to over 300 million. Venmo, a P2P platform owned by PayPal, also saw increased traffic—users transacted approximately \$31 billion just in the first three months of the year.

People want more than just digital payments, though—they also want instant payments. The Clearing House recently announced an expansion of its RTP® Network to include new partners, like Paychex, that will give more employers greater flexibility to deliver real-time payments and support the growth of on-demand services, like delivery or shared apps.

All these facts reveal that more Americans, including many who likely had limited experience with mobile or contactless payments before COVID-19 hit, are seeking electronic payment options to help them meet their needs. Although your business may not have started the year with plans to enhance or expand your payment technologies or products, you probably now find your clients expecting better digital payment experiences and services. Reach out to your financial institution to discuss your options regarding new product implementation and what makes the most sense for your clients. 🟢



Are you ready for ACH Rules changes coming in 2021?



- Fraud Detection for Web Debits
- Same Day ACH Expansion
- Data Security Requirements

Attend EPCOR’s *Payment Systems Update* seminar in the spring!
Watch epcor.org for details.

I Went to Prison for SBA Loan Fraud: 7 Things to Know When Taking COVID-19 Relief Money

by Jeff Grant, Prison Minister, Entrepreneur Contributor

This article originally appeared on May 12, 2020 on Entrepreneur.com.

In the months after 9/11, I was frantic. But, my fears had less to do with the tragedy at the World Trade Center and more to do with the fact that, after 10 years of rampant prescription opioid abuse, my business was failing. I was searching desperately for an out. Meanwhile, the

In 2002, I resigned my law license and started on the road to recovery. But it all caught up with me about 20 months later, when I was arrested for the misrepresentations on my loan application. I served almost 14 months at a Federal prison for wire fraud and money laundering.

My objective in writing this piece is to offer some insight on what business owners should consider before they take out disaster loans. Certainly, the majority of people requesting these loans are honest and upstanding entrepreneurs who have immense need for the

judgment or just plain bad luck, people were wounded, desperate and willing to do anything, anything, to stop the bleeding. But if the wound is too deep, a Band-aid is not sufficient.

Practice point: In any situation, behaving desperately is unlikely to save your business.

2. Beware of the belief that rules are suspended in times of emergency.

The government is advertising that huge amounts of money are available to save our businesses. I recently sat in on a webinar run by a very reputable business consulting group



television and radio were blaring with ads for 9/11 Federal Emergency Management Agency (FEMA) loans administered by the U.S. Small Business Administration (SBA).

So, on an especially bad day, I lied.

I said I had an office near ground zero. I received the SBA loan I requested, and immediately paid down the personal credit cards I had run up while waiting for the SBA money. Even so, the loan did little to stop my spiral into drug addiction, mental health issues, marital problems and magical thinking.

aid and will use the funds properly. I am very glad there is help for them. That said, history has shown us again and again that when people are in dire need, they're more prone to make impulsive, ill-advised decisions. My hope is that sharing my experience will help others avoid the consequences I faced. Here are seven takeaways.

1. Desperate people do desperate things.

There were thousands of fraud prosecutions after 9/11, Hurricane Katrina, Superstorm Sandy and so on. Why? Whether because of overwhelming business issues, poor personal

that recommended that attendees get their SBA disaster loan applications in immediately, regardless of the facts or the actual needs of their business—they said we could always modify our applications prior to taking the money. State unemployment websites are actually giving instructions, in writing, on how to mislead and circumvent the system in order to get approved. Don't take the bait! If you default two years from now, this "good-meaning advice" won't matter to prosecutors.

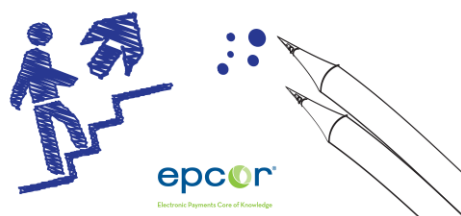
Practice point: Be truthful at all times.

see PRISON on page 6

PLAN NOW TO Advance Your Payments GOALS FOR 2021!

- Start accepting new payment 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 of these challenges for 2021 (or anything else not on this list) reach out to EPCOR (800.500.0100 or memserve@epcor.org) to find out how we can help!



THIRD-PARTY SENDERS MUST COMPLETE AN ACH COMPLIANCE AUDIT BY DECEMBER 31ST

EPCOR's Third-Party Sender ACH Audit workbook will walk you through the process. Or, contact Amy Donaghue at AmyD@epcor.org for a no-obligation quote on your professional audit service.



PRISON continued from page 5

3. Beware of magical thinking.

This is a tough one because entrepreneurs are inherently optimistic. We believe that things will always be better tomorrow than they are today. It drives us, makes us successful, informs our risk-taking. But in times of trauma, that voice can be an entrepreneur's worst enemy. Does this sound familiar? We have learned the hard way that there is no shortcut, and yet we desperately want there to be one right now.

Practice point: Instead of immediately reaching for a bailout or other quick fix, develop a good solid business plan. Maybe a disaster loan will fit into this plan; maybe it won't.

4. This paradigm shift will affect all small to mid-size businesses.

We are in the midst of a massive reordering that has already had a huge effect on small and mid-sized businesses. Business owners are being called to closely examine if our business models are still viable, or if we must pivot to new ways of doing things. Example: the Swiss watch industry completely missed the shift to digital watches. Have we waited too long to have a robust online presence? Are our products or services even needed anymore? Have we been holding on by a thread for years, unwilling or unable to look at the hard facts?

Practice point: Get real, now. Don't borrow money to save a business that can't be saved.

5. Be cautious when borrowing from the government.

As is the case with any loan, the devil is in the details. The terms and covenants in the loan documents dictate what you can or can't do with the money once you get it. You can only use the funds for the purposes you stated in your application—that is, to pay operating expenses of the business to keep it afloat until it starts bringing in sufficient revenue again. You (and your spouse) will probably

have signed for the loan personally, and will probably have to pledge all available collateral, including a second (or third) mortgage on your house. If you maxed out your personal credit cards while anticipating your disaster relief funding, you can't use the money to pay off your cards.

Practice point: Read the terms and covenants of the loan closely. Whatever the loan terms say to do, do that. And whatever they say don't do, don't do. No exceptions.

6. We can't save our businesses and our lifestyles at the same time.

Here's the big trap. We have mortgages, car payments, school tuitions and other personal expenses that have to be paid, and soon. But simply put, [SBA loans](#) are meant to save your business, not your lifestyle. Discuss all your options with advisors and friends you trust—ones that will tell you the truth! It's like going to the doctor. Your diagnosis will only be as accurate as the history you provide. These are trying times, with a triage system designed to be more expeditious than thorough.

Practice point: There is no such thing as a free lunch. Borrowing money comes with responsibility and accountability.

7. Get acquainted with acceptance.

I hope we are all great entrepreneurs who can figure out ways to make our businesses survive and flourish. But let's face it. Some of our businesses will not make it, even with the infusion of government funds. What should we do? We can pare down, embrace change and do things differently as we start a new chapter. Never forget that there will always be opportunity to start again, and to live a fuller, more abundant life.

Practice point: Sometimes less is way, way more! 🍀

Source: *Entrepreneur.com*

Protecting Small Businesses from Fraud

by Shelly Lingor, Partner at
GunnChamberlain, P.L. and Jeannie Ruesch,
Director of Marketing at Bill.com

This article originally appeared on August 13, 2020 on CPAPracticeAdvisor.com.

Many small businesses like to think that their size insulates them from fraud. Though, the opposite is true – small businesses are big targets for would-be fraudsters. According to the [ACFE Report to the Nations](#), small businesses are two times more likely to experience billing and payment fraud and four times more likely to experience check and payment tampering as compared to their larger counterparts. Too often, small businesses lack the necessary security measures to protect against fraud, making it easier for perpetrators to breach the company's financial systems.

The ways small businesses have been handling their bookkeeping and accounting for years are quickly becoming obsolete. Antiquated and manual processes leave small businesses vulnerable to fraud from both the inside and the outside. Reducing fraud starts with understanding your vulnerabilities and instituting the changes needed to secure your business.

Top Vulnerabilities Facing Small Businesses

Business vulnerabilities go far beyond someone trying to steal your credit card number or login credentials for financial sites, though those things still happen. Fraudsters routinely steal bank information from paper checks and use it to make fraudulent transactions. At businesses without stringent approval processes, employees or outside infiltrators can send illegitimate invoices through AP and receive payment through a

shadow company. Scammers are also spoofing employee identities to make fake transactions seem legitimate and even blame the fraud on innocent staff members.

Even the most business-savvy small business owners can fall victim to fraud.



Barbara Corcoran of Shark Tank was [scammed out of nearly \\$400,000](#) in an email phishing scheme. Using a spoofed email address for Corcoran's assistant, the scammer sent a fake invoice to Corcoran's bookkeeper, provided legitimate-seeming answers to the bookkeeper's questions and obtained payment. Although news coverage didn't disclose the internal processes Corcoran's company had in place for invoice approvals, the scam illustrates a classic example of how more robust workflows for processing and approving invoices will help stop fraudsters, who are constantly evolving their tactics.

These external actors aren't the only drivers of fraud at small businesses. Internal vulnerabilities leave small businesses open to fraud every day. Think of your current bookkeeping workflows and who controls them. Many small businesses use a long-time bookkeeper or office manager, who is the only person who knows the business's login information, links and processes for completing crucial bookkeeping tasks. What happens if that person leaves or can't work? When the sole handler of AP is gone, it can take businesses weeks to sort out their processes and set up new, secure procedures and that's if they have an expert AP vendor assisting with recovery. In contrast, if you use controlled, automated AP solutions from the start, it's easy to delete users and set new users up in designated roles with the appropriate access rights.

Top Three Reasons Companies Are Resistant to Change

Accountants hear the same reasons time and time again for why clients don't want to change the way they handle bookkeeping and AP. These reasons, though, are easily debunked.

1. **I don't want people seeing my business on the cloud.** The cloud doesn't let people see your business, especially if you use automated accounting software that lets you limit who can view or access specific information. Do you know what does let people see your business? Vulnerable and outdated processes that allow them to gain access to your bank account.
2. **The cloud isn't safe.** Nothing is 100% secure, but the cloud is far more secure than manual processes. Paper records and local desktop files can be lost in

[see FRAUD on page 8](#)

FRAUD continued from page 7

any number of ways, including fire, flood, theft or hardware failure. Cloud applications, in contrast, include sophisticated security protocols, and cloud providers have teams dedicated to installing and updating security patches. Cloud-based applications offer lower risk when it comes to maintaining your sensitive financial data.

3. **Our company made an investment in QuickBooks 10 years ago, so we're already using solid accounting software.** Desktop software platforms need to be updated regularly. Just as you're constantly upgrading and updating your smartphone and personal devices, you need to stay on top of your accounting and other business software. Any investment in security is ongoing. A benefit of cloud-based applications is that they usually work on a subscription basis and include constant security updates and upgrades with new security features.

Society has changed, and new fraud schemes surface all the time. Small businesses must adapt along with them and always be prepared for the unexpected.

Time for Change

Businesses can't run the same way they did 20 years ago. Those that resist change do so to their own detriment.

It's not just the scammers who are evolving. Your clients and vendors are also

changing how they do business. Therefore, your business must also adapt, even if it's in steps. Particularly in the time of COVID-19, businesses need to be paying extra attention to infrastructure security as virtual work capabilities are now mission-critical.

Start by cutting out inefficiencies and high-contact tasks such as sending paper checks. Focus your staff on high-value work that requires human input, as opposed to data entry and other routine tasks. Moving to cloud-based accounting tools removes tedious, manual processes and creates small efficiencies that can have significant, positive effects on company cash flows and more.

Six Critical Moves to Make Right Now

The good news is that there are a number of changes small firms can start implementing today to stop fraud in its tracks.

1. Create audit trails that track every click and every dollar down to the individual who performed the action.
2. Establish checks and balances to control the movement of funds. Ensure that the same person taking payments isn't also responsible for making payments; if that's not possible, add oversight.
3. Use smart, automated workflows to remove manual tasks from your processes.
4. Shift to online tools that enable virtual work. If your processes rely on your team sitting together, you need to make major adjustments to accommodate the realities of the new normal.

5. Build a long-term relationship with a trusted strategic advisor who knows your business, can help you make big decisions and can advise you on issues related to technology workflows.
6. Don't take anything for granted. The last 20 years have shown us that anything can happen, from major global events to more localized natural disasters. Your business must be prepared for whatever occurs. Recent global events have highlighted how critical it is for people to be able to conduct business remotely. Ideally, you've put those tools and processes into place so you can use them in times of crisis. Be prepared with technology that will work to your advantage and reduce impacts on your company.

Fraudsters will continue to attack small businesses, but your business doesn't have to be their next big payday. By recognizing your vulnerabilities and instituting the changes and new technologies necessary to address them, you'll be positioned to handle the threats that arise in the future. 🟢

Source: *CPAPracticeAdvisor.com*



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.

© 2020, EPCOR. All rights reserved.

www.epcor.org

3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665