


INSIDE: 2016 *ACH Rules* Changes That Could Impact You.....pg. 1
 Direct Deposit and Direct Payment via *ACH* - Simple Solutions with Complex Benefits.....pg. 1
 EMV Adoption Remains Sluggish.....pg. 1
 Same Day ACH for Businesses Essentials Guide.....pg. 3
 Study Examining Corporate Payments Strategies Finds Surprising Results.....pg. 3
 5 Ways Small Businesses Can Protect Themselves from Cyber Attacks.....pg. 4
 Third-Party Sender Registration Rule Passes.....pg. 5

Top 4 Facts Businesses Need to Know About the Unauthorized Entry Fee Rule.....pg. 6
 IRS Warns of Fake Tax Bills.....pg. 7
 Virtual Cards Start Living Up to Their Name.....pg. 8
 Is Your Business Considering Mobile Payments?.....pg. 8
 Why Understanding Your OFAC Compliance Requirements is So Important.....pg. 9
 Changes to Card Processing Will Aid Merchants and Consumers Alike.....pg. 11
 Same Day ACH Sweeps in to Save the Day.....pg. 12

2016 *ACH Rules* Changes That Could Impact You

This fall marks the implementation of two significant *ACH Rules* changes with September 23 marking the effective date for the Same Day ACH Rule, and October 3rd being the implementation of the Unauthorized Entry Fee Rule. And, there have been other changes in 2016 as well. If

you missed the *2016 ACH Rules Update for Originating Companies* that was distributed early this year, ensure your compliance by [downloading](#) it now. You may also be interested in the [Special Same Day ACH Edition](#) of *Inside Origination* that came out in June. 

Direct Deposit and Direct Payment via *ACH* - Simple Solutions with Complex Benefits

Has your business already embraced the benefits Direct Deposit and Direct Payment via *ACH* can provide? Are you reaping all the benefits it has to offer? Or are you still waiting to take the step, not sure it's right for your organization? Wherever you may be in the decision-making process, Direct Deposit and Direct Payment via *ACH* can help grow your business, provide security and really impact your bottom line. Here are just a few reasons to consider implementing these valuable tools right away.

Direct Deposit for Businesses

Direct Deposit via *ACH* transfers funds electronically from your business account directly to your employees' accounts. Enroll your employees, shareholders, or retirees and eliminate manual check preparation and record keeping. Among the many benefits this mechanism provides are:

- **Helps Grow Your Business**—Direct Deposit lets you free up time, money and energy to grow your business. Quick and easy payments, consistent [see DIRECT on page 2](#)

EMV Adoption Remains Sluggish

The Strawhecker Group (TSG), a management consulting firm focused on the global payments industry, released survey results this week that estimate 44% of U.S. card-accepting merchants have EMV terminals. TSG also found that less than a month away from the October 1 anniversary of the EMV liability shift, only 29% of U.S. merchants are actually able to accept chip-based transactions.

TSG's previous survey of payment processors and other payment providers completed in January estimated that more than 50% would have an EMV terminal by this time, showing a slower pace of implementation than expected.



see EMV
on page 2

EMV continued from page 1

“EMV merchant adoption has slowed down a bit, at least comparatively speaking to our last EMV survey results in January 2016,” said Jared Drieling, business intelligence manager at TSG. Approximately one-third of merchants have activated EMV POS systems despite the larger base of U.S. merchants with EMV terminals in place. “EMV terminal vendor supply and delays in the terminal activation/certification process are the

bottlenecks in the migration,” he said.

By December 2016, it is estimated that consumers will be able to use their chip-based credit and debit cards at 51% of U.S. merchant locations, according to TSG. “It is also important to note that EMV adoption by ... industry can vary drastically; for example, quick-service restaurants are suspected to be laggards in the transition,” Drieling added.

The survey also indicated that more than 60% of respondents have experienced an

increase in the number of chargebacks due to a lack of EMV compliance. “It is clear that non-EMV compliant merchants have felt the impact of the liability shift. The good news is that as merchants refresh their terminals for EMV, they are also adopting the contactless capability [that] lays down the foundation for future payments such as mobile proximity payments,” Drieling said. 🌱

Source: NACSONline.com

DIRECT continued from page 1

cash flow, increased efficiency, faster error resolution and cost savings are all by-products of this versatile service.

- **Increases Your Savings**—Direct Deposit eliminates paper checks, saving you money on everything from postage to mailing supplies to staffing resources. And it's not just for payroll. Direct Deposit can be used for bonuses and commissions, child support payments, dividend/interest payments, pension disbursements, travel reimbursements and more.
- **Builds Employee Satisfaction**—Your employees want Direct Deposit *via ACH*, and why wouldn't they? No standing in line at their financial institution on Friday nights, no coming in to pick up their check when they are on vacation. Their payroll goes straight into the account (or accounts) they have designated. Eighty-seven percent of employees who use Direct Deposit are highly satisfied with the service, and employees who are paid by Direct Deposit rate their employers a 9 out of 10 for supporting this service.
- **Provides Security**—Unlike paper checks, which pass through many hands, Direct Deposit *via ACH* transactions are safe and secure; account numbers remain secure. And ACH transactions don't get lost in the mail. Everyone wins.

Direct Payment for Businesses

By implementing Direct Payment in your business, you can automate your accounts payables by making electronic payments to your vendors and service providers. This can allow for better cash flow management and easier reconciliation and reporting.

The logo for Direct Deposit via ACH features a stylized icon of a check with an arrow pointing up and another pointing down, symbolizing a cycle or direct flow. To the right of the icon, the word "DIRECT" is written in a bold, yellow, sans-serif font. Below "DIRECT", the word "DEPOSIT" is written in a larger, bold, dark grey, sans-serif font. Underneath "DEPOSIT", the words "via ACH" are written in a smaller, dark grey, sans-serif font, flanked by two horizontal lines.

The logo for Direct Payment via ACH features a stylized icon of a check with an arrow pointing up and another pointing down, symbolizing a cycle or direct flow. To the right of the icon, the word "DIRECT" is written in a bold, yellow, sans-serif font. Below "DIRECT", the word "PAYMENT" is written in a larger, bold, dark grey, sans-serif font. Underneath "PAYMENT", the words "via ACH" are written in a smaller, dark grey, sans-serif font, flanked by two horizontal lines.

Additionally, you can collect payments from your customers electronically, saving administrative costs, enabling more accurate forecasting and providing your customers with safe, cost-effective and fast payment options that are also good for the environment.

Direct Payment *via ACH* is ideal for:

- Cash concentration and disbursement;
- Charitable donations and recurring gifts;
- Consumer bill payments;
- Vendor and supplier payments.

As with Direct Deposit, using Direct Payment *via ACH* keeps your business transactions secure. Because money is transferred directly between accounts, risks of fraud and identity theft are reduced.

Want to learn more about Direct Deposit and Direct Payment *via ACH*? In the Spring of 2017, NACHA released a white paper [Beyond Simple and Safe: Opportunities to Expand the Use of Direct Deposit via ACH for Payroll](#), which detailed the top reasons employees use Direct Deposit *via ACH*, including faster access to pay, lower cost and the elimination of the risk of losing a paper check.


This informational [website](#) provides a wealth of information, as well as calculator tools for both [Direct Deposit](#) and [Direct Payment](#) to see exactly how much you can save. Contact your financial institution to move your business into the 21st century through Direct Deposit and Direct Payment *via ACH*. 🌱

Source: NACHA

Same Day ACH for Businesses Essentials Guide

NACHA – *The Electronic Payments Association*, has produced a *Same Day ACH for Businesses Essentials Guide*. This suite of resources provides key guidance on Same Day ACH opportunities, benefits and value to businesses and action plans for sending and receiving same-day payments. The “Essentials Guide” includes:

- [Same Day ACH for Businesses Overview/PowerPoint](#)
- [Same Day ACH for Businesses Infographic](#)
- [Same Day ACH for Businesses Hire-to-Retire Essentials List](#)
- [Same Day ACH for Businesses Order-to-Cash Essentials List](#)
- [Same Day ACH for Business Procure-to-Pay Essentials List](#)

For more information on the current phase of Same Day ACH, as well as what lies ahead, be sure to visit EPCOR's [Same Day ACH Portal](#). 

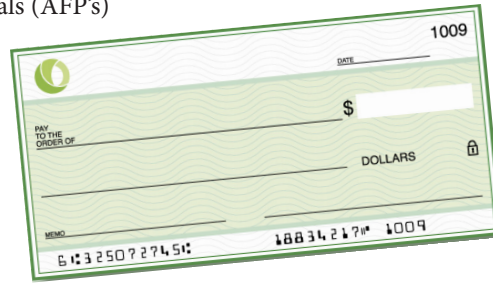
Source: NACHA

What Do You Really Need to Know?

EPCOR's *Same Day ACH: Originator Fundamentals* recording explains everything businesses need to know about Same Day ACH in non-technical terms from considerations of receipt of Same Day ACH transactions to possible consequences of sending stale-dated entries. Contact your financial institution for more information on purchasing this cost-effective and informative tool.

Study Examining Corporate Payments Strategies Finds Surprising Results

Amid the rollout of Same Day ACH—in the midst of several other faster, digital payments initiatives and in a market where Business to Business (B2B) payments seem to finally be getting smarter—the Association of Financial Professionals (AFP's) latest research finding an uptick in corporate use of paper checks leads to one question: What the heck is going on?



Check Use Up

Two revelations emerged from the AFP's *2016 Electronic Payments Survey*. First is that the use of paper checks by corporates increased from surveys in the past, reversing the downward trend of check popularity seen previously. The second is that the 1% increase in check use once again bumped the payment rail to the most popular payment method for corporates at 51%.

“That really got me as a big surprise,” AFP's manager of treasury and payments, Magnus Carlsson said. “Given everything that we hear and talk about, all of these efforts to go away from paper checks, yet we see they're very resilient. That makes me think we have to talk a bit about how we approach this topic. You can't just say, ‘You should get away from checks.’”

Indeed, it appears as if the research—from AFP and others—that highlights the cost and lack of security associated with paper checks hasn't deterred businesses.

That research, Carlsson argued, should mean companies can build a business case to ditch checks and adopt electronic payments, making the survey's results that

much more surprising.

It's unclear, though, whether that 1% increase for 2016, up from 2013, signals a trend of rising check use or whether it's simply an anomaly for this particular report.

But considering the electronic payments initiatives underway, the AFP executive said he's fairly certain the next time the report comes out, in

2019, there will again be

a decline in check usage—though he can't say for sure.

Faster Payments

The report uncovered some reasons why companies are reluctant to adopt electronic payments, with the cost of investing in that change standing as the top barrier, according to the survey.

“This is really what it comes down to, why we're still seeing a lot of checks,” Carlsson stated, adding another crucial part of the puzzle: With all of the faster payments initiatives in the works right now, some businesses say it may not make sense to invest in the shift to electronic payments now when better, faster solutions are ahead.

“Some of the corporates I've talked to say that they have such antiquated systems to handle checks that even starting to mess with it is going to lead to huge investment costs,” he explained. “It's a wait-and-see approach; they don't want to get into a big investment right now knowing there are faster alternatives on the horizon.”

“There is less incentive to change at this point, I think,” he added.

see **STUDY** on page 4

STUDY continued from page 3

Same Day ACH

True, there are faster payments initiatives in the works, but Same Day ACH is finally here, and the AFP did find evidence that corporates are planning to use it.

The most common ways to use Same Day ACH for businesses are likely to be for last-minute bill payments and emergency payroll, the survey found, though Carlsson noted the research was conducted before Same Day ACH's actual rollout, so it remains to be seen exactly how it will be used by businesses.

Carlsson said the faster payments tool offers businesses an alternative to wire transfers, which he said is traditionally used for emergency payments. And there is a possibility that Same Day ACH could infiltrate the supplier payment process, especially when it offers the opportunity to save money.

"If you have a supplier saying you can pay

quickly [using Same Day ACH], maybe you can get a discount from that," he explained. "If you have to pay a little extra, maybe the discount you get back is worth it."

What is certain, however, is that companies need to be prepared for the impact on cash flow Same Day ACH is likely to have, Carlsson said, noting that he's had extensive discussions with corporates about the ability for businesses to get money in faster than anticipated.

Even if they don't use Same Day ACH, if they're on the receiving end of a payment, that faster transaction means a change in how corporations manage the books.

"It's a good precaution to know this, so you're prepared, so if you get cash in quicker that you know where to put it," Carlsson stated.

"Check with business partners how they may pay you," he offered as advice. "If a business partner is really intent on using Same Day ACH, well, then, you need to be prepared for that." 🟢

Source: PYMNTS.com

Prove Your Check Expertise!

TAKE THE PREP COURSE THAT HAS PRODUCED NCP EXAM TOP SCORERS FOR THE PAST FOUR YEARS!

EPCOR'S NCP PREP COURSE KICKS OFF ON JANUARY 12



5 Ways Small Businesses Can Protect Themselves from Cyber Attacks

Every day, cyber attacks become a starker reality for all businesses and organizations—no matter the industry or size. While government, business leaders, and the media have been saying that cyber attacks are no longer a question of if, but when, the clamor isn't enough to minimize the harsh effects of these threats. Unfortunately for most, companies won't know they've been hacked until it's too late.

As data breaches continue to surface and cyber security incidents grow exponentially

in frequency, size, and cost, going at it alone is no longer an effective option. Preparedness requires a collective accountability—an understanding that all affected entities—consumers, businesses, financial institutions, regulators and the government—must prioritize cybersecurity so that together, we can create a safer environment. Cyber security is everyone's responsibility.

While we each have this responsibility to uphold, it's often harder for smaller organizations to secure themselves due to lack

see **ATTACKS** on page 5



Increase Your Cyber Security Awareness

Help keep the internet safe for all of us with these resources from the U.S. Department of Homeland Security and the National Cyber Security Alliance:

- Go go [StaySafeOnline.org](https://www.staysafeonline.org) to learn how you can make an impact
- Sign up to receive the Stop.Think.Connect.™ monthly Friends [Newsletter](#).
- Become an official partner of the [Stop.Think.Connect.™ Campaign](#). Get started by reviewing the [Stop.Think.Connect.™ Campaign Toolkit](#).

ATTACKS continued from page 4

of resources or even lack of awareness. It's not surprising, then, that small businesses have increasingly become the main target. In fact, 71% of cyber-attacks occur at businesses with fewer than 100 employees.

With October the official National Cybersecurity Awareness Month, there's no better time for small businesses to ramp up efforts right alongside their customers. A little education goes a long way:

1. Understand the Evolving Risks.

Cybersecurity preparedness starts with having a complete understanding of the internal and external vulnerabilities that can affect any business, how hackers can gain entry including their different methods and motives, and how to identify points of weakness. Learn the different types of cyber fraud schemes and common threats—everything from phishing and spoofing scams, social engineering, malware, systems hacking, pharming and everything in between.

2. Develop a Security Policy That is Ingrained into Corporate Culture.

Defining protocols to abide by is critical, but in order to be effective, the policy must permeate throughout every process, every decision and the whole mentality of the organization—squarely embedded into its overall business strategy and how each employee operates. After all, your employees are the gatekeepers of your company's information, making them the first line of defense against corporate account takeover. Educate your employees about the warning signs, safe practices and responses to a suspected takeover. Make sure they use complex, unique passwords and maintain a "clean desk environment" where personal and confidential information aren't exposed.

3. Pick Up the Phone.

Verify financial requests and confirm details by phone instead of relying on email to initiate or complete any financial transaction—whether you are dealing with your financial institution, vendors, clients or employees.

Use a two-step verification process

to add another layer of security to approving outgoing funds—it will help protect you from a loss.

4. Keep Your Software Current.

Don't delay updating your anti-virus software or other security applications. Up-to-date software will help you guard against the latest threats and keep your infrastructure secure.

5. Have an Incident Response Plan and Practice It.

Just like a fire drill, having a plan of action for responding to a cyber incident is crucial. Even more important, it should be practiced so that all your employees know exactly what to do in the event of a breach.

As cybercrime escalates and protection and preparedness become increasingly important for every organization, it's ultimately working together that will bolster the ability to combat mounting threats. In an environment where hackers are often one step ahead, a collective accountability can be our first line of defense. 🌱

Source: Forbes.com

Third-Party Sender Registration Rule Passes

NACHA's voting membership passed the Third-Party Sender Registration Rule in August, and the Rule goes into effect September 29, 2017. This rule will require Originating Depository Financial Institutions (ODFIs) to identify and register their Third-Party Sender customers.

If you are a Third-Party Sender, your financial institution will be required to provide basic registration information with NACHA, including:

- the financial institution's name and contact information;
- the name and principal business location of the Third-Party Sender;
- the routing number used in ACH

transactions originated for the Third-Party Sender; and

- the Company Identification(s) of the Third-Party Sender.

To aid financial institutions in collecting registration information, the Rule obligates Third-Party Senders to provide their financial institutions, upon request, with any registration information needed. Further, in order to aid financial institutions with due diligence regarding nested Third-Party Sender relationships, the Rule requires Third-Party Senders to disclose to their financial institutions any other Third-Party Senders for which they transmit ACH entries.

In certain circumstances, NACHA

see VOTE on page 6

Join EPCOR's Third-Party Sender Forum!

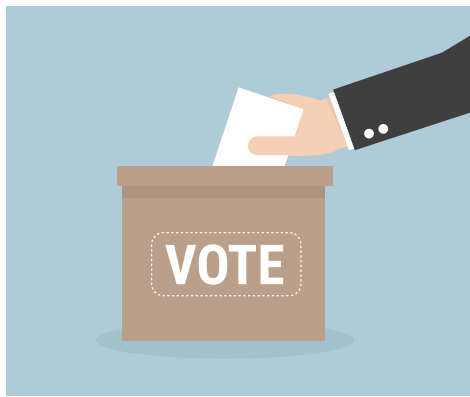
EPCOR's Third-Party Sender Forum is open to all Associate members of EPCOR, allowing for a unique space to collaborate on issues important to Third-Party Senders, discuss best practices for meeting compliance requirements and voice industry concerns to EPCOR.

To learn more about EPCOR's Third-Party Services, Third-Party Sender Forum or the Third-Party Guiding Principles that forum members pledge to abide by contact Kimberly Martin at KimbleryM@epcor.org.




VOTE continued from page 5

would be authorized to request additional information about the Third-Party Sender. This could happen in regard to risk events, which the Rule defines as “cases in which it (NACHA) believes that a Third-Party Sender in the ACH Network poses an escalated risk of (i) financial loss to one or more Participating financial institutions, Receivers or Originators, (ii) violation of the Rules or



Applicable Law, or (iii) excessive Returns.”

Third-Party Senders could possibly incur some direct costs to assemble and provide required information to their ODFIs. Because the information is basic in nature, NACHA does not expect these costs to be so significant as to outweigh the benefits of the Rule.

For additional information, see the [FAQ section of NACHA's website](#). 

Top 4 Facts Businesses Need to Know About the Unauthorized Entry Fee Rule

by Karen Sylvester, AAP, CRCM, NCP,
Director, Risk & Regulatory Compliance

In light of this fall's new Unauthorized Entry Fee Rule, here is a list of the 4 most important facts every business needs to understand about the new Unauthorized Entry Fee Rule.

When does the Unauthorized Entry Fee go into effect?

October 3, 2016 marked the implementation of the Unauthorized Entry Fee Rule for all financial institutions participating in the ACH Network. This fee will be associated with any transaction that is returned as unauthorized on or after October 3, 2016. With that being said, a transaction originated prior to that date but returned on or after that date will also be subject to the fee. The fee is paid by the Originating Depository Financial Institution (ODFI) to the Receiving Depository Institution (RDFI) for any transaction returned with an unauthorized Return Entry Code. The unauthorized return codes include R05, R07, R10, R29 and R51.

How is the Fee Amount Determined?

The Rule defines a methodology by which NACHA staff will set and review



the amount of the Unauthorized Entry Fee every three years. In setting the amount of the fee, NACHA staff will apply the following principles:

1. NACHA will conduct a representative survey of RDFIs of various types and sizes to determine the expense incurred in handling and returning unauthorized Entries.
2. The amount of the Unauthorized Entry Fee will be set at a level that is less than the weighted average cost determined by such a survey.
3. The Unauthorized Entry Fee will be set at a level that NACHA staff reasonably believes will provide an incentive for participating financial institutions to

improve the quality of ACH processing without unduly discouraging participation in the ACH Network; and


4. In re-evaluating the amount of the Unauthorized Entry Fee, NACHA staff will consider the extent to which the existing fee amount has affected return rates.

Can this Fee Impact My Business?

Yes. The *ACH Rules* do not provide any guidelines for financial institutions to pass the fee onto their Originators. Nor does it prohibit this practice. However, the fee should be disclosed to the Originator through the Fee Schedule in the ACH Agreement.

What if We Have a Valid Authorization? Is there still a fee?

Unfortunately, there is still a fee for the return. The Originator may pass those fees onto the consumer based on notices provided to the them. If there is valid authorization for the transaction, the issue should be resolved between the Originator and the Receiver, and no additional transactions should be sent through the ACH Network without proper authorization.

EPCOR has created a [Frequently Asked Questions Document](#) for businesses to provide additional details. 

EXPLORE EPCOR MEMBERSHIP

EPCOR has membership opportunities for companies, businesses, corporations and Third-Parties.

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

EXPLORE EPCOR

IRS Warns of Fake Tax Bills

The Internal Revenue Service and its Security Summit partners recently issued an alert to taxpayers and tax professionals to be on guard against fake emails purporting to contain an IRS tax bill related to the Affordable Care Act.

The IRS has received numerous reports around the country of scammers sending a fraudulent version of CP2000 notices for tax year 2015. Generally, the scam involves an email that includes the fake CP2000 as an attachment. The issue has been reported to the Treasury Inspector General for Tax Administration for investigation.



The CP2000 is a notice commonly mailed to taxpayers through the United States Postal Service. It is never sent as part of an email to taxpayers. The indicators are:

- These notices are being sent electronically, even though the IRS does not initiate contact with

see **FAKE** on page 12



epcor®
Electronic Payments Core of Knowledge

2017 PAYMENT SYSTEMS UPDATE

ACH **Rules** **CFPB** **Fraud Trends**
Card **Reqs** **Third-Party** **Check** **Real-Time**
ISO 20022 **Registration** **Payments**

Join us at one of more than 50 *Payments Systems Update* locations this February and March for your payments update.

Virtual Cards Start Living Up to Their Name

Virtual cards have a dirty little secret, and the Business to Business (B2B) payments space is beginning to catch on: For a technology that's touted as an all-electronic way for corporates to pay, virtual cards sure do involve a lot of paper.

Most of the time, that paper comes in the form of a fax with virtual card information sent to a supplier via the technology of the early 90s. Email, analysts said, was supposed to wipe the fax machine off the market entirely, but alas, the fax lives on.

When it comes to virtual cards, fax machines have been a crucial part of getting card information into



the right hands. And representative of its failure to knock down the fax machine, email, unfortunately, wasn't capable of sending virtual card information to suppliers until only recently.

According to corporate payments technology company Conferma, that's because email wasn't held to the security standards necessary to transmit such sensitive data.

"Email servers didn't have the level of encryption capability required to transit a

Is Your Business Considering Mobile Payments?

Mobile payments have actually been around for a few years now, but have only recently made the kind of impact that makes consumers and businesses take note. Unsurprisingly, mobile payments refer to financial transactions that are performed using a mobile device, most commonly a smartphone. As an alternative method of payment to debit cards or cash, mobile payments have gained in popularity all over the world, with businesses ranging from tech giants to independent startup all vying for market share in this fledgling industry. As with any other new technological phenomenon, mobile payments are sure to create as many disruptions as opportunities, so it's vital that businesses carefully manage the introduction of new payment platforms.

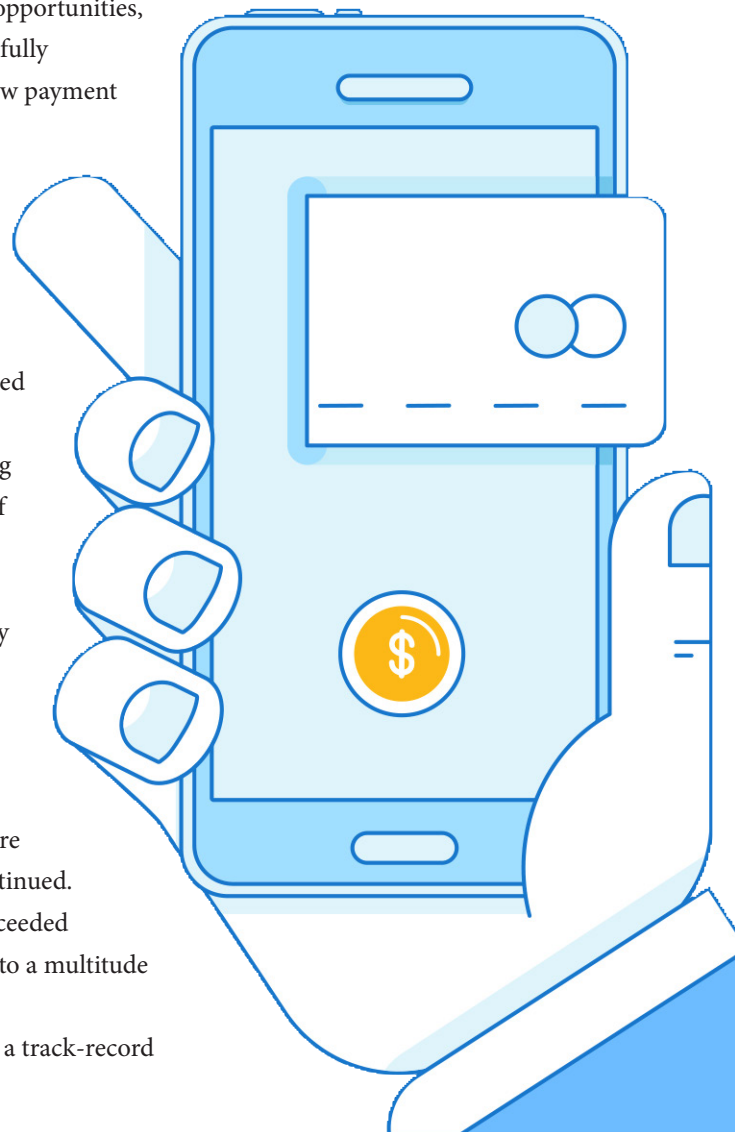
Apple Pay Kicks Things Off

Although Apple Pay was not the first mobile payments platform, Apple is being credited with kick-starting the mobile payments explosion. According to CEO Tim Cook, in excess of one million credit cards were registered to Apple Pay within three days of its U.S. launch. By contrast, prior to the Apple Pay launch a number of other mobile payments platforms struggled to make much of an impact and some, like Square Wallet, were eventually discontinued. The reason why Apple has succeeded where other have failed is due to a multitude of factors.

Firstly, Apple has developed a track-record

for bringing innovation into the mainstream, even when they can't claim to have come up with the idea themselves. MP3 players, smartphones, wearables and now mobile payments have all benefitted from the consumer attitude towards Apple products. Moreover, Apple made sure they created a service that had convenience as its number one concern. Apps like Google Wallet may have existed prior to Apple Pay, but cannot claim to be as intuitive. Google Wallet, for example, required consumers to take their phone out of standby mode and enter a PIN when they wanted to make a transaction.

see MOBILE on page 9



MOBILE continued from page 8

With Apple Pay, users simply press their phone against a payment terminal and let Touch ID verify their identity.

Lastly, the success of Apple Pay in the mobile payments market is also the result of good timing. Other mobile payment businesses were guilty of trying to implement their ideas too soon, particularly when Near Field Communication (NFC) hardware was not mainstream enough to facilitate transactions. Time is also crucial for getting consumers on-board. It now seems completely natural that we would make transactions and carry out bank transfers with our smartphones, but go back a few years and the public were less receptive.

Although Apple Pay is pleased with its initial popularity, competition is mounting. Top contenders include Samsung and Android Pay as big players, and a myriad of smaller players including Bolt, Cover and Coinbase, to name a few. It's an open landscape and more players are joining the game.

Security Concerns

If there is one major hurdle that mobile payments must overcome if they are to


continue their upward momentum it regards security. While fingerprint recognition and PIN authorization can help secure point-of-sale (POS) transactions, online purchases are still being targeted by fraudsters. The use of biometric authorization for online sales has been mooted, but it remains to be seen whether this will gain much traction. Of course, for businesses like Google, Apple and anyone else in the mobile payments space, security must become a number one priority. As well as financial repercussions in the form of fines and compensation, a data breach could lead to long term reputational damage.

Perhaps the biggest security hurdle that mobile payments have to overcome is one of perception. Although progress is being made, consumers may still view mobile payments as being inherently less secure than debit cards or cash. Over time this is likely to change, particularly if mobile payment firms continue to introduce robust security protocols like multi-factor authentication and tokenization.

Innovate or Risk Irrelevance

For businesses looking at the growth of mobile payments, it is important that they do not dismiss the phenomenon. Even financial

institutions, with their long-established methods, are beginning to realize the importance of innovation. Mobile payments are hugely convenient for customers and the introduction of loyalty points and rewards for mobile transactions is only likely to increase the popularity of paying by phone. Smartphone applications are also realizing that mobile payments can help them to monetize their services. Businesses are offering “buy” buttons alongside their mobile ads to streamline transactions. It is likely that further revenue streams will also become available as the mobile payment market develops.

Some retailers in the U.S. and UK have been reticent to accept mobile payments, particularly if they need to invest in new hardware, but this investment is unlikely to go unrewarded. If businesses can use mobile payments to deliver quicker, more reliable transactions to their customers, then everyone stands to benefit. Cash and cards may not be overly worried about being overtaken by mobile payments just yet, but continuing developments will only see this technology go from strength to strength. 

Source: *ITProPortal.com*

Why Understanding Your OFAC Compliance Requirements is So Important

OFAC is the acronym for the Office of Foreign Asset Control. OFAC compliance is critical for U.S. businesses working with overseas partners; the regulations are in place in part to ensure that companies don't unwittingly do business with terrorist organizations or other unsanctioned entities.

The increasing possibility that U.S. businesses, no matter how small, will have foreign suppliers or clients, makes it imperative that they understand what the Office of Foreign Asset Control Compliance is. Businesses are responsible for following OFAC regulations

designed to halt terrorist and other illegal funds from circulating

If you are in an industry with significant foreign business, a small business owner, or an individual doing business, here are the top five areas to familiarize yourself with.

1. What OFAC Compliance Means

The Office of Foreign Assets Control administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either

comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals. All U.S. persons (which by legal definition includes firms) must abide by these sanctions.

2. Who Must Be in Compliance

All U.S. persons must comply with OFAC regulations, including all U.S. citizens and permanent resident aliens regardless of where they are located, all persons and entities within the United States, all U.S. incorporated entities and their foreign branches. In the cases of

see OFAC on page 11

VIRTUAL continued from page 8

credit card number,” explained Simon Barker, CEO of Conferma.

That posed a major problem for the virtual card industry, considering its focus on v-cards as a more secure way for companies to pay suppliers. Despite the paper-intensive process of sending a fax, the technology actually worked pretty well for virtual cards.

“In the past, the only real secure way of getting a virtual card number and sending across an open system that was ubiquitous was the fax machine,” the executive said. “That’s why, to a certain extent, the fax became a little unwieldy and not a 21st century payments technology—although, it does actually work. Transactions every day are done that way.”

The benefits of the virtual card, he said—greater control over who gets paid, for what, for how much, at what time—meant companies and their suppliers simply accepted the fact that, unless they had integrated an Accounts Payable Interface (API) to accept virtual cards, they would have to receive virtual card information to essentially process it as a card-not-present payment.

But according to Conferma, sending a fax that is compliant with Payment Card Industry Data Security Standards isn’t only inefficient; it’s expensive, costing a sender up to \$0.16.

Finally, email has caught up with greater security needs. It’s only recently that email servers can now support the level of encryption necessary to meet PCI standards, Conferma said, which has led the company to launch Conferma Connect, a process

that allows companies to send virtual card information to suppliers over email.

Conferma said it costs 60% less to send v-card information this way. But Barker also pointed to other benefits of this payment method.

“There is work that has to go into the sending process, in the verification of who you’re sending it to and the handshakes that go on between the different servers to ensure the right level of encryption,” the executive explained. Recipients of virtual cards need to opt in to receive payment info via email, while the platform must also verify that encryption capabilities are adequate.

“What you end up with is a process that drives significantly more security into the transmission process over email than you would have gotten in a fax,” Barker said. Plus, he added, email-based transmissions are more data-rich. “You can get a good audit trail about how it was encrypted, who it went to, what time — a lot of detail that you would not get in a fax,” the CEO explained.

Just The Beginning

Some industry players may argue that virtual cards have fallen short of their paperless promises. But Barker told PYMNTS that, even with a process that requires a fax machine, virtual cards have “revolutionized” corporate payments.

“The benefits of virtual cards outweigh that last mile where the fax machine is involved,” he said. “In terms of pure control, speed and automation, virtual cards are, head and shoulders, above anything else.”

But virtual cards remain far from the most common form of payment used by corporations to pay their suppliers. In part, that could be due to the reputation that virtual and other commercial cards have in terms of the expense imposed on suppliers to accept this form of payment.

Barker, however, argued that the speed at which suppliers get paid when paid via virtual card is worth the interchange fee.

“What we find with a lot of our customers is that they say to their supplier, ‘We’re going to pay you so much quicker by using virtual cards that the actual cost of the interchange you’ll have to bear is greatly outweighed by the benefit of getting the money so much faster into your bank account,’” Barker said, adding that v-cards can lessen the time it takes to pay a supplier from 30-plus days to just three.

The CEO is a major proponent of the technology, of course. Over the next decade, Barker predicts that virtual cards will experience massive adoption in B2B payments, especially considering that, compared to other payment technologies, virtual cards remain pretty nuanced.

“There’s a long way to go,” Barker stated. “But we’re seeing more banks wanting to be a part of our network, and more corporates want to use virtual cards than ever before. I think in just the next three to four years, it will become a standard way of making payments.” 🟢

Source: PYMNTS.com

Don't Waste Time with an Outdated ACH Rules Book in 2017!

Pre-Order Now to Get Your Copies Hot Off the Press this January.

[Click here to order your 2017 ACH Rules.](#)

• 2017 •
NACHA
Operating Rules
& Guidelines

Corporate Edition

epcor

NACHA

Changes to Card Processing Will Aid Merchants and Consumers Alike

Every time your business prepares its monthly billing, you face the challenge of automatic card payments being declined due to account changes that have not been communicated to you. Those declines can wreak havoc with your revenue flow and can increase expenses. In addition, consumer services may be disrupted. It's time to build that better mousetrap we always hear about.

As of October 1, 2016, VISA mandated that all U.S. card issuers are required to use the VISA Account Updater® Service. This service allows issuers and acquirers to be able to electronically send updated account information back and forth, benefitting merchants who process recurring payments. [The service](#) will be free to financial institutions at least until September 30, 2018.



MasterCard also provides a similar optional service, MasterCard Automatic Billing Updater. (Merchants interested in the MasterCard service will need to contact their acquirer/payment processor to determine any connectivity requirements and to schedule an implementation date. For additional information, please visit the “For Merchants” section of www.mastercard.ca.)

By automatically maintaining the accuracy of customer card data, these services prevent disruptions due to account changes, extending the life of online and offline automatic payment arrangements by helping to secure these ongoing, revenue-generating relationships, all while helping to lock in revenue, reduce processing costs, maintain service continuity, and strengthen cardholder satisfaction.

VISA has also issued two additional mandates, outlined below:

- October 14, 2016 - All U.S. VISA issuers of consumer credit, debit and reloadable prepaid cards must offer an alert service to their cardholders. These alerts can be delivered via SMS text or email (which may be customized by issuer). Issuers may provide this service utilizing a third-party solutions provider in order to meet the mandate.
- April, 2017 – A change to the Disputes Process will result in moving away from a litigation-based model to a liability-assignment model. This change includes:
 - [Consolidation of 22 chargeback reason codes](#) into four categories: Fraud, Authorizations, Consumer Disputes and Processing Errors.
 - New requirement to use the Transaction Query tool through VISA Resolve Online® to locate the original transaction prior to initiating a claim.
 - Two new processing paths for disputes: Allocation and Collaboration. The Allocation path will be used primarily to resolve Fraud and Authorization disputes and the Collaboration path “may” require more interaction among the merchant, acquirer and issuer.
 - Under the current model, disputes may take months to resolve. It's estimated that this processing change will result in an estimated 60-80% of disputes being resolved within 48 hours of submission. 🕒

Source: VISA and MasterCard

[OFAC continued from page 9](#)

certain programs, such as those regarding Cuba and North Korea, all foreign subsidiaries owned or controlled by U.S. companies also must comply. Certain programs also require foreign persons in possession of U.S. origin goods to comply.

3. Industry Specific Information

OFAC provides downloadable guidelines and FAQs for specific industries, including:

- Financial Sector
- Money Service Businesses
- Insurance Industry
- Exporters and Importers
- Tourism/Travel
- Credit Reporting
- Non-Governmental Organizations (NGOs)/Non-profit
- Corporate Registration

Additional details are available on the [OFAC Information for Industry Groups page](#).

4. OFAC Country and List-based Sanctions

OFAC Country Sanctions and List-Based Sanctions, including general licenses for exceptions; related documents; and laws, rules and regulations authorizing the sanctions are available on the [OFAC Sanctions webpage](#).

5. Specially Designated Nationals (SDN) List

OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list) which includes over 3,500 names of companies and individuals connected with the sanctions targets. A number of the named individuals and entities are known to move from country to country and may end up in unexpected locations. U.S. persons are prohibited from dealing with SDNs wherever they are located and all SDN assets are blocked. It is important to ensure you have a current [SDN list](#) for reference. 🕒

Sources: AboutNews.com and OFAC

FAKE continued from page 7

taxpayers by email or through social media platforms;

- The CP2000 notices appear to be issued from an Austin, Texas, address;
- The underreported issue is related to the Affordable Care Act (ACA) requesting information regarding 2014 coverage;
- The payment voucher lists the letter number as 105C.

A CP2000 is generated by the IRS when income reported from third-party sources such as an employer does not match the income reported on the tax return. It provides extensive instructions to taxpayers about what to do if they agree or disagree that additional tax is owed.

The fraudulent CP2000 notice includes a

payment request that taxpayers mail a check made out to “I.R.S.” to the “Austin Processing Center” at a Post Office Box address. This is in addition to a “payment” link within the email itself. True CP2000 forms ask that checks be made out to “United States Treasury” if the taxpayer agrees additional tax is owed. Or, if taxpayers are unable to pay, it provides instructions for payment options such as installment payments.

IRS impersonation scams take many forms: threatening telephone calls, phishing emails and demanding letters. Taxpayers or tax professionals who receive this scam email should forward it to phishing@irs.gov and then delete it from their email account.

To determine if a CP2000 notice you received in the mail is real, go to IRS.gov,

[Understanding Your CP2000 Notice](#), which includes an image of a real notice.

The IRS and its Security Summit partners—the state tax agencies and the private-sector tax industry—are conducting a campaign to raise awareness among taxpayer and tax professionals about increasing their security and becoming familiar with various tax-related scams. Learn more at [Taxes. Security. Together](#) or [Protect Your Clients; Protect Yourself](#).

Taxpayers and tax professionals should always beware of any unsolicited email purported to be from the IRS or any unknown source. They should never open an attachment or click on a link within an email sent by sources they do not know. 📧

Source: IRS.gov

Same Day ACH Sweeps in to Save the Day

When Same Day ACH became a reality on September 23, bringing expedited settlement to the over 40-year-old payment system, everyone was watching and waiting, wondering - when will we see this new offering put to work?

The wait wasn't long. Within days, NACHA – *The Electronic Payments Association* began sharing Same Day ACH success stories. And, barely one week into the new processing environment, EPCOR member UMB Bank, NA in Kansas City found success with Same Day ACH.

One of UMB's existing Originators—let's call them ABC Company—alerted UMB on the morning of October 3rd that they had missed sending in a file containing over 2,300 pension payments. Even though the company had not yet signed up for UMB's Same Day ACH offering, the UMB team had a thorough and well developed process in place and was able to fast-track the Originator into their program. The bank was then able to process the company's approved file before the final

Same Day ACH processing window, and the pension payments were received that same day. This solution helped the customer with their immediate need and saved them money as they now have a more cost-effective choice to send emergency payments instead of sending wire transfers.

EPCOR recently spoke with Tristan Thompson, Vice President, Payment Group Manager at UMB about the steps the bank has established to utilize Same Day ACH and proactively respond to emergency situations such as these.

Tristan explained that UMB offers Same Day ACH for their Originators that benefit from the network enhancement. For those companies who request to participate, UMB follows its standard due diligence process which includes gathering needed information to vet and approve Same Day ACH Originators. In urgent cases, such as that with ABC Company, UMB's relationship management, operations, and product teams follow a predetermined process to expedite

obtaining required documentation, initiate necessary system changes, and ultimately process the Same Day ACH files to meet ABC's emergency need.

“NACHA provided multiple use-case scenarios when preparing the industry for Same Day ACH,” Tristan said, “and this one was text book. It was gratifying to see this situation play out and result in a positive experience for our customer, always our top priority. Having this in our tool kit will only enhance our service to clients across the company.”

Preparing for Same Day ACH processing, and especially for emergency exceptions such as this one, meant a lot of internal training for UMB staff, from Treasury sales to Operations. No one could have expected, however, how quickly that training would pay off for both UMB and its customer. Visit the Web for more information on [UMB's Same Day ACH offerings](#).

Can you picture your company utilizing Same Day ACH? If you would like to learn more about this new, expedited payment option, contact your financial institution. 📧



Electronic Payments Core of Knowledge

EPCOR is your electronic payments core of knowledge and influence. We are a member-focused association devoted to providing personalized support and services.

The mission of EPCOR is to provide our members with the knowledge, support and industry representation necessary to succeed in the ever-evolving electronic payments business.



© 2016, 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