

INSIDE: Study Shows Merchant Fraud Costs Are Increasing.....pg. 1

Small Businesses Missing Out on Benefits of Direct Deposit.....pg. 1

E-commerce Fraud Increase May Threaten Small Businesses Post EMV Switch.....pg. 2

October is National Cyber Security Awareness Month.....pg. 3

Rules Changes Recappg. 3

White Paper: Every Small Business Should Use the NIST Cybersecurity Framework.....pg. 4

More than 90% of Payroll Professionals Believe Same Day ACH Can Help Support Payroll Needs.....pg. 5

Bitcoin Regulation Roundup, Regulator Divide and "Life On Bitcoin"pg. 7

Federal Reserve Support of the NACHA Rule Ensures Same Day ACH Ubiquity.....pg. 8

Small Businesses Now the Target of Large Sanctions Penalties.....pg. 9

Small Business Payments Toolkit—Top 5 Takeawayspg. 10

CFPB's Use of Behavioral Economics Validated by Executive Order.....pg. 11

Why Should You Choose ACH for Healthcare Payments?.....pg. 11

Study Shows Merchant Fraud Costs Are Increasing

The annual LexisNexis® True Cost of FraudSM study offers important insights into the profound effects of fraud on merchants, consumers and financial institutions. It establishes the actual cost of fraud as witnessed by merchants and provides key findings and specific recommendations for the industry.

This year is an especially demoralizing year for merchants as fraud consumes even more revenue.

All merchant segments are losing more revenue to fraud this year and, in the face of these losses, more merchants believe that the additional costs of mitigation are prohibitive.

The upward trend of fraud losses as a portion of revenue for all merchants

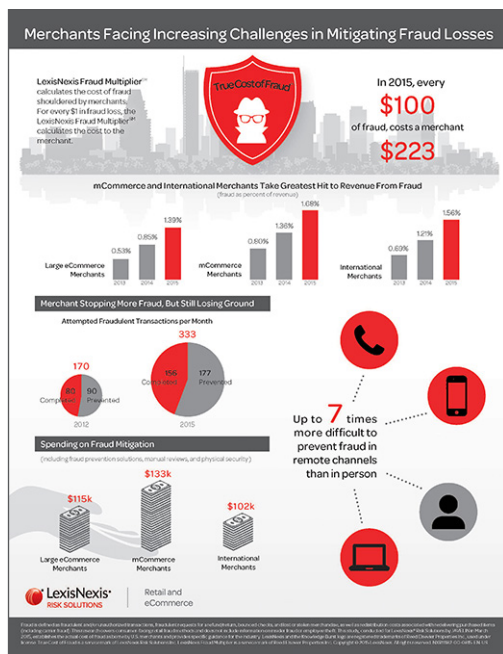
continues in 2015 at 1.32 percent, up from 0.68 percent in 2014. While all merchant segments took a substantial hit on fraud losses

as a percentage of revenue, international and mCommerce merchants were hardest hit with 1.56 percent and 1.68 percent loss, respectively.

Merchants prevented more fraudulent transactions overall, but online and Mail Order/Telephone Order (MOTO) transactions provide considerably more

challenging. While merchants prevented more fraudulent transactions overall in the past year, merchants find it up to 7x more difficult to prevent transactions through remote channels compared to in-person.

[Click here](#) to read the report. 



**click image to view large version*

Small Businesses Missing Out on Benefits of Direct Deposit

by Scott Lang, NACHA

In the last 10 years, the electronic movement of money has become easier than ever. More people are banking online, paying bills electronically and making payments with their mobile devices. In fact, one-quarter of all smart-phone users have made a mobile payment in the last 12 months and half of consumers already use automated bill pay.

Yet, many employers are still lagging when it comes to one of the simplest forms of electronic payment: Direct Deposit via ACH. According to a study conducted in 2011 by NACHA—*The Electronic Payments Association*, nearly half of small businesses (48 percent) don't use Direct Deposit for their payroll needs.

Direct Deposit can offer plenty of benefits for employers. May was National Direct Deposit and Direct Payment via ACH Month, so now is a great time for small-business

see **BENEFITS** on page 2

BENEFITS continued from page 1

owners to learn about the perks of Direct Deposit for payroll and how to switch.

Switching to Direct Deposit has plenty of advantages for employers as well as their employees, including:

1. It's employee-friendly. Direct Deposit eliminates the need for employees to travel to the bank and cash their checks. Instead, they get quick access to their money on a reliable basis, even if they're out of the office or on vacation. Additionally, many financial institutions waive checking or savings account fees when the account receives regular direct deposits, saving employees money. It's no surprise, then, that three in four employees who have Direct Deposit available to them use it. And 97 percent of employees who use direct deposit say they're satisfied.

2. It's safe. While some electronic banking and payment methods are new or unproven, Direct Deposit has been in use since the

1970s. The ACH network handled 23 billion electronic payments in 2014, almost half of which were recurring payments, such as Direct Deposit.

What's more, with Direct Deposit, money is transferred electronically—securely and directly from the employer's bank to the employee's bank. By contrast, paper checks often pass through many hands and they can be lost or stolen, altered or counterfeited.


3. It's a money-saver. Direct Deposit savings can be significant for many companies. Electronic payments create accounting efficiencies and reduce costs, particularly those costs associated with paper checks, like postage and other supplies. Employers can save up to \$1.25 per payment by converting from paper checks to direct deposit.

Additional cost savings come from productivity gains. Employers lose up to \$2 per payment due to employees leaving to cash their checks. Direct Deposit eliminates

those trips to the bank—and the costs associated with them.

Switching to Direct Deposit can seem intimidating, but it's actually very simple. In most cases, employers just contact their financial institutions or their payroll-solution provider to find out what needs to be done.

Savings gained from Direct Deposit increase as more employees enroll, so it's beneficial for employers to promote their new Direct Deposit offering to all employees. Providing employees with information on the benefits of Direct Deposit can help encourage enrollment.

To learn more, employers can visit [NACHA's online information center for Direct Deposit and Direct Payment via ACH resources](#). The site answers common employer questions and provides information for employees as well. 

Source: Digital Transactions

E-commerce Fraud Increase May Threaten Small Businesses Post EMV Switch

With the October deadline for EMV behind us (Europay, Mastercard and Visa) fraud liability shifts from issuers to retailers, merchants and financial institutions are focusing on making the change happen as soon as possible. However, this does not take into account a potential increase in e-commerce fraud.

The adoption of EMV chip cards will create roadblocks for fraudsters hacking POS systems in-store, but cybercrime experts ThreatMetrix predict online retail fraud and fraudulent account creation for financial institutions in the U.S. will increase drastically following the EMV transition. The precedent has been set in other countries. For example, online fraud increased 21 percent in Europe in 2012, in part due to the introduction of EMV cards.

"Cybercriminals will always exploit the weakest link," Alisdair Faulkner, chief products officer, ThreatMetrix, told *FierceRetailIT*. "Prior to the adoption of EMV, fraudsters could easily hack POS systems in-store to skim credit card numbers and security codes when customers would swipe their magnetic stripe credit cards. But after the widespread adoption of EMV in the U.S., cybercriminals will have a much harder time obtaining credit card information through compromised POS systems."

"As a result, they will focus their efforts on using previously stolen credit card information and other personal data, such as username/password combinations compromised in previous data breaches, to commit fraud online, where exploitable security holes still exist for card-not-present uses," he said.

U.S. retailers lost about \$32 billion to fraud in 2014, up from \$23 billion the year before. Most of that was due to the weak security of credit and debit cards. But with the EMV transition, U.S. merchants and credit card networks will follow many other countries around the world in abandoning the technology associated with magnetic stripe credit and debit cards. The magnetic stripe technology allows hackers to skim card numbers and security codes to use for stolen credit cards, but EMV chip card technology will prevent this, ThreatMetrix reported in a press release.

EMV will make it more difficult for criminals to copy the account numbers, security codes and magnetic stripes associated with those cards. However, in the countries that preceded the U.S. in adopting

see PERCENTAGES on page 3

RULES CHANGES RECAP

September 18 marked the date for several *ACH Rules* changes that could impact your business. Did you see our Special Edition of *Inside Origination* that provided details of the impact of the changes? If not, [CLICK HERE](#) to review that issue.

Also, if you missed our *2015 ACH Rules Update for Originating Companies* that was distributed early this year, ensure your compliance by downloading it [HERE](#).



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.

PERCENTAGES continued from page 2

EMV, a significant increase in online fraud followed. The same thing is expected to happen here.

“From a consumer perspective, the shift to EMV is good news as it will make it harder for cybercriminals to counterfeit credit cards and conduct fraudulent purchases in stores,” said Faulkner. “But from an online merchant perspective, as it becomes more difficult for cybercriminals to monetize on counterfeit cards, their goals are now going to shift to use stolen credit card data through online channels. There’s no time to waste for retailers to start implementing systems that look at cybercrime in context to combat the growing breadth and intelligence of fraud following the widespread adoption of EMV in the U.S.”

As of the October 1st deadline, retailers still relying on magnetic stripe card technology are liable for any fraud losses that result, rather than the issuer paying these costs. However, an increase in online fraud can create liability issues for financial institutions. To ward off this expected growth in fraudulent online account

creation, they also will need to increase security.

Additionally, with the switch to EMV, financial institutions will need to prioritize mobile security. Thirty percent of customer acquisition now comes from some kind of mobile device. This trend is continuing to grow, which creates even more of a challenge for financial institutions, as the mobile channel is easily compromised by cybercriminals.

“The vast majority of financial institutions are using very rudimentary intelligence about user behavior, Internet connections and devices to determine whether the end user is a good customer or a cybercriminal,” Faulkner said. “For example, many financial institutions still rely on the geolocation of the user based on IP addresses and cookies for authentication—but those can be easily spoofed through proxies and by bots. With the adoption of EMV, financial institutions must have the capabilities to authenticate users by assessing their digital identities as a whole to prevent cybercriminals from opening new credit cards with a stolen identity.”

Source: *FierceRetail*

October is National Cyber Security Awareness Month

We now live in a world that is more connected than ever before. The Internet touches almost all aspects of everyone’s daily life, whether we realize it or not. Recognizing the importance of cybersecurity to our nation, President Obama once again has designated October as National Cyber Security Awareness Month (NCSAM).

MCSAM is designed to engage and educate public and private sector partners through events and initiatives with the goal of raising awareness about cybersecurity and increasing the resiliency of the nation in the event of a cyber incident.

One aim of National Cyber Security Awareness Month is to provide independent business owners with the resources to protect their intellectual property and customer data. In an era of growing cybercrime, a safe and secure Internet is vital to building a prosperous business.

As a business owner, you can help make the Internet safer and more secure by participating in NCSAM. Whether you are able to show your support for just one day or every day this October, consider the following ways you can make a difference to raise cybersecurity awareness.

see **SECURITY** on page 4

SECURITY continued from page 3

- Display an NCSAM banner on your company website. [Click here](#) to download.
- Send an email informing your employees, clients and business contacts that October is National Cyber Security Awareness Month. Encourage them to review tips and advice from the global cyber security awareness campaign, [STOP. THINK. CONNECT.](#)
- Strengthen your company's email and online accounts by adding extra layers of security and enabling technologies

like 2-factor authentication. To learn more about these services, visit STOP. THINK. CONNECT's [2 Steps Ahead Campaign page](#).

- Review Verizon's [2013 Data Breach Investigations Report](#). By knowing today's threats, you can better protect your organization tomorrow
- Download the [Federal Communications Commission's Small Biz Cyber Planner 2.0](#) to help you chart a path to a more cyber-secure business.

There are countless resources available to aid businesses in ensuring they are meeting

the current cyber threats head on. Here are just a few:

- [StaySafeOnline.org](#)
- [Department of Homeland Security's Small and Midsize Business Toolkit](#)
- [Stop. Think. Connect. Toolkit](#)
- [Federal Small Biz Cyber Planner 2.0](#)
- [Internet Essentials for Business 2.0](#)
- [Geographically Specific Resources](#)



Source: U.S. Department of Homeland Security

White Paper: Every Small Business Should Use the NIST Cybersecurity Framework

Turn on the TV or open a newspaper on any given day and the headlines will scream of another company, large or small, that has been targeted or significantly damaged by hackers. Small and medium-sized businesses (SMBs) are much more vulnerable to cybersecurity attacks than those with large infrastructures and protection investments.

In 2014, 60 percent of all targeted attacks were aimed at SMBs according to Symantec's 2015 Internet Security Threat. Often, these companies have fewer resources to invest in security, putting not just their companies, but also their business partners at higher risk. Not to mention, the average cost of \$300,000 for these attacks according to news reports. And these costs may not fully reflect all the associated indirect costs such as lost productivity, loss of customer trust or opportunity costs such as lost revenue or a damaged reputation.

As an SMB, if you feel safe and out of reach from a cyber-attack, you are not alone, but consider these facts. A recent survey from National Cyber Security Alliance (NCSA)



showed that 77 percent of SMBs feel they are safe from a cybersecurity breach. Those numbers don't match the reality. In 2014, according to Symantec, one in two small business organizations with 250 employees or fewer were targeted. So, what can or should an SMB do?

There is good news. The National Institute of Standards and Technology (NIST) Cybersecurity Framework V1.0, released in February 2014, proposes five core functions: Identify, Detect, Protect, Respond and

Recover, to which every organization, large or small, should pay attention and implement to proactively address and better manage cybersecurity risks to their business.

There are five things every SMB should know about the NIST Cybersecurity Framework:

1. It is actionable—and allows you to assess your organization's risks in the five core functions;
2. It leverages industry standards and best practices;

see FRAMEWORK on page 5

More than 90% of Payroll Professionals Believe Same Day ACH Can Help Support Payroll Needs

As Same Day ACH looms on the horizon, results from an American Payroll Association survey show broad support for the benefits of Same Day ACH to their roles and organizations.

The survey, conducted during National Payroll Week in September, targeted 1,500 payroll professionals nationwide. More than 90 percent of respondents indicated that Same Day ACH would help them in meeting their payroll needs.

Specifically, respondents indicated that enhancing existing ACH next-day capabilities with the option of Same Day ACH would better support direct deposit functions (for hourly workers, temporary staff and termination pay needs), contingency plans for missed deadlines, payroll error corrections,

“The results of the survey show that having the option of Same Day ACH can meet a number of unmet corporate payment needs, particularly as they relate to payroll,” said Janet O. Estep, president and CEO of NACHA. “The positive support for this capability confirms that our efforts will ultimately bring additional value to more employees who will benefit from the efficiency of delivering Direct Deposit of payroll *via* ACH.”

“APA members overwhelmingly support the concept of Same Day ACH settlements, which will allow businesses greater flexibility when making payments and correcting errors and to maintain compliance without reverting to paper checks,” said Dan Maddux, executive director of the American Payroll Association.

WHAT MORE DO I NEED TO KNOW ABOUT SAME DAY ACH?



Same Day ACH is less than one year away from becoming a reality. How will this affect your organization as an Originator? Join EPCOR for our *Same Day ACH: What Originators Need to Know NOW!* webinar on **October 30** to take a look at the benefits, impacts and considerations that all Originators should examine in preparation of a Same Day ACH environment.

tax withholdings remittances and remittances of garnishments. Additionally, 97 percent of respondents identified Same Day ACH as a service that would add value to their organizations and more than 86 percent confirmed that same-day ACH capabilities would benefit their organizations beyond payroll functions.

NACHA moved forward with formal rulemaking on the phased implementation approach for Same Day ACH by issuing a Request for Comment to the industry. The Rules changes subsequently passed on May 19, 2015 and support from the Federal Reserve on which implementation was contingent was received on September 23, 2015.

FRAMEWORK continued from page 4

3. It helps you focus and prioritize important cyberrelated investment decisions;
4. It can help reduce legal risk with evidence of your organization's good faith efforts to manage cybersecurity risks;
5. It is flexible—and allows SMBs in different industries and of various sizes to adapt the Framework and make it work for them.

Identify Risk Areas within the Company

With a goal of readiness, preparedness and resilience, every small business should know and understand which organizational systems, assets, data and capabilities need to be protected.

Cybersecurity is about risk management; therefore, your C-Suite must participate in identifying and understanding the cybersecurity risks to the organization. This should include the CEO or president as well as the COO, CFO, CIO, CRO (chief risk officer) and CAO (chief administrative officer). For smaller companies that typically do not have the resources for all of these roles, at a minimum, the CEO or president and the individuals who have responsibility for operations and finance should be involved. Since many small businesses outsource their IT operations, it is recommended that companies involve outside experts in assessing the five core elements.

Protect the Company's Assets

One of the easiest and most affordable protections a company can take to protect its assets is to train its people. It sounds simple, but unfortunately many small businesses don't take the time or think it necessary to make sure their employees understand how they can help protect their company assets. There are also a myriad of industry

see SAME DAY on page 7

see FRAMEWORK on page 6

FRAMEWORK continued from page 5

best practices for safeguards that include recommendations like:

- Make backup copies of important business data and information;
- Change default credentials for all systems and require individual user accounts for all employees;
- Limit employee access to data and information and limit the authority to install software;
- Change passwords regularly;
- Protect information, computers and networks from viruses, spyware and other malicious code;
- Provide firewall security for your IT infrastructure;
- Control physical access to your computers and network components; and
- Secure your Wi-Fi networks. If you have a Wi-Fi network for your workplace make sure it is secure and hidden.

If your business uses an outsourced IT provider, work with them to make sure that these safeguards are implemented. They can also assist with developing or providing training to your employees on cybersecurity do's and don'ts.

Detect a Cybersecurity Event

How do you know if your organization has been attacked? Many times, there are visible signs. Examples may include your website being down or displaying random or negative content that is not authored or approved by

your company. Your network may suddenly become unavailable or certain software applications may behave strangely or provide errant information.

There are a variety of products and services on the market today to help your company develop and implement appropriate activities to assist you in identifying a potential cybersecurity event. For many small businesses, the investment needed to procure all of these tools solutions may be cost prohibitive, so some small business may want to consider using a vendor that specializes in monitoring and detecting anomalous activity, rather than doing it themselves.

Respond to a Cybersecurity Event

Responding to a cybersecurity event means taking action to develop or implement appropriate activities in response to a detected cybersecurity incident. It is important that your response processes and procedures are developed before a cybersecurity event occurs. Depending on the type of cybersecurity event, a response may include:

- Taking steps to quarantine the breach, so other systems or users are not affected;
- Implementing a response plan that describes what processes and procedures need to be executed to address the event;
- Communicating the status of response events and coordinating with stakeholders; and
- Performing forensics.

Recover from a Cybersecurity Event

A recovery plan supports your organization's ability to return to normal during or after an attack. The plan does not need to be overcomplicated and should include, at a minimum, lessons learned, which should then be incorporated into future activities. The plan should also address any holes in the communication coordination between internal and external parties such as employees, vendors and public relations partners, among others

Key Take Away

The #1 action every SMB should take is to assess where they are vulnerable to cyber-attacks or breaches so targeted actions can be implemented to reduce their cybersecurity exposure. Using the NIST Cybersecurity Framework can help SMBs:

- Become more knowledgeable about their organization's cybersecurity threats and risks;
- Determine areas of vulnerability that may exist with people, processes or technology;
- Have greater confidence and control to prioritize and determine where to invest cybersecurity resources; and
- Provide evidence of their organization's good faith efforts to manage cybersecurity risks and implement reasonable security measures 🟢

Source: Ola Sage, e-Management

ARE YOU IN COMPLIANCE?

Required Task: ACH Rules Compliance Audit
Responsible: Third-Party Senders
Deadline: December 31

Tip: Simplify the Process with EPCOR's
Third-Party Sender ACH Audit Workbook.

>> DOWNLOAD



SAME DAY continued from page 5


The Same Day ACH phased-implementation plan will add new ACH Network functionality over time that will provide greater value to end users. In addition to the current early morning settlement, this functionality includes two new Same Day ACH clearing and settlement windows at mid-day and the end of the business day and be available for virtually any ACH transaction.

Additionally, the phased implementation approach provides faster funds availability, improving the efficiency of hourly payroll disbursements and last-day tax or bill payments. All of this provides a solid foundation on which to build other innovative services.

“By moving forward with Same Day ACH, we can act now to provide important choices

for consumers and businesses who want to efficiently move money more rapidly directly between bank accounts,” said Estep. “It can serve as an important step in meeting the needs of today and providing a building block for the innovations of tomorrow.”

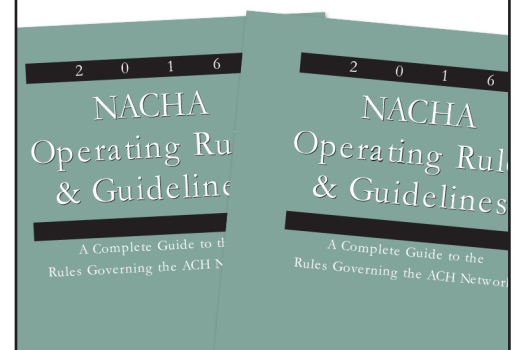
**GET ALL OF THIS AT EPCOR'S MEMBER PRICE
BY CLICKING HERE NOW TO REGISTER!**

Find out how to use Same Day ACH to your benefit and examine problem solving potential use cases that could be a game changer for your organization. Learn what changes will be necessary so that you can smoothly transition to a Same Day ACH environment and begin processing in 2016. Leave with action items and follow up questions you can take to your internal staff and your ODFI to ensure your organization's success in a Same Day ACH environment. 

ORDER YOUR 2016 ACH RULES TODAY!

RELYING ON OUTDATED
VERSIONS CAN BE CONFUSING
AND HURT COMPLIANCE.

**CLICK HERE TO PRE-ORDER
YOUR 2016 ACH RULES.**



ARE YOU A THIRD-PARTY PROCESSOR OR THIRD-PARTY SENDER?

EPCOR has specific, dedicated resources to help you understand and meet your compliance obligations.

Email
thirdpartyservices@epcor.org
to find out more!

Bitcoin Regulation Roundup, Regulator Divide and “Life On Bitcoin”

The regulators are coming, the regulators are coming.

It was bound to happen sooner or later.

Since venture money keeps fueling the beast called bitcoin and the blockchain, regulators have decided to put their arms around that which is bitcoin in an effort to better control its every move.

So, to keep up with all the ebbs and flows of who is regulating what, we've gathered the recent news on regulation.

New York

New York State's Department of Financial Services granted its first official business license for a bitcoin exchange, itBit, in early May. The license will allow the bitcoin exchange to bring in customers across the

country in a legal manner, which then puts the onus of regulation on the state. Allowing itBit to align itself in a similar manner to how banks are regulated is a first for the bitcoin exchange community and a victory (of sorts—although most don't necessarily characterize regulation as a victory) for the bitcoin community, as it marks the first fully regulated digital currency exchange in the U.S.

New Jersey

New Jersey seems to be following New York's footsteps and giving bitcoin a regulatory framework. Now, the New Jersey Legislature is attempting to push through a bill that would help regulate digital currencies—and also offer tax breaks for companies that exchange bitcoins.

see BITCOIN on page 8

Federal Reserve Support of the NACHA Rule Ensures Same Day ACH Ubiquity

On September 23, 2015, the Federal Reserve Board announced the approval of enhancements to the Federal Reserve Banks' Same Day automated clearing house (ACH) service. The enhancements are intended to align the Reserve Banks' Same Day ACH service with recent amendments to NACHA's *ACH Operating Rules* and will facilitate the use of the ACH network for certain time-critical payments, accelerate final settlement and improve funds availability to payment recipients.

The enhancements become effective September 23, 2016 and require Receiving Depository Financial Institutions (RDFIs) to participate in the service and Originating Depository Financial Institutions (ODFIs) to pay a fee to RDFIs for each Same Day ACH forward transaction.

The enhancements will be adopted by incorporation of NACHA's amended *Operating Rules* into Operating Circular 4, governing the Reserve Banks' ACH services.

"With the Federal Reserve's support of the NACHA Rule, the industry's commitment to modernizing the payments system and enabling a ubiquitous faster payment option can be fully realized," said [Janet O. Estep](#), president and CEO of NACHA. "Same Day ACH is a game changer as it will enable new options for consumers, businesses and government entities that want to move money faster and will serve as a building block for enabling payments innovation in the development of new products and services."

In May, the Same Day ACH Rule was [approved](#). The new Rule builds upon existing, next-day ACH Network capabilities by establishing two new Same Day settlement windows. The Rule also requires that all Receiving Depository Financial Institutions (RDFIs) receive Same Day transactions and provide faster funds availability to customers. Additionally, the Rule establishes the methodology for a Same Day Entry fee as a

mechanism for RDFIs to recover some of their costs for enabling and supporting mandatory receipt of Same Day ACH transactions.

The Rule will be implemented in three phases. In Phase 1, ACH credit transactions will be eligible for Same Day processing, supporting use cases such as hourly payroll, person-to-person (P2P) payments and Same Day bill pay. In Phase 2, Same Day ACH debits will be added, allowing for a wide variety of consumer bill payment use cases like utility, mortgage, loan and credit card payments. Phase 3 introduces faster ACH credit funds availability requirements for RDFIs; funds from Same Day ACH credit transactions will need to be available to customers by 5 p.m. RDFI local time. Phase 1 will become effective September 23, 2016.

For more information about Same Day ACH, [click here](#). 

Sources: Federal Reserve Bank and NACHA

BITCOIN continued from page 7

That measure could potentially push more businesses to accept bitcoin.

"I want to encourage innovation here in New Jersey. I think there's an opportunity for job creation," said New Jersey Assemblyman Raj Mukherji, who is credited with spearheading the bill with Assemblyman Gordon Johnson.

North Carolina

As a major banking hub, North Carolina is also investigating how it can legislate bitcoin to help protect consumers and prevent the currency in being used in money laundering efforts. The state's banking commissioner is trying to help push through legislation, which has passed the state house and is making its way into the state's senate.



"There's two sides to the bitcoin. One side is the clear potential value of the innovation and what that could portend for the payment system. Since we're a business friendly state, we want to facilitate that," North Carolina

State Banking Commissioner Ray Grace said in an interview. "We wanted to mitigate the risk while facilitating the potential benefits down the road."

California

While the East Coast looks to bulk up its bitcoin laws, the West Coast might soon want in, too. Reports indicate that California's Department of Business Oversight will not look into how to regulate bitcoin itself, but will allow the state's lawmaking body to weigh in on what to do. While no proposals have made their way to the legislative floor, it appears as though discussions are still in the works.

"We're still in the process of how or if at all to regulate virtual currency business under our current statutory scheme," Department of

[see BITCOIN on page 9](#)

Business Oversight spokesman Tom Dresslar said in an interview.

Legislation that was introduced in March would require maintaining bank-style reserves against possible losses for bitcoin exchanges, but that law hasn't moved forward. Licensees would have to pay a non-refundable \$5,000 registration fee, provide identifying information and keep enough capital in "investment-grade permissible investments" to cover customers' deposits.

California is a particularly interesting state for regulation since it is home to bitcoin companies Coinbase, Ripple Labs and ChangeTip.

What Other States Are Doing

Outside of those listed above, reports from CEX.IO, the international bitcoin exchange that joined the U.S. market in April, announced that it was unable to work with

businesses or consumers in the following states because they required additional money transmitter licenses for bitcoin companies. These states include: Alabama, Alaska, Arizona, Arkansas, Colorado, Florida, Georgia, Guam, Idaho, Iowa, Kansas, Louisiana, Maryland, Michigan, Mississippi, Nebraska, New Hampshire, North Dakota, Ohio, Oregon, Tennessee, Texas, Vermont, Virginia and Washington.

But as more states look to clarify bitcoin and digital currency legislative frameworks, it's likely more of these states will join the ranks of the ones above which plan to put official bitcoin license regulations on the books as statewide measures help give the regulatory measures more clarity for bitcoin businesses looking to open shop.

International Bitcoin Bans

While bitcoin seems to be moving rapidly in Europe, with places like the U.K. looking

to be the hub for bitcoin, there are still plenty of regions around the world looking to heavily regulate—or hold outright ban bitcoin. Countries like China have a partial ban on the digital currency and Thailand and Vietnam do not recognize bitcoin as an acceptable form of currency—in large part because the digital currency is not issued by the government. Particularly in regions like China and Russia, regulatory hurdles will always remain a struggle for bitcoin. India has also reportedly looked into banning bitcoin but hasn't moved toward doing so. Bitcoin is also currently banned in Bangladesh, Bolivia, Ecuador, Iceland and Kyrgyzstan.

But on the bright side for bitcoin, Russian authorities just announced they were lifting the country's ban on bitcoin. So it appears bitcoin will be back in Russia—at least for now. 🟢

Source: PYMNTS.com

Small Businesses Now the Target of Large Sanctions Penalties

The U.S. Treasury Department's Office of Foreign Assets Control (OFAC) enforces the nation's sanction laws—such as those that prohibit exports to sanctioned countries or transactions involving individuals, companies and shipping vessels on sanctions lists. The OFAC enforcement stories that make the news are often those with record-setting fines against major international companies.

However, in recent months OFAC has increasingly made a point of levying fines and penalties against small businesses.

What has been the crime? Regulatory violations stemming from ignorance of OFAC's sanctions regime and a failure to institute export control and sanctions compliance programs. While the sizes of the fines pale in comparison to those larger

companies have been subjected to, they can still cripple and even bankrupt small businesses. Recent examples include:

- Aug. 5, 2015—Production Products, Inc., a small Maryland-based, family-run manufacturer with only 10 employees, was fined \$78,500 in connection with charges that the company exported three HVAC duct fabrication machines to China National Precision Machinery Import/Export Corporation, a Chinese company on the Specially Designated Nationals and Blocked Persons List. OFAC considered the company's failure to implement a sanctions compliance program to be an aggravating factor in determining the amount of the fine. Given the value of the machines,

OFAC could have fined the company \$1 million—but the agency reduced the penalty in part because the company took remedial steps to implement a sanctions compliance program.

- July 24, 2015—Great Plains Stainless Co., a small Oklahoma-based distributor of stainless steel pipe, tube, fittings and flanges, was fined \$214,000 for selling goods to a legitimate and non-sanctioned customer in Dubai. The company fell afoul of Executive Order 13382 and OFAC regulations because its Chinese vendor shipped the goods from Shanghai aboard a sanctioned vessel, the M/N Sahand. Again, OFAC found an aggravating factor leading to an

see TARGET on page 10


increased penalty was the company's failure to have a sanctions compliance program in place.

- July 29, 2015—Blue Robin, Inc., a Massachusetts-based information technology firm was fined \$82,260 for the 2009-2010 importation of web development services from an Iranian company called PersiaBME—a violation of the Iranian Transactions and Sanctions Regulations. Despite the company's pleas that it was unaware it was violating U.S. law and was struggling financially, OFAC determined the penalty amount was appropriate because the business had no OFAC compliance program in place at the time of the transactions and had not implemented one since.

These enforcement actions illustrate that OFAC will not provide a free pass if you are a small company or have a lack of experience in international trade. Given the ongoing crackdown, investing in compliance today could save your business thousands in fines and penalties down the road. 📌

Source: *Mcdonaldhopkins.com*

2016



WHAT DO YOU REALLY NEED TO KNOW IN 2016?

Find out at *Payment Systems Update!* We will cover recent and upcoming payments and regulatory changes all payment professionals need to know, including, their effective dates, compliance considerations and potential impacts on you and your customers/members.

Small Business Payments Toolkit—Top 5 Takeaways

Earlier this year, the Remittance Coalition released the first volume of the Small Business Payments Toolkit. The toolkit is intended to encourage the adoption of electronic business-to-business payments and remittance information exchanges by small businesses. The Remittance Coalition is a group of payments industry players (including Federal Reserve Banks) that works to increase the efficiency of business-to-business (B2B) payments made and reconciled by US businesses. The toolkit provides a host of useful information that can be leveraged by financial institutions, vendors, small businesses and anyone interested in learning more about payments.

Here are our top five takeaways from the Small Business Payments Toolkit:

1. Adopting B2B electronic payments and remittance information exchanges will make life easier for small business owners

- A. Although it may not currently be a top priority, choosing to enhance the efficiency of your payments process can make life easier in a number of ways:
 - i. Increased ease of paying taxes, bills and your payroll
 - ii. Increased ease of receiving payments for businesses that bill clients on a recurring basis
 - iii. Higher savings from reducing the labor and administrative costs needed to process payments and remittance details

2. Learn about the various types of payments fraud and tips to help avoid fraud

- A. Educating all levels of your organization on basic payment security practices can go a long way towards avoiding fraud and data breaches. Some payment security best practices include:
 - i. Use strong passwords with lengthy combinations of letters, numbers and special characters and make sure to change them often
 - ii. Dedicate a PC to be used only for online banking activities
 - iii. Use dual control for origination of ACH files and wire transfers. This means assigning roles to two different individuals so it is not possible for one person alone to complete a transaction

3. Small businesses that accept ACH payments will benefit from a slew of increased business opportunities

- A. Accepting ACH payments opens the door for new opportunities that include:
 - i. Increased business retention
 - ii. Reduced fraud—ACH payments are safer than checks
 - iii. Ability to work with companies and government entities that exclusively do business with those accepting ACH payments

4. When looking to improve the efficiency of your payments processes, choosing the right financial institution is key

see TOOLKIT on page 11

TOOLKIT continued from page 10

- A. Be proactive and contact banks about payment needs; don't expect them to come to you. Specifically, you should seek out financial institutions that offer services like:
- Small business-focused online banking with robust bill presentment and payment services
 - Services to set up small businesses as ACH receivers and originators
 - Fraud monitoring and prevention tools, including alerts

5. Contrary to the name, this toolkit isn't just for small businesses

- A. While small businesses are the toolkit's primary target, small business bankers, advisors and anyone else interested in learning more about B2B payments will

also find this toolkit helpful. Some of the great resources within the document include:

- An explanation of the different types of payments (Page 3)
- An explanation of how the ACH network electronically moves money and data (Page 8)
- Fraud prevention and mitigation tips (Page 19)
- A "resource" section full of links to external sites where interested parties can learn more about the specific toolkit information that most interests them (Page 30)

We encourage you to take a peek at the [Toolkit](#)—It's a quick and easy read for everyone! 📖

Source: [FedPaymentsImprovement.org](#)

Why Should You Choose ACH for Healthcare Payments?

The Patient Protection and Affordable Care Act (ACA) identified NACHA's CCD+Addenda as the HIPAA healthcare Electronic Funds Transfer (EFT) standard for payments processed through the ACH Network.

With so many choices available, how does the ACH Network compare to other payment types cited in the final rule? What are the providers' rights to request and receive claims through the ACH Network?

Funds Availability:

- ACH—Next day or same day with the upcoming Same Day ACH Rules enhancements
- Virtual Card—2 or 3 business days,

depending on card type and agreement

- Wire Transfer—same day

Average Cost to Receive \$2500 Payment:

- ACH—Approximately \$ 0.34 (for any dollar amount)
- Virtual Card—Percentage of total payment plus transaction fee
- Wire Transfer—\$10.73 (for any dollar amount)

Enrollment/Acceptance:

- ACH—must have a bank account; one time with each health plan
- Virtual Card—must have a bank account and agreement with merchant

see [HEALTHCARE](#) on page 12

CFPB's Use of Behavioral Economics Validated by Executive Order

Since opening its doors for business, behavioral economics has played a central role in the CFPB's regulatory agenda. Behavioral economists posit that consumers are not rational decision makers and instead have certain frailties or weaknesses that lead them to make decisions that they would later recognize as not in their own best interest.



The CFPB's use of behavioral economics was validated by an [Executive Order](#) issued by President Obama this week that encourages federal agencies to "identify policies, programs and operations where applying behavioral science insights may yield substantial improvements in public welfare, program outcomes and program cost effectiveness" and to develop strategies for applying such insights to programs. It also encourages agencies to "recruit behavioral science experts to join the Federal Government" and "strengthen agency

see [CFPB](#) on page 12

CFPB continued from page 11

relationships with the research community to better use empirical findings from the behavioral sciences.” The CFPB has already hired **behavioral economists** and appointed behavioral economists to its Academic Research Council.

The Executive Order also directs agencies to “improve how information is presented to consumers, borrowers, program beneficiaries and other individuals, whether as directly conveyed by the agency or in setting standards for the presentation of information, by considering how the content, format, timing and medium by which information conveyed affects comprehension and action by individuals as appropriate.” Behavioral science is already an element of the CFPB’s development of new disclosures. For example, in its recent notice indicating that it was seeking approval from the Office of Management and Budget to conduct a national web survey as part of its study of ATM/debit card overdraft disclosure forms, the CFPB stated that the survey will explore “financial product usage, behavioral traits and other consumer characteristics that may interact with a consumer’s experiences with overdraft programs and related disclosure forms.” 🟢

Source: Barbara S. Mishkin, CFPB Monitor

Is It Too GOOD TO BE TRUE?

33 ON-DEMAND COURSES AND
18 PUBLICATIONS
FOR ONE LOW PRICE?!

IT'S TRUE! WE CALL IT THE 2015 EPCOR ELECTRONIC RESOURCES LICENSE



ELECTRONIC RESOURCES LICENSE
OPEN KNOWLEDGE FOR EVERYONE

HEALTHCARE continued from page 11

card processing provider, plus a point of sale processing terminal

- Wire Transfer—must have bank account; one time with each health plan

Risk:

- ACH—very low risk with credit payments; some financial institutions can support additional account monitoring tools such as debit blocks or filters
- Virtual Card—higher risk; card numbers mailed or faxed can be compromised
- Wire Transfer—very low risk with immediate payment

Manual Processing for Payments:

- ACH—none; automatically deposited to bank account
- Virtual Card—each payment must be manually entered into the point-of-sale terminal by office staff
- Wire Transfer—none; automatically deposited to bank account

Reassociation with Electronic Remittance

Information:

- ACH—standardized inclusion of reassociation number included in payment; delivered by financial institution after service is established
- Virtual Card—not included with payment; manual access through Web portal
- Wire Transfer—not required to include reassociation number with payment; IF provided, financial institution can provide

Providers Benefit from Choosing ACH

All providers have the right to request and receive claims reimbursements via the ACH Network. Under HIPAA (45 CFR §

162.925), health plans must deliver the claims reimbursement payment, when requested, starting January 1, 2014.

The benefits to the provider of requesting claims reimbursement through the Network are many:

- **Easy, Automatic Payments**—Receiving healthcare EFTs *via ACH* is as quick as receiving Direct Deposit *via ACH*.
- **Improved Cash Flow**—Healthcare EFTs *via ACH* ensure funds are available up to 7 days faster than with paper checks.
- **Safe and Secure**—Checks continue to be the dominant payment form targeted by fraudsters. Replacing all checks with healthcare EFTs *via ACH* is the single best way to combat fraud.
- **Automatic Reassociation**—Only healthcare EFTs *via ACH* offer providers the ability to automatically reassociate remittance information.
- **Consistent with Medicare**—Beginning January 1, 2014, Medicare will be implementing healthcare EFTs *via ACH* for all claims reimbursements, creating accounts receivable consistencies.
- **Smart, Cost-Effective Choice**—The cost of claims *via ACH* is, on average, only \$0.34 versus \$10.73 or more for other EFT payment types. 🟢

Source: NACHA



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 financial institutions with reliable payments and risk management education, information, support and national industry representation.



Through our direct membership in NACHA, EPCOR is a specially recognized and licensed provider of ACH education, publications and support.

© 2015, 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