epcor®
Electronic Payments Core of Knowledge

INSIDE ORIGINATION

INSIDE:

2014 *ACH Rules* Update for Originating Companies

As an originator of ACH entries it is important to stay up-to-date with your *ACH Rules* obligations, including updates and changes as they arise. How do the 2014 *ACH Rules* changes impact your organization?

Click here to download the *2014 ACH Rules Update for Originating Companies* summary document and review which *ACH Rules* changes may apply to you. Be sure to contact your financial institution regarding any questions you have in regard to how these changes pertain to your current Origination activity.

Federal Reserve Payments Study Offers Expanded View of U.S. Noncash Payment Trends

The *2013 Federal Reserve Payments Study*, shows that card payments—credit and debit—now account for more than two-thirds of all noncash payments, while the number of checks paid continued to decline.

The Study, conducted triennially and available at www.frbservices.org, examines noncash payment trends in the United States. The 2013 Study has been expanded to include new information related to various payment initiation methods and unauthorized payments. To provide perspective on consumer and business payment trends over the past decade, the results are compared to previous payment studies conducted in 2004, 2007 and 2010.

The 2013 Study's highlights include:

- The total number of noncash payments, excluding wire transfers, was 122.8 billion, a growth rate of 4.4 percent annually from 2009 to 2012. The rate of growth was down slightly from the previous 10 year (2003 - 2012) growth rate of 4.7 percent. The total value of noncash payments grew from $72.2 trillion in 2009 to just under $79 trillion in 2012.
- The number of credit card payments, which had shown a decline in the 2010 Study, grew at an annual rate of 7.6 percent from 2009 to 2012. Debit card payments grew at a rate of 7.7 percent over that same period.
- Automated Clearing House (ACH) growth slowed to 5.1 percent annually from 2009 to 2012, down from the average annual growth of 10.9 percent over the previous 10 years. From 2009 to 2012, the number of ACH payments as a percentage of total payments increased less than 1 percent while the value of ACH as a percentage of total noncash payments rose almost 10 percentage points, from 51.5 percent to 61.3 percent.
- The number of checks paid continues to decline, falling to 18.3 billion, less than half the number a decade earlier (37.3 billion). Checks are increasingly being

see PAYMENTS STUDY on page 2

PAYMENTS STUDY continued from page 1

deposited as images, with 17 percent being deposited as an image at the bank of first deposit versus 13 percent as reported in the 2010 Study.

- The 2013 Study estimates that there were 31.1 million unauthorized payment transactions in 2012, with a value of $6.1 billion

The study was made possible by broad-based industry support and information sharing. "Payments industry participants in the Study provided a robust response, affording the Federal Reserve the opportunity to review a full range of traditionally collected information on the number and value of noncash payment types, as well as new data on payment initiation methods, third-party fraud and other relevant noncash payment factors," said Jim McKee, senior vice president of the Federal Reserve Bank of Atlanta, which sponsored the Study. "Furthermore," he continued, "as part of the Fed's long-standing commitment to collaborate with the industry in making the payments system more efficient, we hope the longer-term, 10-year view provided in the 2013 Study offers increased insight into shifts in consumer and business payments choices."

As in previous studies, the estimates reported are based on information gathered in three survey efforts: the *2013 Depository and Financial Institutions Payments Survey* (DFIPS), the *2013 Network, Processors and Issuers Payments Surveys* (NPIPS), and the *2013 Check Sample Survey* (CSS). The Federal Reserve partnered with McKinsey & Company and Lieberman Research Group, as its subcontractor, on the DFIPS, and with Blueflame Consulting and MH Consulting, as its subcontractor, on the NPIPS. McKinsey & Company reviewed a large random sample of images for the CSS. The information collected in each survey is combined with information about payments trends from previous studies and then analyzed and adjusted for seasonality to produce comprehensive estimates not available in other studies. "The objective of the study is to produce trend information valuable to the industry in serving the public interest to improve the U.S. payments system," McKee said.

A more detailed report, anticipated in Spring 2014, will include a complete description of the methodologies used and data collected for the 2013 Payments Study.

Download the Summary Report and Initial Data Release.

Source: Federal Reserve Banks

PCI Security Standards Council to Launch eLearning Courses for Companies

The PCI Security Standards Council (PCI SSC), an open global forum for the development of payment card security standards, has announced new online training courses aimed at educating companies about how to keep their customers' payment data secure, and how to become and remain compliant with PCI Security Standards.

These courses, developed in response to increased commercial interest in security awareness training, are the latest additions to the Council's pro-active program of training and education. PCI SSC offerings include more than 40 instructor-led classes at locations around the world as well as online, eLearning offerings available anytime, anywhere. The range of training options is diverse, representing today's reality that managing security within a commercial enterprise is a responsibility shared across a company. In the last five years, more than 20,000 people have participated in PCI SSC workshops and training courses.

"PCI 3.0 Insider's Guide", is a new eLearning course that provides a comprehensive review of the intent, interpretation and implementation of the major changes in the newest version of the PCI Data Security Standard (PCI DSS), version 3.0—the keystone for developing a robust payment card data security process. "Insider" is definitive professional and technical training targeted to professionals who need to understand and implement the important recent updates to the PCI DSS and the Payment Application Data Security Standard (PA-DSS).

In Spring 2014, the new "PCI Essentials" series, part of the PCI SSC's PCI Security Awareness Education curriculum, will be released. The goal of this series is to reduce the impact of today's threats to payment card security by equipping staff with the knowledge needed to protect data assets. It includes 10 highly interactive and immersive online modules, each focusing on a specific area of PCI security, which can be combined to provide appropriate training for all levels of employees. The content has been designed to be engaging, relevant and memorable, ensuring that it will have a tangible impact on information security.

"It's important that organizations continuously assess payment security and maintain their defenses against malicious breaches, as fraud takes no holidays. Every employee has a stake in this effort, and it's part of the Council's mission to educate them to accomplish it," said Bob Russo, General Manager, PCI Security Standards Council. "These new eLearning offerings demonstrate our ongoing commitment to promoting the best possible security

see SECURITY STANDARDS on page 3

SECURITY STANDARDS continued from page 3

awareness education, both general and technical, regularly augmenting our course offerings and consistently supporting our PCI certification tracks."

These new courses will be available through the Council's longtime training partner Security Innovation, which employed state-of-the-art educational design techniques to develop an optimal experience for large and small organizations alike.

The PCI Security Standards Council offers educational programs designed to assist organizations who want their employees to better understand the compliance process, as well as courses geared for security firms and industry professionals who seek to assist companies with standards implementation and compliance. Education is also an important component of the Council's Community Meetings, which are held annually in several regions of the globe.

The Council maintains as public resources lists of firms and individuals who have successfully completed certification training, such as Qualified Integrators and Resellers (QIRs), Qualified

Security Assessors (QSAs), Payment Application Qualified Security Assessors (PA-QSAs), and Approved Scanning Vendors (ASVs). Large firms seeking to educate their employees can take advantage of the Internal Security Assessor (ISA) or the PCI Professional (PCIP) educational programs.

To learn more about playing a part in securing payment card data globally, please visit: pcisecuritystandards.org.

Source: Pymnts.com

OFAC Compliance 101

Do you know what an SDN is? More important, do you know if you are doing business with one of them?

An SDN is a "specially designated national" or person, which means you should take special care to avoid doing business with a person who has this designation—or risk running afoul of the Office of Foreign Assets Control (OFAC).

OFAC is the U.S. Department of the Treasury agency that "administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of weapons of mass destruction, and other threats to the national security, foreign policy or economy of the United States."

OFAC maintains an SDN list, which is available here. In addition to individuals, countries, such as North Korea, Iran, and Cuba also appear on the list (Buying Cuban cigars violates OFAC rules).

"OFAC is a concern for a growing number of U.S. companies," notes Gene Truono, managing director, BDO Consulting, which is a division of BDO Seidman, LLP.

Truono ought to know: he oversees his firm's financial institution consulting practice, which includes a hefty emphasis on regulatory compliance initiatives, including anti-money laundering work. Earlier in his career, Truono served as vice president of compliance and ethics and chief compliance officer at American Express Bank Limited.

OFAC compliance can be tricky because:

1. Companies with newly global operations may not be well-versed in the requirements;
2. OFAC rules, along with the names on the SDN list, change periodically;

see OFAC on page 4

9 Cyber Security Tips for Small Business Owners

Small businesses are becoming a larger target for criminals seeking to access sensitive data because attackers are well aware that small businesses have limited resources or personnel dedicated to information system security. Here are 9 cyber security tips for small business owners:

1. **Use the FCC's Small Biz Cyber Planner to create a cyber security plan**. The Small Biz Cyber Planner is valuable for businesses that lack the resources to hire a dedicated staff member to protect themselves from cyber threats. The tool walks users through a series of questions to determine which cyber security strategies should be included in the planning guide, and generates a customized PDF that serves as a cyber-security strategy template.
2. **Establish cyber security rules for your employees**. Establish rules of behavior describing how to handle and protect personally identifiable information. Clearly detail the penalties for violating cyber security policies.
3. **Protect against viruses, spyware, and other malicious code**. Install, use, and regularly update antivirus and antispyware software on every computer used in your business. Such software is readily available online from a variety of vendors.
4. **Educate employees about safe social media practices**. Depending on what your business does, employees might be introducing competitors to sensitive details about your firm's internal business. Employees should be taught how to post online in a way that does not reveal any trade secrets to the public or competing businesses. This type of safe social networking can help avoid serious risks to your business.

see TIPS on page 5

OFAC continued from page 3

3. Compliance can be tricky (Hewlett-Packard received scrutiny after news broke that one of its resellers distributes HP products in Iran).

Large, U.S. corporations with extensive global operations and sophisticated risk and compliance programs typically include OFAC compliance in their normal due diligence (of vendors and customers) and internal auditing processes. Smaller companies just venturing outside the U.S. may not have sufficient steps in place.

Correcting that is not terribly complex.

To begin, recognize and, if necessary, correct two common OFAC compliance misconceptions.

First, many companies overlook the value of documentation. "You might say, "I *know* this individual," or "I *know* this company," but do you really?" Truono notes. "How well do you know them? More important, how well have you documented that you know them? Documentation substantiates your knowledge and understanding of that individual or third party."

Second, failing to uncover any negative information about a new vendor or customer does not mean that your due diligence is complete. "If you don't find any information about a [company or person's] name, that also should raise a red flag," Truono emphasizes. "Why isn't this person or entity more well-known?"

Companies that do not have mature OFAC compliance programs in place should start by ratcheting up the level of due diligence they conduct and by performing a risk assessment of their current portfolio of international trading partners. Truono suggests the following steps:

- **Start due diligence now**. Sometimes, the simplest investigations are the most useful. Start by using the Internet. "I find Google to be a very good first source of information," says Truono, "and it's free." Since Google remains somewhat U.S.-centric in its reach Truono suggests considering using a service to run deeper data-mining on new trading partners if in-house due diligence efforts produce little in the way of documentation. Many of the major accounting and consulting firms offer "investigative due diligence (IDD)" services; sometimes, these services are housed in a consulting firm's Anti—Money Laundering (AML) practice.
- **Examine your trading partners' gatekeepers**. How well do you know their accountants, lawyers, and other advisors, and what type of due diligence have you done on those individuals to ensure that they are legitimate and that there is nothing negative out there about them?" Truono asks. "Taking this step will help protect you from a regulatory perspective, and also from a fraud-prevention perspective."
- **Conduct a risk assessment of your existing portfolio**. Take a page from financial institutions, which are required to conduct risk assessments of their customers. Truono suggests risk-ranking trading partners according to where they are located, how well you know the customer or vendor, and what the types of services or products is involved in the relationship. Ranking trading partners in those risk areas can help risk and compliance managers see what level of additional due diligence as well as ongoing monitoring should be applied to each partner.

"The risk ranking makes sense from an overall business perspective," Truono adds. "It can also help companies avoid fraud losses and credit losses."

Sources: BusinessFinance; Eric Krell

TIPS continued from page 4

5. **Manage and assess risk**. Ask yourself, "What do we have to protect? And, what would impact our business the most?" Cyber-criminals often use lesser-protected small businesses as a bridge to attack larger firms with which they have a relationship. This can make unprepared small firms a less attractive business partner in the future, blocking potentially lucrative business deals.
6. **Download and install software updates when they are available**. All software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install such updates automatically.
7. **Make backup copies of important business data and information**. Regularly backup the data on every computer used in your business. Critical data includes word processing documents, spreadsheets, databases, financial files, human resources files and accounts receivable/payable files. Backup data automatically if possible, or at least weekly.
8. **Control physical access to computers and network components**. Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft, so make sure they are stored and locked up when unattended.
9. **Secure Wi-Fi networks**. If you have a Wi-Fi network for your home business make sure it is secure and hidden. To hide your Wi-Fi network, configure your wireless access point or router so that it does not broadcast the network name, known as the Service Set Identifier (SSID). In addition, make sure that passwords are required for access. It is also critical to change the administrative password that was on the device when it was first purchased.

Click here for a list of cyber security events and webinars.

Sources: U.S Small Business Administration (SBA.GOV); FCC's Cyber Security Tips for Small Business

April is PayItGreen Month

How green are you? You may be greener than you think!

The PayItGreen Seal of Approval allows you to display your efforts to customers, members and peers who care about environmental practices.

By taking a quick, FREE survey your organization can quantify your "green efforts" and earn the 2014 PayItGreen Seal of Approval. Displaying the seal clearly demonstrates that your organization has been independently acknowledged for positively impacting the environment by using and enabling 'green' products and solutions such as Direct Deposit *via ACH*, Direct Payment *via ACH*, eBills and eStatements.

Click here to find out how you measure up by completing PayItGreen's free assessment survey.

You can also measure your organization's Financial Paper Footprint using PayItGreen's Paper Footprint Calculator.

Bitcoins Are Property, Not Currency, IRS Says Regarding Taxes

Wading into a murky tax question for the digital age, the U.S. Internal Revenue Service has said that bitcoins and other virtual currencies are to be treated, for tax purposes, as property and not as currency.

"General tax principles that apply to property transactions apply to transactions using virtual currency," the IRS said in a statement, meaning that bitcoins would be taxed as ordinary income or as assets subject to capital gains taxes, depending on the circumstance.

Bitcoin, the best-known virtual currency, started circulating in 2009. Its present market value is around $8 billion, with up to 80,000 transactions occurring daily, according to accounting firm PricewaterhouseCoopers LLP.

Recent incidents have brought the currency under new regulatory scrutiny, such as the failure of Mt. Gox, a Tokyo-based exchange that filed for bankruptcy after losing an estimated $650 million worth of customer bitcoins.

Unlike conventional money, bitcoin is generated by computers and is independent of control or backing by any government or central bank, which its proponents like, but which also has led to calls for more guidance on U.S. tax treatment.

The IRS supplied that in its statement, which dealt a blow to bitcoin "miners," who unlock new bitcoins online. The IRS said miners must include the fair market value of the virtual currency as gross income on the date of receipt.

This change "is a disincentive to start looking for bitcoins," said John Barrie, a partner with law firm Bryan Cave LLP, who advises charities that receive bitcoins as donations.

see BITCOIN on page 6

BITCOIN continued from page 5

Not Legal Tender

The IRS also said that virtual currency is not to be treated as legal-tender currency to determine if a transaction causes a foreign currency gain or loss under U.S. tax law.

For other forms of gains or losses involving virtual currency, the IRS explained how to determine the U.S. dollar value of virtual currency and said taxable gains or losses can be incurred in related property transactions.

"The character of gain or loss from the sale or exchange of virtual currency depends on whether the virtual currency is a capital asset in the hands of the taxpayer," the IRS said.

If a taxpayer holds virtual currency as capital—like stocks or bonds or other investment property—gains or losses are realized as capital gains or losses, the agency said.

However, when virtual currency is held as inventory or other property mainly for sale to customers in a trade or business, ordinary gains or losses are generally incurred, the IRS said.

Capital gains and losses are taxable and deductible at different rates and amounts than ordinary gains and losses.

Democratic Senator Tom Carper, who chaired a Senate committee hearing last year on bitcoin, said in a statement that the IRS guidance "provides clarity for taxpayers who want to ensure that they're doing the right thing and playing by the rules when utilizing bitcoin and other digital currencies."

Miners Hurt

New bitcoins come from a process called mining. Computer programmers around the world compete to crack an automatically generated code and the first to do so is rewarded with a small stash. This happens about every 10 minutes.

Some online retailers will accept bitcoins as payment. The maximum potential number of bitcoins in circulation is 21 million, compared with around 12 million currently.

On the IRS guidance, William Lewis, a lawyer in Sunnyvale, California, who represents a start-up company creating a platform for virtual currencies, said: "This is going to be unfavorable to bitcoin miners because they're going to have to include in income the fair market value of the virtual currency on the date they mined it.

"It's going to make life difficult for a lot of people who have been mining over the past year, who have to go back and see what the values were on those dates when they mined it."

Source: Reuters; Kevin Drawbaugh; Patrick Temple-West

NACHA Working to Strengthen Safety, Security and Integrity of the ACH Network

NACHA is reviewing potential *Rules* to strengthen the safety, security and integrity of the ACH Network by reducing the incidence of transaction returns and exceptions. A public comment period on these proposed rules changes closed in January. NACHA accepts comments from all Network participants including financial institutions across the country, ACH Operators, service providers, business users and other vested parties, as well as law enforcement, consumer organizations, and financial services regulators.

NACHA received more than 100 responses to the most recent rules proposals, and will give each its due consideration. It is still too early in the review and evaluation process to determine the outcome and next steps, but NACHA intends to make this determination in the near future. Although NACHA does not comment on individual responses received to ensure open and honest feedback, summative findings and proposed plans for moving forward in the rulemaking process in will be shared.

Background

On November 11, 2013, NACHA - *The Electronic Payments Association* issued a Request for Comment (RFC) on two proposed rules that serve as complementary approaches to improve ACH Network quality. As components of NACHA's Risk Management Strategy, both proposed rules support NACHA's holistic and interconnected approach and the consumers, governments, businesses and financial institutions that use the Network every day.

Specifically, the two proposals would amend the *ACH Rules* and provide new ways to reduce incidents of exceptions—or payments that do not process through the ACH Network flawlessly—thus increasing overall ACH Network quality. The first of the two proposed rules would improve NACHA's ability to identify and enforce *Rules* against "outlier" Originators that are responsible for the highest, and most disproportionate, levels of exceptions. The second would establish economic incentives for Originating Depository Financial Institutions (ODFIs) and their Originators to improve origination quality, and provide partial cost-recovery to Receiving Depository Financial Institutions (RDFIs) for handling exceptions.

For more information on NACHA's rulemaking process, please visit www.nacha.org/RMprocess.

Source: NACHA

More Than Eight Million Healthcare EFTs via ACH in January

More than eight million healthcare electronic funds transfers (EFTs) *via ACH* were made in January 2014, the first month in which health plans were required to be compliant with the newly adopted healthcare EFT standard transaction, according to NACHA. Speaking at a hearing of the U.S. Department of Health and Human Services (HHS) National Committee on Vital and Health Statistics' (NCVHS) Subcommittee on Standards, Janet O. Estep, president & CEO of NACHA, testified that in January, there were a total of 8,154,530 healthcare EFTs *via ACH*. These transactions moved approximately $45 billion from health plans to providers.

In October 2012, NACHA's members approved changes to the *NACHA Operating Rules* to support the healthcare EFT and electronic remittance advice (ERA) standards designated by HHS, and the CAQH CORE healthcare operating rules for EFT and ERA. These changes became effective on September 20, 2013, and allow NACHA, the standards organization for the EFT *via ACH* transaction, to identify and track the number of healthcare EFTs that are transmitted using the ACH Network. Since the *ACH Rules* changes became effective, the ACH Network has processed more than 28 million healthcare EFTs *via ACH*, totaling more than $144 billion. "Even with no additional growth in the use of the standard for the rest of the year, the ACH Network would move 100 million healthcare EFTs in 2014, and transfer more than $540 billion from plans to providers," said Estep.

During her testimony before the NCVHS Subcommittee on Standards, Estep shared that based on the data, "implementation of the EFT standard appears to have been reasonably smooth," but also that providers' use of the EFT standard can be "impacted when they are not informed of choice in the method to receive claim payments." Providers have the right to receive EFT standard transactions. Use of the healthcare EFT standard with remittance advice will help the healthcare industry save between $3.2 million and $4.6 million over 10 years[1]. With health plans making EFT payments to providers *via ACH*, the full benefits anticipated through this technology can be achieved by the industry.

For more information about the healthcare EFT standard and healthcare EFT and ERA Operating Rules, visit **healthcare.nacha.org**.

Source: NACHA

[1] www.federalregister.gov/articles/2012/01/10/2012-132/administrative-simplification-adoption-of-standards-for-health-care-electronic-funds-transfers-efts

CFPB Scrutinizes Consumer Deposit Advance Products

The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) imposes sweeping regulations on nearly all aspects of consumer lending. In addition to establishing these new rules, Dodd-Frank also created the Consumer Financial Protection Bureau (CFPB) to enforce them. While most of the CFPB's regulatory authority applies to all consumer lenders, certain provisions apply only to specific types of non-depository creditors, including payday lenders. The result is the CFPB's new power to regulate payday lenders, as well as the ability to levy substantial penalties on those who violate federal consumer financial law. Payday lenders need to become familiar with the new regulations in order to implement procedures to protect themselves.

The CFPB's Regulatory Power Over Payday Lenders

Under Dodd-Frank, the CFPB has been granted the authority to punish any unfair, deceptive or abusive act or practice by a seller of a consumer financial product. Dodd-Frank broadly defines an "abusive act or practice" as one that:

1. Materially interferes with the ability of a consumer to understand a consumer financial product or service, or
2. Takes unreasonable advantage of:
   a. A consumer's lack of understanding of the material risks of the product.
   b. The consumer's inability to protect his or her own interest in using the product.
   c. The consumer's reasonable reliance that the provider of the product would act in the interest of the consumer.

The CFPB's examinations procedures for the payday lending industry suggest several ways in which payday lenders may violate this standard, including a lender's failure to disclose check cashing fees, material terms

see CFPB on page 8

CFPB continued from page 7

of a financial product or the consumer's rights regarding payment. Because of Dodd-Frank's all-encompassing definition of "abusive acts," payday lenders will likely face increased scrutiny over their products. Such lenders should create procedures to ensure compliance with these disclosure requirements.

The CFPB's Supervisory Power over Payday Lenders

To help the CFPB investigate and identify suspected violations of federal consumer financial law, Dodd-Frank gives the CFPB broad supervisory powers over payday lenders. Under Dodd-Frank, the CFPB is required to collect reports and conduct examinations of payday lenders for the purpose of (1) ensuring compliance with federal law, (2) obtaining information about the payday lender's procedures to prevent violations, and (3) detecting risks to consumers created by the products offered by payday lenders.

In addition, the CFPB can create rules requiring payday lenders to generate, provide or retain records to assist in the supervision. The CFPB even has the authority to impose background checks on principals, officers, directors and other personnel of the payday lender to ensure that such lenders are "legitimate entities." Failure to respond to the CFPB's request for information can result in a court order for contempt.

The CFPB's Enforcement Power over Payday Lenders

The CFPB's role does not end at supervision; if it detects a violation of federal consumer financial law, it has the power to impose substantial penalties on the offender. The CFPB generally has two levels of enforcement power: cease and desist orders and civil penalties. If the CFPB discovers a violation, it may send a letter ordering the suspected offender to cease and desist the offending behavior. If the suspected offender does not respond within 30 days, the order automatically becomes effective.

The CFPB also has the authority to bring a civil action against a suspected offender in the District Court of the district where the offender is located. Damages may include restitution, payment of damages, return of money or property and public notification regarding the violation. In addition, the Act also imposes substantial civil penalties for violations of federal consumer financial law. These penalties are as follows:

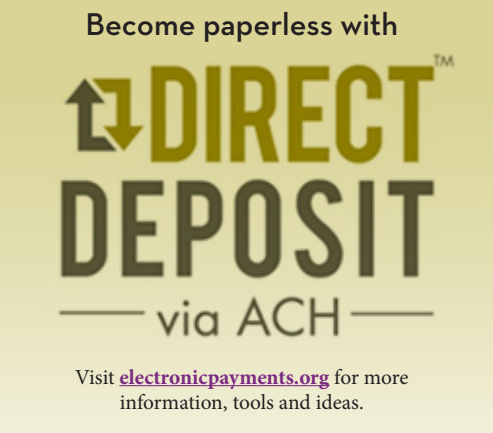
a. For any violation, a fine of up to $5,000 for each day that such violation continues.
b. For a reckless violation, a fine of up to $25,000 for each day that such violation continues.
c. For a knowing violation, a fine of up to $1,000,000 for each day that such violation continues.

Conclusion

The CFPB will undoubtedly attempt to snare payday lenders under the expansive "abusive acts and practices" prohibition. If it finds evidence of such practices, or any other violation of consumer financial law, it will impose substantial penalties that most small, non-traditional lenders cannot afford to pay. Payday lenders should implement procedures, such as periodic monitoring reviews by management or a regular independent compliance audit, to ensure that they are making the necessary disclosures, preserving all loan documentation and minimizing the risk of violating these new regulations.

Source: Henry E. Hildebrand; Baker Donelson Bearman Caldwell & Berkowitz PC

Fast Facts about Direct Deposit via ACH



Every year paper checks use more than 674 millions gallons of fuel!

Direct Deposit *via ACH* is the electronic transfer of funds from a company or government agency into an individual's checking and/or savings account.

These transfers:

- Include payroll, travel and other employee reimbursements, tax and other refunds, pension/401K disbursements, dividends, bonuses, and more
- Can be split between checking and savings accounts
- Never get lost or stolen
- Are confidential, reducing fraud and identity theft
- Help protect the environment

Calculate your savings at ElectronicPayments.org.

Target Breach Lesson: PCI Compliance Isn't Enough

"Compliance can protect us from liability, but whether it actually protects us from loss of business and loss of data is not so clear," said PerfectCloud CTO Vijay Murty. "Compliance is a minimal deterrent that everyone has to have in place. ... If you're driving a car, you're expected to have a driver's license. That doesn't make you a safe driver."

"Target was certified as meeting the standard for the payment card industry in September 2013. Nonetheless, we suffered a data breach." Those words by Target Chairman, President, and Chief Executive Officer Gregg Steinhafel affirmed what security experts know as gospel: Compliance does not equal security.

"Just because you pass a PCI audit does not mean that you're secure," said Eric Chiu, president and founder of HyTrust. "Clearly we saw that in the Target scenario."

PCI standards can suffer from a common regulatory affliction.

"A standards body takes many years to develop a standard," Chiu told TechNewsWorld. "In that time frame, threats change."

In the retail sector, Target was a security standout when it passed its PCI audit in September.

"The lesson here is even if you're pretty vigilant and at the top of your industry, being secure today doesn't mean being secure tomorrow," Sonali Shah, vice president of products for BitSight, told TechNewsWorld.

Opiate for Executives

While CEOs may not know that, security pros do. Compliance rules are formulated with the best of intentions, but they can be an opiate for denizens of corner offices.

"Compliance can give you a false sense of security," said Vijay Kumar Murty, CTO of PerfectCloud.

"Compliance can protect us from liability, but whether it actually protects us from loss of business and loss of data is not so clear," he told TechNewsWorld.

"Compliance is a minimal deterrent that everyone has to have in place. That doesn't give us complete assurance that everything is OK," Murty said.

"If you're driving a car, you're expected to have a driver's license," he pointed out. "That doesn't make you a safe driver."

Source: TechNewsWorld; John P. Mello Jr.

5 Issues That Could Hamper EMV Smartcard Adoption in the U.S.

Migrating U.S. payment systems to the Europay MasterCard Visa (EMV) smartcard standard could take significantly longer than envisioned and offer fewer security benefits than what's being touted by proponents of the technology.

In the weeks following the massive data breach at Target, the EMV standard has received considerable attention from stakeholders in the payment industry and from lawmakers.

Cards based on the EMV standard use an embedded microprocessor instead of a magnetic stripe to store cardholder data. Typically, cardholders need to authenticate themselves with a Personal Identification Number (PIN) when using the card.

Chip-and-PIN credit and debit cards are considered significantly safer than magnetic

see ISSUES on page 10

Mobile Payment Fraud Especially Risky for Small Business

As mobile payment options become more prevalent among small businesses, so too do the opportunities for fraud, new research shows.

A study by LexisNexis and Javelin Strategy & Research discovered that smaller mobile merchants—small businesses that accept at least one type of payment through either mobile browsers, mobile applications or mobile point-of-sale systems—rely on fewer fraud-prevention solutions, meaning they are often more exposed to deceptive schemes.

Specifically, smaller mobile merchants use an average just two different types of fraud-technology solutions, compared with an average of four types for larger businesses. Fraud-technology prevention includes such tools as PIN and signature authentication, check verification services, transaction and customer profile databases, browser/malware tracking, IP geolocation and real-time transaction tracking tools.

The use of more prevention techniques is helping larger businesses stop significantly more mobile fraud attempts than small businesses. The research revealed that large retailers that accept mobile payments prevent nearly eight times as many fraudulent transactions as smaller merchants do.

"Mobile payment options and point-of-sale hardware are providing more business opportunities for small merchants," said Dennis Becker, vice president of corporate markets and identity management solutions for LexisNexis. "Despite the surge in retailers using mobile payments to conduct business, we've found in our study the unfortunate correlation between the size of the business

see MOBILE on page 10

MOBILE continued from page 9

and the impact of mobile fraud on their business."

The study found that mobile fraudulent transactions result in nearly three times the cost of the actual product stolen. That means that for every $1 worth of product that is stolen, the merchant experiences additional costs for things like chargeback fees, payment-processing expenses, fraud investigation and restocking of lost merchandise. On average, the total of direct and indirect costs equals $283 lost for every $100 of direct fraud loss, the study found.

Overall, 22 percent of the mobile merchants surveyed said fraud incidents increased over the last year, compared with just 6 percent who said incidents dropped in 2013.

The research shows that credit-card fraud is one of the largest threats facing mobile merchants. Nearly three in five fraudulent transactions were credit-card-based, while only 23 percent were attributable to debit cards.

Identity theft is also a major problem for mobile merchants. The study discovered that 21 percent of mobile merchants have experienced fraud via identity theft, compared with just 17 percent of all retailers.

The researchers offered several recommendations to help mobile merchants combat fraud:

Mobile merchants selling digital goods should thoroughly authenticate card-not-present transactions through mobile devices. Mobile e-commerce merchants should take extra care to verify the identity of both the consumer and the device, to mitigate fraud through identity theft.

Combine a mobile app with strong authentication to counter the threats of payment compromise and identity fraud. With authentication solutions, such as device fingerprinting, merchants can establish identity while protecting consumer payment data.

Identify fraudulent mobile transactions separately from online transactions, to better understand the risk and mechanisms associated with the channel. In the study, only 48 percent of mobile merchants said they track fraud by payment channel.

Maintain open communications with financial institutions and other mobile merchants to better understand the evolving nature of fraud threats and solutions. Groups such as the Merchant Risk Council provide forums for sharing expertise and assessing concerns.

The study was based on surveys of 1,139 risk and fraud decision makers and influencers. They included representatives from companies of all sizes, industry segments, channels and payment methods.

Source: BusinessNewsDaily; Chad Brooks

ISSUES continued from page 9

stripe cards used in the U.S. Though the rest of the world moved to chip-and-PIN long ago, the U.S., for a various reasons, has lagged in adopting the technology.

But the Target breach appears to have convinced many that the time has finally come to cast aside reservations about EMV and move to it wholesale.

Even before the breach, MasterCard and Visa announced that they want merchants and card issuers to be ready for EMV card transactions by October 2015. They have noted that the liability for any fraud that occurs at point-of-sale terminals will shift either to the merchant or the card-issuing bank after that date.

If the retailer's point-of-sale systems are EMV-ready but the card-issuing bank's cards are not EMV-compliant, the cost of any fraudulent transactions associated with those cards would be borne by the bank after October 15, 2015. On the other hand, if the bank is EMV-ready but the merchant's POS does not support the technology, the merchant would bear responsibility for any fraud.

Gas station owners will have an additional two years to migrate automated fuel dispensers to EMV before the liability switch occurs.

Despite continuing reservations about the deadlines, MasterCard and Visa solidified their plans only in the weeks since the Target breach. Senior executives from both card associations publicly confirmed their intention to stick with their EMV implementation roadmaps, citing the Target breach as an example of why the move is needed.

The problem is that moving over the EMV won't be easy, but it will be expensive.

1. Upgrading to EMV will cost billions

One of the biggest obstacles is cost. POS systems capable of reading EMV cards can cost hundreds of dollars apiece. Retailers like Target can expect to pay tens of millions of dollars just swapping out the hardware. In addition, they will also need to spend on software, testing and deployment.

Gray Taylor, executive director of the Petroleum Convenience Alliance for Technology Standards (PCATS), a trade group representing convenience store and petroleum retailers, expects his industry will have to spend up to $4 billion to swap out an estimated 800,000 POS systems.

Gray estimates that across the U.S., merchants will need to either replace or upgrade an estimated 13 million POS systems to be ready for EMV card transactions. "That is a big expense that we are going to have to pass down to the consumer," Taylor said.

In addition, card-issuing banks will need to spend tens of millions to upgrade their networks and internal systems if they want to be ready for PIN debit and PIN credit transactions.

2. Security ROI still iffy

It's not clear if the investments will yield the kind of security benefit that many assume it will.

That's because the EMV standard can be implemented in a variety of ways. A majority of EMV implementations around the world

see ISSUES on page 11

ISSUES continued from page 10

require cardholders to enter a PIN as an authentication measure when conducting a transaction. These kinds of Chip-and-PIN EMV implementations are believed to yield the strongest security benefits.

But EMV can also be implemented in less secure ways. For example, EMV can be implemented simply as a chip card without a PIN, or as a chip card requiring either a signature or a PIN to authenticate the cardholder. Such smartcard implementations still offer more security than magnetic stripe cards, but they are less secure than chip-and-PIN formats.

MasterCard and Visa have left it largely to the card-issuing banks in the U.S. to decide which route they want to take.

But without a mandatory PIN requirement, any move to EMV standards in the U.S. is half-baked at best.

"It is not the enhanced security system that retailers have long-called for," says Brain Dodge, senior vice president of communications at the Retail Industry Leaders Association (RILA). "There is an enormous cost with moving systems to EMV. From the retailers' perspective, the added protection we are getting (from smartcards) is not enough to justify the expense," without a mandatory PIN requirement, Dodge said.

3. Not just a PIN issue

EMV implementation plans in the U.S. also permit the use of a magnetic stripe on the back of the card. This further weakens any benefits that might be gained from having a smartcard in the first place, said James Huguelet, an independent consultant who specializes in retail security.

In addition, EMV implementation plans do not require encryption of cardholder information on all transactions, which is another major weakness, Huguelet said.

For instance, EMV technology would have done little to prevent data thieves from harvesting credit and debit card data from Target's POS systems because the data was grabbed before it could be encrypted.

Even if all such issues were to be magically solved, EMV alone does nothing to make online and mobile payment methods more secure, Huguelet said. EMV cards are fundamentally designed to make so-called card present transactions more secure. The technology makes it harder to clone cards and use them to make fraudulent transactions. However, they are of less use in card-not-present situations such as online or mobile transactions.

In the wake of the Target breach, "there is a meme that has developed that the U.S. isn't moving quickly to EMV—[and] if it did, that will make consumers safe," Huguelet said. "But there are several inconvenient truths to the current state of EMV in the U.S. that this sort of storyline ignores."

Seth Eisen, senior business leader with MasterCard North American Markets, downplayed such concerns. He noted that the liability structure under the proposed EMV model would be incentive for both U.S. banks and retailers to implement the most secure form of EMV.

"The terminal where the transaction takes place would determine the technology for the liability shift. If that terminal is not EMV and the card is, then the merchant is liable for any counterfeit fraud," Eisen said.

"After the liability shift goes into effect, the party that has the lower security standard will be liable for fraud if that were to take place." So banks and retailers have equal incentive to move to the strongest form of EMV, he said.

Visa did not respond immediately to a request for comment.

4. Time is also an issue

Moving the entire U.S. payment system to EMV will take a whole lot longer than October 2015 deadline.

Canada first began moving to EMV in 2003. More than 10 years later, only about 85% of the country's POS systems can take EMV cards, Taylor from PCATS said, and that's in a country with a more centralized payment system and far fewer POS systems, compared to the U.S.

Meanwhile, in countries where merchants have almost completely shifted to EMV-enabled POS systems, the banks have been slow to issue smartcards, Taylor said.

Migrating the U.S. payment system to EMV will take years, and by the time the process is complete, most payments would have shifted to mobile and online applications, Taylor said. "Visa and MasterCard are hell bent on making us homogenous with the rest of the world. But the fact is that we're going to be the last guys in on an aging technology."

Instead of focusing so much on EMV standards, the effort should be to develop technologies and techniques for securing payment methods of the future, Taylor said. In the meantime, several options are available to make payment technology safer, including end-to-end encryption, tokenization and mandatory PIN use, he noted.

5. Legal obstacles

One other obstacle to EMV adoption in the U.S., at least as far as retailers are concerned, has to do with the manner in which debit PIN and debit signature transactions are routed for processing.

Under a federal measure known as the Durbin Amendment, merchants are supposed to have a choice of at least two independent networks for processing debit transactions. The measure is aimed at increasing competition and reducing the controversial "interchange" fees that merchants pay banks and credit unions for each debit transaction.

However, a legal dispute between banks and merchants over a court's interpretation of the Durbin Amendment's intent has delayed implementation of the measure. In mid-March, a three-judge panel of the U.S. Court of Appeals for the District of Columbia Circuit overturned a decision by a federal district court that had previously struck down the Federal Reserve Board of Governors' rule related to debit interchange fees and payment network routing practices. In response to the appeals court decision, retail industry trade groups have announced that they are considering a further appeal.

Source: Computerworld; Jaikumar Vijayan

Cyber Insurance Policies

If the last year has proved anything it's that no organization is immune to cyber-attacks. Some of the most sophisticated PCI-compliant companies in the country have fallen victim, and recent trends show an increase in attacks against small and mid-sized businesses, ones whose networks are likely not as sophisticated. Attacks will continue to happen to businesses of all sizes, regardless of the nature of their business. Every company in this country has something criminals want. Another more alarming trend is that many businesses don't understand the hefty price tags associated with these incidents.

The Ponemon Institute reports that U.S. organizations spend an average of $565,020 on post-breach notifications alone (i.e. notifying consumers that their information was compromised or was potentially compromised, generally required by state law). Ponemon also reports that, on average, a business loses an additional $188 per compromised consumer record ($277 in the case of malicious attacks) and that in 2012 the average number of breached records per incident was 28,765, for a total of $5.4 million.

In addition to expenses related to reporting, businesses also face lawsuits, especially when consumer data is compromised. And when you factor in government and regulatory investigations (like the FTC), fines and penalties, reputational damage, and even payment network fines such as those issued by the Payment Card Industry, I think you can see why some businesses attempt to recover losses via insurance policies.

Analyzing Commercial General Liability Insurance Policies

Numerous reports indicate businesses frequently turn to their insurance company to recover costs associated with breaches; yet many claims are denied by insurance companies citing that Commercial General Liability (CGL) Policies do not extend to cyber-attacks. Case and point, more than half of the private companies interviewed for the new Private Company Risk Survey by Chubb Corp. said that they chose to forego certain types of liability insurance because they felt they were already covered through their Commercial General Liability Insurance policy. While CGLs do cover a great deal, they do not cover everything.

For example, a typical Commercial General Liability Policy does not cover (Source):

- **Directors and Officers Liability**. This would be a situation in which someone accuses one of your directors or officers of foul play that resulted in financial harm. This is most often a concern for nonprofit businesses.
- **Employment Practices Liability**. This includes harassment, discrimination or retaliation related to employment.
- **"Expected or Intended" Incidents**. This includes expenses related to workplace violence.
- **Fiduciary Liability**. This includes breaches of fiduciary duty.
- **Errors & Omissions Liability**. Expenses related to professional errors or mistakes.
- **Employee Theft/Dishonesty Liability**. This liability involves incidents related to employee fraud.
- **Cyber Risk Liability**. Costs associated with data breaches when private company information is compromised.

Another troubling aspect of the Chubb report is that 44% of the surveyed companies experienced at least one of the above loss events in the past three years. It's estimated that only 5% of private companies carry Cyber Risk Liability Insurance despite the uptick in data breaches of businesses across the country.

Many businesses found out the hard way that their CGL didn't protect them as fully as they thought it would. In fact, a number of businesses have filed lawsuits against their insurance provider attempting to recover costs they felt should have been covered under the CGL, but the insurance company denied the claim. I'm not going to recap the court cases here. If you would like more information I suggest you read Another Reason to Consider Cyber Insurance.

In light of these recent findings and lawsuits waged by businesses who thought their CGL covered cyber-related incidents, the Insurance Services Office definitely states that effective May 1, 2014, CGLs will not cover cyber-attacks or any related expenses. Businesses will have to have a unique cyber insurance policy to cover such incidents.

Cyber Policies

Cyber insurance policies go by many names, but they are designed to cover losses associated with cyber-attacks and data breaches. While cyber insurance policies can be extremely valuable, selecting and negotiating the right cyber insurance product presents significant challenges, especially for small businesses. There are an overwhelming array of cyber products on the marketplace, each with its own insurer-drafted terms and conditions, which vary dramatically from one insurer to another.

Some policies only cover hardware (i.e. computers, servers, etc.), not consumer record expenses. Others include losses related to consumer records and account takeovers (i.e. criminals gained access to your credentials and submitted fraudulent Wires or ACH Files). More than a few have extremely high deductibles which could make the policy useless to a small business. It is very important that businesses weigh policy

see CYBER on page 13

CYBER continued from page 12

options carefully and ensure they are selecting a policy that meets their unique needs.

Businesses need to carefully evaluate what they need insurance for, considering all possible impacts of a cyber-attack or compromise, including legal and reputational repercussions, lawsuits, fines and penalties, lost income if the business is unable to operate, etc. To accomplish this, it's recommended that a business identify needs and then consult with legal counsel and IT professionals before attempting to negotiate with an insurance broker.

For more information, consult legal counsel or review the following resources:

PRIVACY ALERT: GET READY! NEW CYBER EXCLUSIONS COMING IN MAY 2014

Another Reason to Consider Cyber Insurance | Insurance Thought Leadership

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.

NACHA DIRECT MEMBER
Regional Payments Association®

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

www.epcor.org
3100 Broadway, Ste. 609, Kansas City, MO 64111
800.500.0100 | 816.474.5630 | fax: 816.471.7665