epcor®
Electronic Payments Core of Knowledge

INSIDE ORIGINATION

2016 *ACH Rules* Changes That Could Impact You

Are you up-to-date on the 2016 *ACH Rules* changes? As an Originator of ACH entries it is important to stay up-to-date with the *ACH Rules*, including updates and changes as they arise.

Need more information? Download the [*2016 ACH Rules Update for Originating Companies*] to find out which *ACH Rules* changes may apply to you. Be sure to contact your financial institution with questions regarding how these changes pertain to your current Origination activity.

Annual Report Projects Significant Increase in Phishing Attempts

Wombat Security Technologies recently released their annual 2016 State of the Phish Report, which reveals the results of a survey of hundreds of security professionals as well as data compiled from millions of simulated phishing attacks sent between October 1, 2014, and September 30, 2015. The report reflects the reality that Chief Information Security Officers, Chief Security Officers and their information security teams are facing worldwide on a daily basis: phishing and spear phishing attacks are more prevalent — and more dangerous — than ever.

Survey Says...Attacks, Victims Continue to Rise

Three key data points from the survey show year-over-year increases related to frequency and susceptibility to attacks:

- 85% of respondents said they were a victim of a phishing attack (up 13% from the prior report)
- 67% said they experienced a spear phishing attack (a 22 % increase)
- 60% said they believe the rate of phishing attacks has increased overall

see PHISHING on page 2

57 Percent of Shoppers Still Prefer Stores

Brick-and-mortar shopping isn't dead, but it is certainly on the decline: just 57% of urban consumers said they preferred to make discretionary purchases in stores, while 39% claim their last such purchase was made online.

The internet is playing an increasingly critical role in the path to purchase, according to a new study from Aptos. The commerce platform polled shoppers in three large metropolitan markets and found that city dwellers in Chicago, Los Angeles and New

see SHOPPERS on page 2

SHOPPERS continued from page 1

York had some distinct shopping preferences.

It also found a common thread—the use of Amazon as a research tool. Roughly 32% of shoppers said they used retailers' websites to research their most recent purchases, but 22% used Amazon even when purchasing elsewhere. More survey participants used Amazon for research and inspiration than Facebook, Pinterest, Twitter, Instagram and blogs combined.

Mobile, of course, played a large role with 40% of shoppers using mobile devices and apps to research purchases.

Shoppers showed a keen interest in having access to a wide range of delivery options. Forty-six% ranked "ship to neighborhood locker locations" as the most important delivery option while 23% cited "shop in-store, ship to home."

Same-day delivery was popular with 34% of respondents, while buying online and picking up in store was preferred by 24%.

The study confirms that consumers in dense urban areas have different needs and priorities than those in suburban and rural communities. Retailers' push to provide ship from store, such as Lowe's urban format in New York, and same-day delivery are good efforts to meet those needs.

Source: Fierce Retail

PHISHING continued from page 1

So, what are the ramifications of a successful phishing attack? From Wombat's perspective, it's a question of means and ends; attackers have different means of exploiting their access, just as they have different end games — and those end games have different implications for the organizations targeted. When asked about the technical issues that resulted from successful phishing attacks on their organizations, respondents indicated that they faced the following:

- Malware infections (42%)
- Compromised accounts (22%)
- Loss of data (4%)

Looking beyond the technical side of phishing, Wombat also asked respondents to identify the business impacts associated with successful attacks:

- 44% complained of lost employees productivity
- 36% faced consequences related to the loss of proprietary information
- 20% dealt with damage to their reputation

In general, the report shows that more aggressive social engineering practices are making phishing more difficult to prevent. Case in point, 55% of survey respondents reported experiencing voice phishing (vishing) and/or SMS/text phishing (smishing). Given that email-based attacks are often preceded by information gathering efforts like phone calls, social media trolling and even in-person reconnaissance, it's clear that cyber security is a many-faceted thing.

Data Says...Personalization, Topics Matter

As the report mentions, the survey told only one side of the phishing story. Wombat also looked to the data generated through their simulated phishing attack tools over the course of a year (October 2014 through September 2015). They analyzed a variety of data points, including the types of templates used during the simulated attacks, endpoint vulnerabilities discovered, and the types of emails reported by end users. In doing so, they gained important insights into end-user behaviors and the factors that drive employees to click and interact with emails.

Templates and Click Rates

- Personalization increases engagement. Emails that included users' first names had a 19% higher average click rate than messages with no personalization.
- Organizations used corporate-style templates in 56% of their mock attacks. Consumer-style templates were used in 29% of simulated messages.
- The most popular attack template used by organizations in 2015 was an electronic fax notification message. It had an average click rate of more than 15%. Another popular attack was an Urgent Email Password Change request, which had an average failure rate of 28%.
- Employees were most likely to click on emails that they expected to see in their business inboxes, including HR documents and shipping confirmations. They were more cautious with "consumer-oriented" emails like gift card offers and social networking notifications.

Wombat Says...Awareness, Education Training Can Help

In looking through the report, you're likely to notice something they noticed as well: When asked what they use to protect themselves from phishing, a whopping 99% of respondents indicated they used email spam filters. This helps to prove an important point: spam filters cannot catch everything.

"Phishing continues to be a highly effective attack vector that is increasingly responsible for a significant percentage of data breaches in the market today," said Trevor Hawthorn, Chief Technology Officer for Wombat. "In spite of continued investments in a number of popular security technologies, phishing messages continue to reach end users and can result in serious damages to a company's critical data and reputation."

see PHISHING on page 3

PHISHING continued from page 2

The good news is that security awareness training helps to reduce click rates. The report shows that companies that used simulated phishing attack products were able to reduce click rates by 50% after two years.

"Our methods have shown that a Continuous Training Methodology, which educates end users on cyber security threats, changes employee behavior and reduces risk within an organization," said Hawthorn.

The simple fact is that lowering click rates lowers costs and improves the productivity of employees in general and information security teams in particular. As was noted in a 2015 Ponemon Institute study sponsored by Wombat, the majority of costs caused by successful phishing attacks are the result of the loss of employee productivity and uncontained credential compromise, among other factors—and these cost an average-sized company $3.77 million per year.

Source: Gretel Egen, Wombat Security

EPCOR's Third-Party Senders Agree to NEW! Third-Party Guiding Principles

epcor

Third-Party Sender Guiding Principles

The Guiding Principles were developed by EPCOR's Third-Party Sender Forum* as a means to demonstrate each company's commitment to compliance and ethical business practices to their financial institution partners, customers and the collective payments industry.

Tenet 1

Be dedicated to the concepts of effective and reliable financial networks and believe that processing with integrity and compliance with all laws and rules is essential to the achievement of this objective.

Tenet 2

Recognize that at all times the chief function of a Third-Party Sender in the ACH Network is to serve the needs of the Originator and Originating Depository Financial Institution as well as the Receiver and the Receiving Depository Financial Institution in accordance with the ACH Rules, all applicable laws and regulations and agreements.

Tenet 3

Be dedicated to the highest ideals of honor and integrity in managing and facilitating the flow of funds on behalf of an Originator.

Tenet 4

Make it a duty to continually improve the competence and training of personnel in the rules and "best practices" to insure the integrity of the ACH and banking network.

By agreeing to the NEW! Third-Party Guiding Principles EPCOR's Third-Party Sender members pledge to abide by 10 tenets to demonstrate their integrity.

INTERESTED IN DOING THE SAME?
CONTACT KIMBERLYM@EPCOR.ORG
TO LEARN MORE.

NACHA Proposes Third-Party Sender Registration

Last August, NACHA issued a request for comment (RFC) on a proposed rule that would require Originating Depository Financial Institutions (ODFIs) to register their Third-Party Sender (TPS) customers with NACHA. The RFC generated significant industry feedback, including a number of suggestions and requests for modifications. As a result, NACHA is proposing to make several changes to the Original Proposal.

This proposal on Third-Party Sender Registration will benefit the ACH Network by ensuring that all Originating Depository Financial Iinstitutions (ODFIs) undertake a deliberate review of whether or not they have Third-Party Sender customers. Additionally, for those ODFIs that do have Third-Party Sender customers, the proposal will establish and standardize baseline information that the ODFI should know and possess on each TPS customer as well as any "nested" Third-Party Sender. In these two ways, the proposal intends to level the playing among ODFIs field by furthering the performance of appropriate due diligence by all ODFIs.

Third-Party Senders are already required under the ACH Rules to provide the ODFI with certain information, upon the ODFI's request, to aid the ODFI in knowing with what other organizations the Third-Party Sender does business.

In the Original Proposal, NACHA proposed that Third-Party Senders also would be required to provide the ODFI with the information necessary for the ODFI to complete the registration of the Third-Party Sender. Commenters to the proposal identified additional reporting requirements; namely, that a Third-Party Sender should disclose to its ODFI any of its customers that are also Third-Party Senders.

Some ODFIs have said that the identification of such "nested" Third-Party Senders can be challenging, and that they would benefit from having additional tools or means by which to know when these relationships exist. The revision to the Original Proposal, therefore, would require a Third-Party Sender to disclose to the ODFI any of its customers that are also Third-Party Senders, prior to transmitting entries to the ODFI for that other Third-Party Sender. This revision would aid an ODFI in its know-your-customer due diligence, and also provide the ODFI with the information necessary to comply with its registration requirements.

If this proposed change is approved, it would result in your ODFI being required to report their relationship with any Originators who are Third-Party Senders to NACHA. To read more about this proposed change to the , refer to NACHA's website.

Source: NACHA

Simplify Your Payment Processes with Direct Deposit and Direct Payment *via ACH*

May is officially Direct Deposit and Direct Payment *via ACH* Month, and it's right around the corner! If you don't currently utilize Direct Deposit *via ACH* for your payroll, don't you think it's time you started?

Direct Deposit is convenient and secure, both for you and for your employees. It just makes business sense. Here are just a few ways it will save you time and money:

- It simplifies your payroll processes
- It reduces the risk of fraud
- It increases confidentiality
- It transfers funds securely
- It helps protect the environment

DIRECT™ DEPOSIT via ACH

It's easy to get started—simply click this link to get up-to-speed on everything you need to know.

And don't forget Direct Deposit's twin—Direct Payment *via ACH*. What works well with deposits also works well for paying your invoices. Direct Payment is easy to set up and use. It can automate your accounts payable and receivable process, result in a more predictable cash flow and reduce your administrative costs. Learn more today!

The Top Ways Cybercriminals Are Picking Retailers Pockets

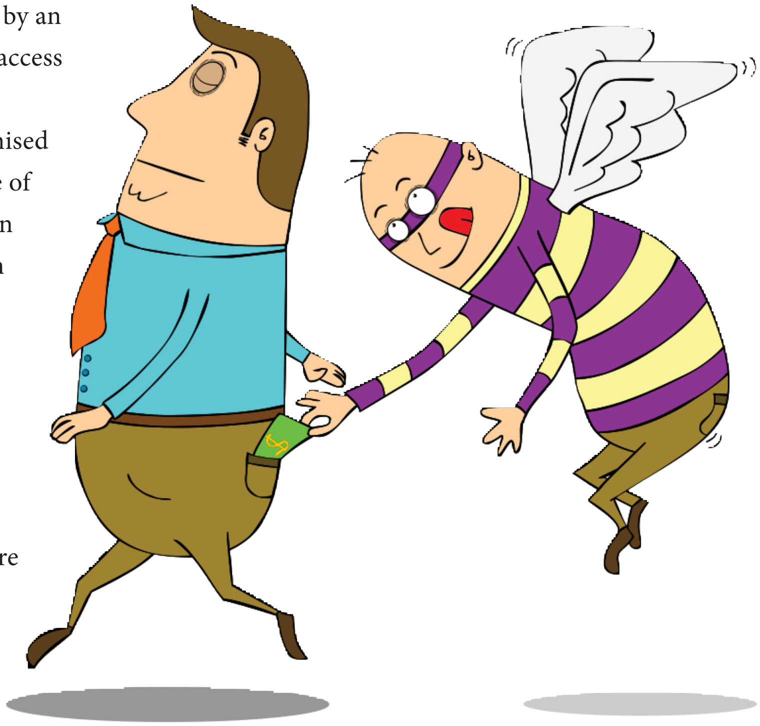
You may have heard an iconic line attributed to infamous bank robber Willie Sutton: When asked why he robbed banks, he responded by saying "because that's where the money is." Here we are all these years later, and the story is no different regarding the security of point-of-sale (POS) systems in retail environment. Criminals seek out these systems because they know that's where they can gain access to a large number of records of customer data, specifically credit and debit card information.

How Do Cybercriminals Steal Customer Data?

Here are two common attack vectors and some details on what can be done to keep such systems mostly immune from attack:

1. Malware Infections

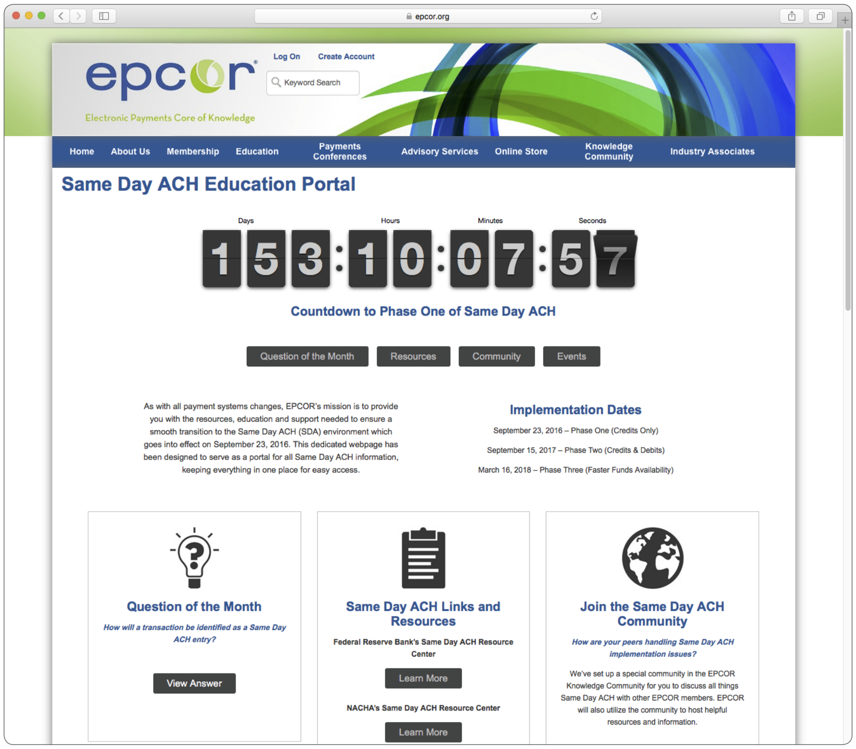
Malware that extracts magnetic stripe data directly out of the POS computer's memory is the biggest concern facing retailers. This malware can be installed by an attacker who has gained access to the network via other means (such as compromised credentials, as in the case of the Target breach) or even social engineering. Given the open nature of retail environments and the high turnover rate of employees, there are other possible attack avenues, as well, such as the installation of malware directly onto the POS system via a thumb drive.



There are plenty of big-box retailers running highly vulnerable and unsupported Windows XP and Windows 2003 servers at this very moment. That's not necessarily bad in and of itself, as long as there are compensating controls such as advanced malware protection and positive security white-listing systems that control what runs on the registers.

see POCKETS on page 5

EPCOR Introduces Same Day ACH Education Portal



Same Day ACH Education Portal

Countdown to Phase One of Same Day ACH

As with all payment systems changes, EPCOR's mission is to provide you with the resources, education and support needed to ensure a smooth transition to the Same Day ACH (SDA) environment which goes into effect on September 23, 2016. This dedicated webpage has been designed to serve as a portal for all Same Day ACH information, keeping everything in one place for easy access.

Implementation Dates

September 23, 2016 – Phase One (Credits Only)

September 15, 2017 – Phase Two (Credits & Debits)

March 16, 2018 – Phase Three (Faster Funds Availability)

Question of the Month

How will a transaction be identified as a Same Day ACH entry?

Same Day ACH Links and Resources

Federal Reserve Bank's Same Day ACH Resource Center

NACHA's Same Day ACH Resource Center

Join the Same Day ACH Community

How are your peers handling Same Day ACH implementation issues?

We've set up a special community in the EPCOR Knowledge Community for you to discuss all things Same Day ACH with other EPCOR members. EPCOR will also utilize the community to host helpful resources and information.

A newly-created webpage has been developed to provide a one-stop destination for all Same Day ACH information.

On this page, you will find:

- A handy countdown to Phase One Implementation on September 23, 2016
- A reminder of the scheduled Implementation dates for all 3 phases
- A listing of all upcoming Same Day ACH webinars and in-person learning events, several of which will be geared to the Originator perspective
- A Question of the Month, posed by EPCOR members
- A quick link to join the Same Day ACH Community in the EPCOR Knowledge Community
- Links to previously recorded Same Day ACH webinars
- Quick links to other Resource Pages including: Federal Reserve Bank's Same Day ACH Resource Center NACHA's Same Day ACH Resource Center
- And More!

While you don't need to be an EPCOR member to access the portal, some aspects of the portal are only available to EPCOR members. To take full advantage of EPCOR's Same Day ACH resources, and to receive member pricing on Same Day ACH learning events, contact Member Services to inquire about membership.

Access this page from the new SDA Portal button on the EPCOR home page or go to www.epcor.org/sameday. Be sure to bookmark this handy reference on your computer and visit often to make sure you're in sync with all that's happening in this exciting space!

POCKETS continued from page 4

2. Exploiting Missing Patches

An attacker connecting to the POS environment via an unsecured wireless network is a common attack. Once a foothold is gained, odds are that numerous patches are missing, offering flaws that can be exploited using a tool such as Metasploit. Again, retail systems often involve legacy programs or machines, which put them at risk. The last thing that any self-respecting system admin or retail software vendor will allow is the installation of service packs, hot fixes and related patches. With the risk of system outages due to risky software updates, there's simply too much lose. Or is there?

Other Security Risks

It's not uncommon for large amounts of cardholder data to end up in an unstructured fashion on mobile devices (e.g., in spreadsheet files, PDFs and the like), often unprotected in the event of loss or theft. There are plenty of stories about auditors, contractors and even software developers who have such data in their possession. All it takes is one car being broken into or one bag being lost at the airport to make a customer data breach reality.

The solution? Encrypt laptops, phones, tablets and any other mobile storage media. Given all the hands in the pie in large retail enterprises, encryption is likely not enough. A proven control that can really help lock down cardholder data is a data loss prevention (DLP) measure, which keeps the data from ever leaving its secure location to begin with.

If it's not one of the above items exposing critical systems and sensitive information, odds are very good that it will be some other predictable security flaw such as a weak password or physical security vulnerability. There's always a chance that other unrelated corporate systems and applications can

see POCKETS on page 6

POCKETS continued from page 5

be breached, leading to the exposure of cardholder data. Of course, there are third-party vendors with all of their network systems and applications that you have to consider, as well. As seen in the Target breach, all it takes is one vendor that's not all that security-savvy to lead to a world of hurt.

What Can Retailers Do to Protect Data?

There are additional security measures retailers can use to lock down their vulnerable POS environments. These include:

- File integrity monitoring that checks for system changes;
- Securing card readers and point-to-point encryption, which ensures that cardholder data is encrypted in transit;
- Installing firewalls and intrusion prevention systems;
- Limiting outbound Internet access for POS systems and disabling remote inbound access.

In the end, if people looking to commit such crimes against retailers really want in, they're going to find a way. It's up to retailers to make their systems as secure as possible. The thing that makes it so difficult is that the criminals have nothing but time; those working in IT and security for retailers don't. But with periodic system upgrades, consistent security evaluations and open communication among involved parties, secure customer data can be closer than ever before.

Source: Security Intelligence

Card-Not-Present Fraud on the Rise

by Marcy Cauthon, AAP, NCP, Director, Payments and On-Demand Education

During EPCOR's *Payment Systems Update* last year, a topic of discussion was the U.S. adoption of EMV. We discussed the merchant liability shift that was to go into effect in October of 2015 and the fact that this technology would help make card fraud at the point-of-sale harder to commit. Some institutions anticipated a rise in e-commerce CNP (card-not-present) fraud due to EMV chip cards protection against counterfeit fraud at the physical point of sale.

What's interesting is that the industry saw a surge in online fraud attempts beginning with the 2015 holiday shopping season and the U.S. market is far from having completed its conversion to EMV. Around the world where EMV is already established, CNP fraud has spiked and the same thing is expected to happen in the U.S., especially in the high-growth channel of e-commerce.

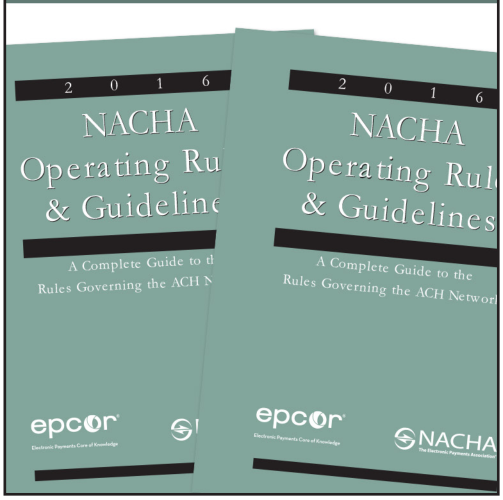
A fraudster's deceptive trade is to exploit the weakest link in a security chain. With the EMV chip card standard having become official for U.S. point-of-sale merchants in October of 2015, the weakest link for merchants and credit and debit card issuers became the card-not-present transaction. All a criminal needs to make a fraudulent transaction via the CNP channel is the card number, cardholder name, expiration date and sometimes the CVV2 or card-verification value which can all be obtained from a lost or stolen card.

The prospect of CNP fraud skyrocketing as EMV continues to roll out in the U.S. is a frightening thought for merchants. To fend off fraudsters, payment experts have said that merchants will need to deploy an array of potent new fraud-detection technologies that will not cause a high number of false positive situations. This is critical, since false positives cost merchants sales, and can damage their brands as well as costing issuers interchange revenue. All of this can be tricky because merchants and issuers do not want to push consumers away by requiring them to jump through multiple authentication hoops at the checkout resulting in the consumer abandoning electronic shopping altogether.

The industry predicts U.S. CNP fraud will hit approximately $6 billion by 2018 which is double the estimated $3 billion in 2015. It is believed that merchants and issuers will embrace other technologies, including biometrics and behavioral analytics, as part of a multi-layered approach to security. One of the advantages of biometric authentication is that it eliminates the use of passwords, and if a consumer's card data is stolen, a criminal can't fake a biometric authentication. Biometric capabilities on mobile devices is definitely a promising solution to fighting fraud but the key will be standardization and acceptance of this method.

With criminals continually advancing the methods they use to perpetrate fraud, payment experts recommend that merchants and issuers use behavioral analytics in conjunction with fraud-detection technologies such as biometrics and cardholder authentication.

Source: Digital Transactions


2 0 1 6
NACHA
Operating Rules
& Guidelines
A Complete Guide to the
Rules Governing the ACH Network
epcor
Electronic Payments Core of Knowledge
NACHA
The Electronic Payments Association

Moving to Faster Payments

by Ann-Marie Bartels, AAP, CEO

Strategies for Improving the U.S. Payment System

It was just over a year ago that the Federal Reserve Banks released "Strategies for Improving the U.S. Payment System" that focused on improving the speed, efficiency and security of the U.S. payment system from end-to-end.

In May 2015, the Federal Reserve established the Faster Payments Task Force to identify effective approach(es) for implementing a safe, ubiquitous, faster payments solution in the United States. EPCOR and many of our member organizations joined the Task Force. With over 300 participants, the Task Force includes representatives from small, medium and large financial institutions, industry trade organizations, technology and solution providers, payments network operators, business end-users, consumer interest organizations and government.

Walking into the first Task Force meeting, I couldn't help asking myself "*how can such a large, diverse group of stakeholders accomplish anything?*" The Federal Reserve Banks were committed to assuring a collaborative process and they made it work!

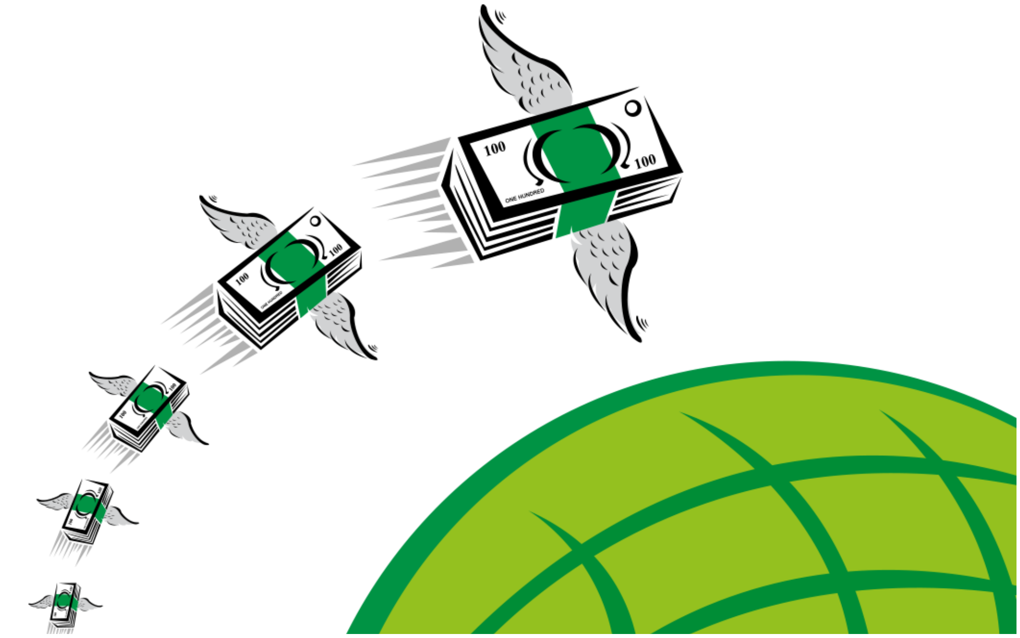
The Faster Payments Task Force focused its efforts on defining "faster" in the form of the Faster Payments Effectiveness Criteria, which can be used to assess faster payments solutions and guide industry innovation. The 36 criteria of the Effectiveness Criteria are categorized into six groupings, Ubiquity, Efficiency, Safety and Security, Speed, Legal and Governance, and represent the collective views of payments stakeholders for measuring effective faster payments solutions in the United States.

We have provided a copy of the *Overview of the Faster Payments Effectiveness Criteria* in the EPCOR Knowledge Community. You can view the complete Effectiveness Criteria and the Glossary of Terms, which defines terms key to understanding the Criteria, on FedPaymentsImprovement.org.

In 2016, the Task Force will focus on the development and assessment of faster payments solution proposals.

While I had some doubts and concerns when I attended my first Faster Payments

see FASTER on page 8



FASTER continued from page 7

Task Force meeting, in just nine months the collaborative efforts of this group, working in conjunction with dedicated staff of the Federal Reserve Banks, have identified the key components of a faster payments solution for the U.S.

The next step, of course, is for solution providers to come to the table to build a solution or solutions that satisfy the Criteria and meet the needs of the vast and diverse population of payments stakeholders in the U.S. I wouldn't have said this a year ago, but I think we are well on our way to achieving a new near-real time or possibly a real-time payments capability in the U.S.

Same Day ACH

That being said … we cannot ignore the fact that the ACH Network is currently focused on a near-term faster solution. Same Day ACH will launch on September 23, 2016 with Phase One allowing credits only. Even in its first phase, Same Day ACH will satisfy the needs of many stakeholders with use cases including emergency and hourly payroll, urgent claims payments and refunds, invoice and tax payments, and same-day bill payments.

The ACH Operators, vendors and processors, and of course financial institutions are working diligently to prepare for Same Day ACH implementation, which is certainly the most significant change to the ACH Network since its introduction some 40 years ago. Same Day ACH will be the focus of numerous EPCOR educational offerings in 2016, including Same Day ACH Symposiums in June and webinars addressing the topic from the different Network participant roles.

I also encourage you to check out our new Same Day ACH portal on the EPCOR website. It's a one-stop shop for all EPCOR Same Day ACH offerings.

Have Consumer Authorization Requirements Changed?

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

The rumor is spreading that the CFPB is changing the authorization requirements for EFT Transactions.

On November 28, 2015, the CFPB issued a bulletin about authorizations for consumer Electronic Funds Transfers. The bulletin was meant simply as a reminder to the industry regarding the importance of obtaining an authorization before a transaction is processed through the various payment networks. The bulletin discusses the importance of making the authorization clear to the consumer and providing the consumer with a copy or confirmation of the authorization.

While the bulletin is referring to all EFTs, let's look at what the ACH Rules say. They are fairly straightforward in Section 2.3 on page OR 6 outlining the authorization requirements for each type of transaction. The Standard Entry Class code may impact the specifics, but as a whole, the requirements are not complicated.

Here are the basics:

- The authorization for a consumer account debit must be in writing and signed or similarly authenticated.
- For recurring transactions, the Originator must provide notice of a change in amount 10 days prior to initiating the transaction, and a change in date 7 days prior to the transaction.
- The consumer must be provided a copy of debit authorizations.
- The Originator must keep a copy of the authorization for two years following the date of the termination or revocation of the authorization. (In other words, if the consumer is debited for 5 years, the Originator would need to keep a copy of the authorization for 7 years.)
- The RDFI can request a copy of the authorization from the ODFI and a copy should be provided to them within 10 banking days of the request.

As mentioned earlier, the CFPB is concerned about all EFT transactions. The Bulletin is meant as a reminder of the obligations for those who originate EFT transactions. A copy of the CFPB's Compliance Bulletin 2015-06 is available here. f you have concerns about whether or not your authorizations meet these requirements, work with your ODFI to determine any changes that you might need to make.

Retailers Tell Fed Debit Swipe Fee Cap is Still Too High

A cap on debit card swipe fees enacted by the Federal Reserve five years ago has helped reduce costs for retailers and consumers but is still higher than intended by Congress and should be lowered, the National Retail Federation (NRF) said today.

"In most cases, 24 cents per transaction represents a significant savings over the prior non-competitive pricing," NRF Senior Vice President and General Counsel Mallory Duncan said. "However, it is still substantially higher than issuers' incremental costs."

Duncan said the cap "has worked moderately well" but that "additional changes are necessary" if Congress' goal of swipe fees that are proportional to banks' costs for processing transactions is to be realized.

Retailers have passed along two-thirds of the $8.5 billion in annual savings to consumers but there would have been more savings to share if the Fed had set the cap at the level expected by lawmakers, Duncan said.

Duncan's comments came in a letter to the Federal Reserve, which is reviewing the cap under requirements of the federal Paperwork Reduction Act.

Under the Dodd-Frank Consumer Protection and Wall Street Reform Act of 2010, the Federal Reserve was required to adopt regulations that would result in debit swipe fees that were "reasonable and proportional" to the actual cost of processing a transaction. Federal Reserve staff calculated the average cost at 4 cents per transaction and proposed a cap no higher than 12 cents. Nonetheless, after heavy lobbying from banks the Federal Reserve Board of Governors eventually settled on 21 cents plus 0.05% of the transaction for fraud recovery and allowed another 1 cent for fraud prevention in most cases. The cap, which applies only to financial institutions with $10 billion or more in assets, took effect in 2011 and totals about 24 cents on a typical debit card transaction.

While lower than the average of 45 cents before the cap was set, NRF argued that the cap included costs that went beyond those allowed under the legislation and filed suit against the Fed in U.S. District Court in 2011. A judge ruled in NRF's favor and ordered the Fed to recalculate the cap, but an appeals court overturned the ruling and the U.S. Supreme Court refused to grant NRF's petition to review the case.

Duncan said the shift of more fraud liability to merchants last fall under the conversion to Europay MasterCard Visa chip-and-signature cards is evidence that the 0.05% for fraud recovery "may no longer have a legitimate basis."

NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs—42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy. **NRF's *This is Retail* campaign** highlights the industry's opportunities for life-long careers, how retailers strengthen communities, and the critical role that retail plays in driving innovation.

Sources: PYMNTS.com

Federal Trade Commission (FTC) Final Telemarketing Sales Rule (TSR) Approved

by Marcy Cauthon, AAP, NCP, Director, Payments and On-Demand Education

Summary

Following a public comment period, the FTC approved the final amendments to the Telemarketing Sales Rule (TSR), including a change that will help protect consumers from fraud by prohibiting four discrete types of payment methods that have been favored by con artists and scammers.

The TSR changes will stop telemarketers from dipping directly into consumer bank accounts by using certain kinds of checks and "payment orders" that have been "remotely created" by a telemarketer or seller. In addition, the amendments will bar telemarketers from receiving payments through traditional "cash-to-cash" money transfers (i.e. MoneyGram or Western Union) and prohibit telemarketers from accepting as payment "cash reload" mechanisms (i.e. MoneyPak or Reloadit packs) used to add funds to existing prepaid cards.

Who Must Comply?

The amended TSR regulates "telemarketing" which is defined in the Rule as "a plan, program, or campaign to induce the purchase of goods or services or a charitable contribution" involving more than one interstate telephone call. With some exceptions, any businesses or individuals

see FTC on page 10

Unfair, Deceptive or Abusive Acts or Practices: Compliance Tips for Third-Party Senders

by Kimberly Martin, AAP, Director, Third Party Services

In light of recent court settlements regarding Unfair, Deceptive or Abusive Acts or Practices, it is becoming increasingly more important to ensure that, as a Third-Party Sender, your organization has a strong UDAAP compliance model. Building a strong UDAAP compliance program can be anything but simple; however there are steps that a Third-Party Sender can take to ensure their ongoing UDAAP compliance.

Every compliance effort should begin with detailed policies and procedures. Understand what types of Unfair, Deceptive or Abusive Acts or Practices could occur within your unique environment and develop procedures to ensure you are continually monitoring your customer's activities for any sign of these unfair business practices. Your procedures should require a thorough review of your customer's practices when you begin working with them, and a periodic review for on-going compliance.

Review the pricing for your customer's products or services to assess if the pricing seems appropriate. Further determine what benefits there are from the product or service to the consumer. Is there the possibility that the consumer may feel that the pricing of the

see TIPS on page 11

TARGET continued from page 9

that take part in "telemarketing" must comply with the Rule. This is true whether, as "telemarketers", "they initiate or receive telephone calls to or from consumers, or as "sellers", they "provide, offer to provide or arrange to provide goods or services to consumers in exchange for payment."

Some Types of Businesses/ Individuals Exempt from Rule:

- Banks, Federal Credit Unions and Federal Savings and Loans
- Non-profit Organizations
- Common Carriers such as long-distance telephone companies and airlines when they are engaging in common carrier activities

What Your Business Needs to Know:

The Rule prohibits telemarketers from using certain payment methods that legitimate telemarketing businesses don't use, but con artists have been known to exploit: remotely created checks, remotely created payment orders, cash-to-cash transfers and cash reload mechanisms.

The payment methods prohibited are all slightly different, but they have a few things in common: 1) they aren't subject to federal laws that protect consumers when paying by credit or debit card; and 2) they're difficult to reverse, which is why scammers like them.

The Rule will have no effect on the routine ways people use newer payment technologies for example, when consumers pay a bill by authorizing an online payment from their bank account. Rather, the Rule is carefully crafted to target the ways scammers exploit novel payment methods that reputable telemarketing companies don't use.

Additional revisions state:

- A new provision that expands the ban on charging advance fees for recovery services to cover losses both in prior telemarketing and non-telemarketing transactions.
- Clarification that a description of the goods or services purchased must be included in the tape recording of a consumer's express verifiable authorization to be charged.
- If a consumer's number is on the Do Not Call (DNC) Registry, the Rule states that sellers or telemarketers have to demonstrate they have an existing business relationship with the person or have the person's express written agreement to receive calls.
- It is a Rule violation to deny or interfere with someone's right to be placed on the National Do Not Call Registry or on any entity-specific Do Not Call list.
- Specifications that if a seller or telemarketer doesn't get the information needed to place a consumer's number on their entity-specific do not call list, the business is disqualified from the safe harbor for isolated or accidental violations.
- It is illegal for multiple entities to split the cost of accessing the DNC Registry.

Source: www.ftc.gov

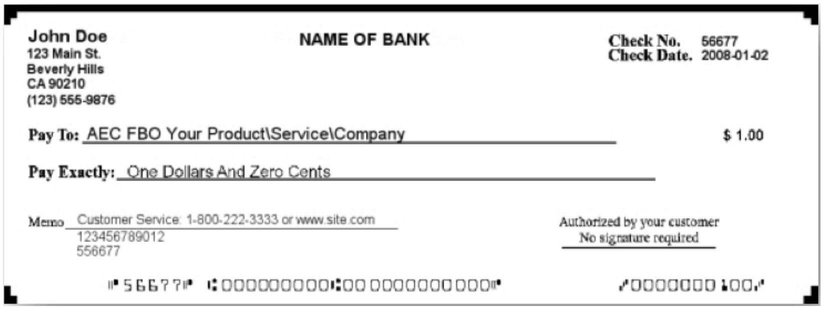
New Remotely Created Check Identifier

by Marcy Cauthon, AAP, NCP, Director, Payments and On-Demand Education

If you are a business or merchant that creates remotely created checks similar to Example A, there is a new identifier that may be used when producing these types of checks.

The Magnetic Ink Character Recognition (MICR) line of a check consists of the string of odd-looking numbers at the bottom of the item. Originally, high-speed equipment at financial institutions “read” those numbers by the unique amount of magnetic ink that each numeral held. Even though that type of processing is becoming obsolete, this line on a check still carries all the pertinent information about the item—the routing number, the account number, the check number and more.

Ⓐ



John Doe
123 Main St.
Beverly Hills
CA 90210
(123) 555-9876

NAME OF BANK

Check No. 56677
Check Date. 2008-01-02

Pay To: AEC FBO Your Product\Service\Company $ 1.00

Pay Exactly: One Dollars And Zero Cents

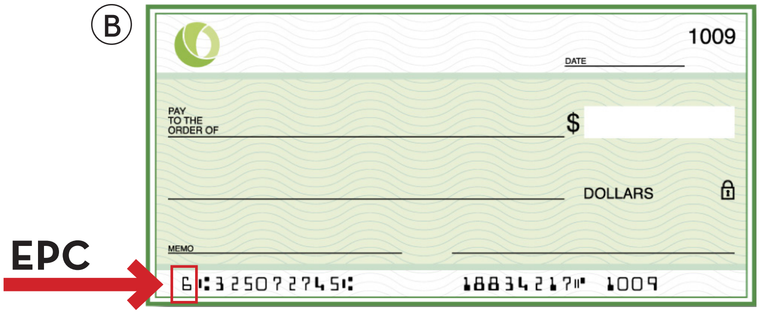
Memo Customer Service: 1-800-222-3333 or www.site.com
123456789012
556677

Authorized by your customer
No signature required

⑈56677⑈ ⑆000000000⑆00 0000000000⑈ ⑇0000000100⑇

In order to better identify items clearing through the Check Processing Network, a new EPC (External Processing Code) code was developed by the X9.100-160 check standard. There are several standards that are used in check image processing, however; the X9.100-160 standard is used to tell where information should be on a MICR line and it consists of two parts.

Ⓑ



1009

DATE

PAY TO THE ORDER OF $

DOLLARS

MEMO

6⑆325072745⑆ 18834217⑈ 1009

Part 1 defines what the EPC code is since it is one of the fields on the MICR line. Part 2 explains the location of where the EPC code must be placed on the MICR line. The EPC field is an optional one MICR-digit number to the direct left of the routing number on the MICR line of a check (Example B). It is a digit that will convey special information regarding the correct handling or routing of a check or check data to a financial institution or processor. An example of this is today you may see a “4” in this field to indicate that you are receiving a substitute check in a forward cash letter or you may see a “5” in this field if you are receiving a substitute check return. The new code for Remotely Created Checks is “6” and may be placed in position 44 of the MICR line when producing a Remotely Created Check. This new code will help the industry identify the entities that are generating these items and help them monitor for proper draft authorization.

see RCC on page 12

TIPS continued from page 10

product or service does not match the benefit? In addition, ensure that pricing for products and services are never misrepresented.

Examine your customer’s website and print marketing materials to ensure that a consumer is provided accurate information regarding products and services. Verify that all marketing is carefully scripted to be accurate and not contain misleading language or references. In addition verify that any additional fees or charges associated with products and services are clearly disclosed to the consumer.

UDAAP compliance can seem like an ever-moving target, however, with a commitment to on-going due diligence, issues with UDAAP compliance can be mitigated.

RCC continued from page 11

Why a New Code?

So why did the X9 standard and the industry feel it was time to make a change? Remotely Created Checks have been criticized for years due to their vulnerability to fraud and the rising number of unauthorized RCC claims being filed against them. The industry felt that remotely created checks have little or no systematic fraud monitoring like ACH or card transactions. So, this new code will enable financial institutions to track how many RCC's they are receiving as well as pushing out in the check image environment. This will also give merchants/businesses a way to differentiate Remotely Created Checks from other checks that they are passing through the check processing network. Gaining usage information throughout the check processing network will help identify the percentage of RCC's clearing vs. how many are being returned as unauthorized.

Optional vs Mandatory

The EPC field is an optional field today, however; a financial institution may enforce the use of the EPC 6 within their deposit agreements with business account holders. If you are an entity that creates these types of checks, contact your financial institution today to determine if this is a requirement within their deposit agreement with your business.

Source: NACHA

Can the CFPB Really Impact My Organization?

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

The Consumer Financial Protection Bureau (CFPB) was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010. The CFPB is now responsible for the oversight of financial institutions and other organizations with ties to consumer finance. This oversight includes many consumer-focused regulations including Regulation E and Regulation Z. Most of the changes we have seen to these regulations have been a result of intricacies within the Dodd-Frank Act, including the introduction and implementation of Regulation E Subpart B, which add requirements for any entity providing international funds transfers to consumers. Besides the changes to consumer regulations, the CFPB is also responsible for ensuring consumers are treated fairly in dispute situations.

According to the CFPB website their role is to:

- Write rules, supervise companies and enforce federal consumer financial protection laws
- Restrict unfair, deceptive or abusive acts or practices
- Take consumer complaints
- Promote financial education
- Research consumer behavior
- Monitor financial markets for new risks to consumers
- Enforce laws that outlaw discrimination and other unfair treatment in consumer finance

In a recent speech, CFPB Director Richard Cordray said, "Listening and responding to consumers is central to the Bureau's mission. The Bureau continues to provide consumers with numerous ways to make their voices heard."

The Director went on to say, "Reasonable regulations are essential for protecting consumers from harmful practices and ensuring that consumer financial markets function in a fair, transparent and competitive manner." The CFPB and other governing agencies work together to ensure products and services are not subject to unfair, deceptive or abusive acts or practices.

The CFPB is required under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to give a semi-annual report to congress. The latest report was given on March 16, 2016 By Director Richard Cordray. A link to the full report is provided **here**.

Though the CFPB may not have direct oversight or jurisdiction over your specific organization, they are definitely a governing agency to pay attention too. Their awareness of consumer issues, coupled with their connection to other agencies including the Federal Trade Commission and Department of Justice, makes them a very influential governing agency.

Why is the Effective Entry Date so Important?

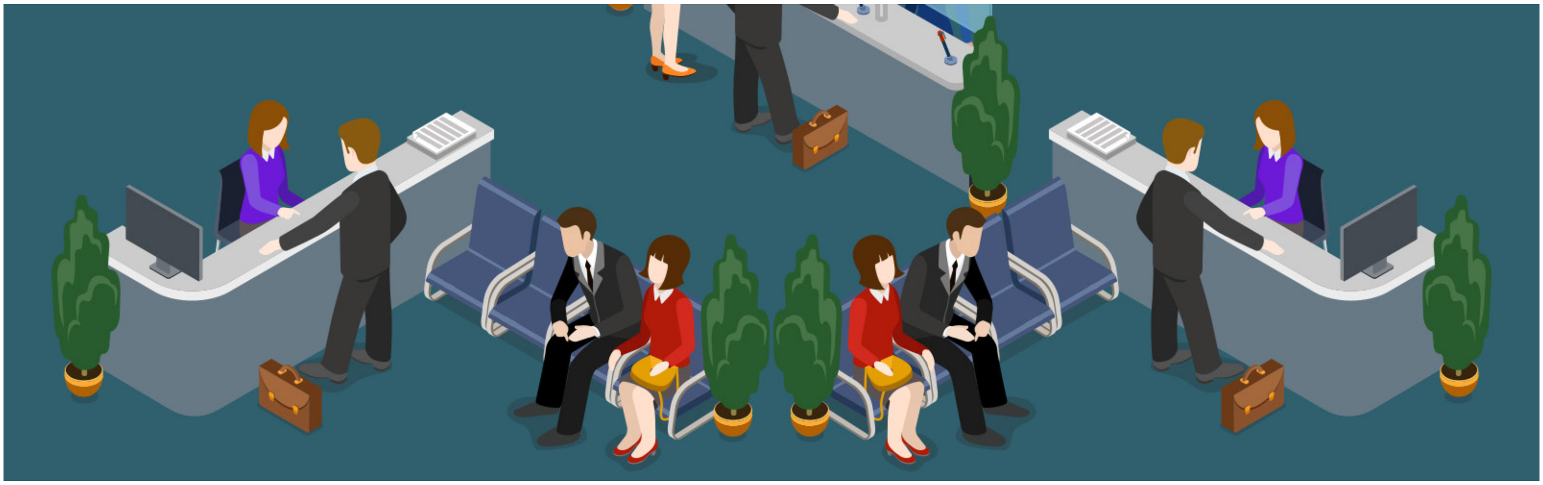
by Brian Laverdure, AAP, Director, ACH Rules and Education

Over the past 40 years, the ACH Network served Originators large and small as an efficient way to send credits, collect payments and pay bills. Last year, the industry voted to adopt and implement the Same Day ACH rule, which will offer Originators the choice to initiate ACH transactions and receive funds on the same day! Effective September 23, 2016, Originators may initiate an ACH credit entry, input the current day's date as the transaction Effective Entry Date, submit the transaction within a prescribed timeframe, and that transaction will be processed and settled on the current day. The Effective Entry Date will be the only identifier of same-day transactions.

What is the Effective Entry Date? The Effective Entry Date is not new to ACH processing; it is the day the Originator wants a transaction to post to a Receiver's account. The Effective Entry Date Field is located in the Company Batch Header Record and is used by the ACH Operators to determine when funds will be settled for ACH transactions. If an Originator selects any federal holiday or a Saturday or Sunday as the Effective Entry Date, the ACH Operator will assign the next banking day as the Settlement Date; likewise, if the Effective Entry Date is stale dated, or dated for a day in the past, the Operators will settle those entries on the next available opportunity, which is the typically the next banking day. Some Originators currently use incorrect dates in the Effective Entry Date field, either due to system limitations or misunderstanding, but the transactions still move through the network and occur on a future date.

When the Same Day ACH Rule takes effect on September 23, 2016, the Effective Entry Date will serve as the only way to identify a Same Day ACH credit transaction and using this field correctly will be critical for all Originators. In order to initiate a Same Day ACH credit transaction, the Originator must select the current date as the Effective Entry Date, then submit that transaction to their ODFI on the current date prior to the last deposit window for Same Day ACH entries that has been established at 2:45 p.m. ET. For example, if an Originator wants to pay a same day credit on September 23, 2016, the Originator must choose September 23, 2016 as the Effective Entry Date. Originators will still have the option to enter a date in the future and those items with a future date will continue to process just as they do today, with next-day settlement. However, on September 23, 2016, ACH credit entries submitted to an ACH Operator with invalid or stale dates may process the same day as the ACH Operators will continue to process those items at the first opportunity, which could be the same day. This could result in unintended Same Day entries and pose other issues for ODFIs and Originators.

As a part of an implementation strategy to prepare for Same Day ACH, Originators are encouraged to take steps to ensure they are using the Effective Entry Date field appropriately. If you have concerns about the proper use of the Effective Entry Date, contact your financial institution to discuss potential options available to limit unanticipated Same Day ACH entries. EPCOR recognizes the need to educate Originators on appropriate use of the Effective Entry Date and how the new rule will affect current origination practices, so we are offering several training opportunities throughout the year. EPCOR will host a webinar on June 2, ***SDA – Effective Entry Date Issues***, which is dedicated to providing Originators with the information they need to appropriately use the Effective Entry Date field. ***SDA – Originator Fundamentals*** on July 13 will provide Originators with an overview of the Same Day rule and other elements to consider in preparation for Same Day ACH.



epcor®

Electronic Payments Core of Knowledge

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

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

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 Blvd., Ste. 555, Kansas City, MO 64111
800.500.0100 | 816.474.5630 | fax: 816.471.7665