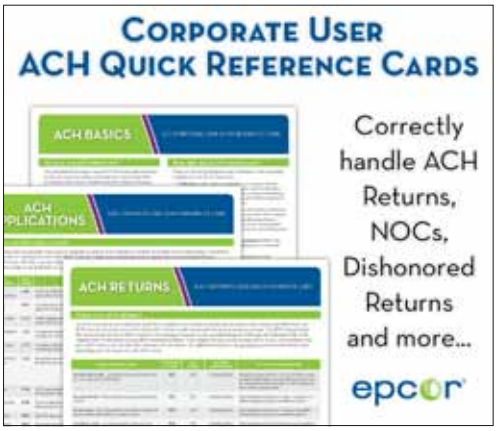
epcor®
Electronic Payments Core of Knowledge

INSIDE ORIGINATION

2013 *ACH Rules* Update for Originating Companies

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. How do 2013 *ACH Rules* changes impact your organization?

Click here to download *2013 ACH Rules Update for Originating Companies* to find out which *ACH Rules* changes 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.



It's Time to Show Off Your GREEN

April is PayItGreen month.

Your customers and peers care about your environmental practices. PayItGreen month is the perfect month to show them what you're made of!

By taking a quick, FREE survey your organization can quantify your green efforts and earn the 2013 PayItGreen Seal of Approval. Displaying the seal clearly demonstrates to your customers and peers 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.

Now is the Perfect Time to Offer Direct Deposit via ACH

May is Direct Deposit and Direct Payment via ACH Month and a great time for your organization to finally free itself from paper checks and begin reaping the benefits of Direct Deposit via ACH. Direct Deposit via ACH is the go-to payroll option for

see DIRECT DEPOSIT on page 2

DIRECT DEPOSIT continued from page 1
employees and simplifies your payroll processes and eliminates the need for issuing costly paper checks.

Why do I want all-electronic payroll for my employees?

IT'S SMART. Electronic payroll benefits you and your business. Here are some points for consideration:

- Adoption of electronic payroll provides you with increased efficiency, decreased costs and simplified payroll procedures.
- On average, you can save approximately $3.00 per payment by using Direct Deposit via ACH instead of paper checks.
- By taking out the manual process of issuing paper checks and using more efficient electronic payroll options, you save time, letting you focus on what matters most—growing your business.
- Direct Deposit via ACH and payroll cards ensure on-time payroll delivery, including in inclement weather and natural disasters when paper checks aren't issued.
- Electronic payroll provides employer solutions for easing compliance. It helps with the timely payment of final wages and enables on-time receipt of pay. Electronic payroll makes you competitive as a hiring organization. The generation entering the workforce today doesn't use checks.
- IT'S SAFE. Check fraud is the number one type of payments fraud. Using electronic payroll means there's no circulation of routing and account numbers, which are on all checks, so there's no ability to launder or fraudulently create checks.
- IT'S GREEN. Every business can make a great environmental impact by switching to all-electronic payroll. For example, a business with 20 employees moving to all-electronic payroll can:
  - Prevent 71.3 gallons of wastewater from being discharged into lakes, streams and rivers.
  - Stop 21.3 pounds of greenhouse gases from being emitted.
  - Preserve 9.3 square feet of forestland.

How can I set up all-electronic payroll?

IT'S EASY. Talk to your financial institution or payroll provider today. For more information on how to set up Direct Deposit via ACH visit www.electronicpayments.org.

Source: ElectronicPayments.org

Updated U.S. EMV Roadmap White Paper Released

Toward the end of 2012, with the move to EMV chip-based payments accelerating in the United States, the Smart Card Alliance Payments Council re-released an updated educational white paper, *Card Payments Roadmap in the United States: How Will EMV Impact the Future Payments Infrastructure?*. The white paper aims to educate issuers, merchants, acquirers, processors and hardware and software suppliers about the critical aspects of deploying an EMV solution in their unique business environments.

To reduce counterfeit fraud and help diminish the value of stolen cardholder data, nearly every country in the world is widely deploying EMV; now, the United States is following suit. Four major United States payment brands have announced harmonized key milestones for United States implementation of EMV. The white paper, an extensive update from the first version released in February 2011, contains all of the important details of the milestones and recommended implementation guidelines from American Express, Discover, MasterCard and Visa in one document for the first time.

Additional white paper topics include:

1. An overview of the EMV specifications and key implementation options for issuers, acquirers/processors, merchants and ATM operators.
2. A discussion of the relationship between U.S. contactless bank card transactions and EMV and the relationship between the Near Field Communications (NFC) specifications and EMV.
3. Actions stakeholders need to take to issue EMV cards, and to accept and process EMV transactions.

"Now that all of the major payment brands have announced their plans and milestones, we are anticipating fairly rapid deployment of EMV in the U.S., harmonized with contactless and NFC payments acceptance," said Randy Vanderhoof, executive director of the Smart Card Alliance.

He continues, "Through this white paper containing all of the latest information and guidance, the Payments Council is providing guidance about the roadmap for EMV migration to make this important shift in the United States as seamless and successful as possible."

The white paper is in addition to a number of educational initiatives the Smart Card Alliance is providing to the industry on EMV chip migration. Last summer, the Alliance launched the website EMV Connection, which provides up-to-date information on the status of EMV migration, along with tutorials and educational resources that will assist with migration.

The Alliance has also formed an independent, cross-industry organization, the EMV Migration Forum, that supports the alignment of the EMV implementation steps required for global payment networks,

see ROADMAP on page 3

ROADMAP continued from page 3

regional payment networks, issuers, acquirers/processors, merchants and consumers to successfully move from magnetic stripe technology to secure EMV contact and contactless technology in the United States.

White Paper Contributors included: Accenture LLP; American Express; Apriva; Bell Identification B.V.; Capgemini; Chase Card Services; Connexem Consulting; Discover Financial Services; First Data Corporation; FIS; Gemalto; Giesecke & Devrient; Heartland Payment Systems; Infineon Technologies; Ingenico, North America; INSIDE Secure; Interac Association/Acxsys Corporation; MasterCard Worldwide; Morpho; NACHA–The Electronic Payments Association; NagraID Security; NXP Semiconductors; Oberthur Technologies; Quadagno & Associates; Thales e-Security; Toni Merschen Consulting; TSYS; VeriFone Systems; Visa Inc.; Watchdata; Wells Fargo.

Download the whitepaper.

Source: Smart Card Alliance

AFP Survey Finds Corporate Payment Fraud Decreasing

The Association of Financial Professions (AFP) just released the results of the 2013 survey of payments fraud among its corporate members. The survey reports on incidence and types of fraud in business-to-business payment types. Respondents indicated that 61 percent of organizations were targeted in 2012, representing a 12 percent decline from the high point in the 2009 survey.

which supports the continued trend away from corporate use of checks for payment. The second most commonly targeted payment method was corporate/commercial purchasing cards, attacked in 29 percent of those organizations affected by fraud.

Interestingly, the survey also reports that in the case of corporate/commercial card fraud, unlike other methods, a significant amount

According to Jim Kaitz, CEO of AFP:

"Today's corporate treasury professional takes proactive steps to combat fraud. Many organizations are transitioning to more electronic payment methods. They are aware of potential vulnerabilities. They engage in dialog with their key banks about fraud prevention."

The survey revealed that 87 percent of affected organizations had their checks targeted, usually by non-employee outsiders, of fraud (26 percent) is committed by an organization's own employees. Commercial card program managers should take note; the card usage controls embedded in most commercial card management software will only work if they are properly implemented!

For more information or to download the survey results, go to www.afponline.org/fraud.

Source: Payments Journal

Emerging Trends and Threats for 2013

During 2012, cyber security incidents included theft of public and private intellectual property, hacktivism, ransomware, malware targeting mobile devices, and a surge of other malware, Black Hole Rootkit and Zero Access Trojan. What will we see in 2013? Below is a brief round up, listed in no particular order, of several threats and trends we can expect this year.

Mobile Devices in the Enterprise

As the use of mobile devices grew in 2012, so too has the volume of attacks targeted to them. Every new smart phone, tablet or other mobile device provides another opportunity for a potential cyber attack. Many enterprises have incorporated these devices into their networks. In some cases, organizations are allowing employees to "Bring Your Own Device" (BYOD). This increases the cyber security risks for an organization particularly if it does not have control over the employee's personal mobile device. Risks include access to corporate email and files, as well as the ability for the mobile device apps to download malware, such as keyloggers or programs that eavesdrop on phone calls and text messages.

New capabilities, such as NFC (Near Field Communication), will be on the rise in 2013 and will increase the opportunities for cyber criminals to exploit weaknesses. NFC allows for smartphones to communicate with each other by simply touching another smart phone, or being in close proximity to another smart phone with NFC capabilities or an NFC device. This technology is being used for credit card purchases and advertisements in airports and magazines, and will most likely be incorporated into other uses in 2013. Risks with using NFC include eavesdropping—through which the cyber criminal can intercept data transmission, such as credit card numbers—and transferring viruses or other malware from one NFC-enabled device to another.

Ransomware

Ransomware is a type of malware that is used for extortion. The attacker distributes malware that will take over a system by encrypting the contents or locking the system; the attacker then demands money from the victim in exchange for releasing the data and/or unlocking the system. Once payment is delivered, the attacker may or may not provide the data or access to the system. Even if access is restored, the integrity of the data is still in question. This type of malware and delivery mechanism will become more sophisticated in 2013.

Social Media

Use of social media sites has grown beyond just sharing personal information, such as vacation photos and messaging. These sites are being increasingly used for advertising, purchasing and gaming. For 2013, attackers will look to exploit this volume and variety of data being shared to credentials or other Personally Identifiable Information (PII), such as social security numbers.

Hactivism

Attacks carried out as cyber protests for politically or socially motivated purposes, or "just because they can" have increased, and are expected to continue in 2013. Common strategies used by hactivist groups include denial of service attacks and web-based attacks, such as SQL Injections. Once a system is compromised, the attacker will harvest data, such as user credentials, to gain access to additional data, emails, credentials, credit card data and other sensitive information.

Brought to you by:

MS-ISAC MULTI-STATE Information Sharing & Analysis Center™

A DIVISION OF CENTER FOR INTERNET SECURITY

PCI, Security Standards Council, Issues New Cloud Security Guidance

More organizations move to the Cloud every day. Security concerns exist, depending on the service provider, the Cloud itself (i.e. Private vs. Semi-Private), and more. But oftentimes the business or organization moving to the Cloud doesn't understand the true security risks, their liability or security measures.

Outsourcing the management of security controls really doesn't equate to outsourcing your responsibility to be PCI-DSS compliant. Cloud services are not all created equally, so you need to understand what "PCI-compliant Cloud service" really means. The guidance is for any organization that stores, processes or transmits card data.

Download PCI DSS Cloud Computing Guidelines.

Source: PCI Security Standards Council

Fraud Advisory for Businesses: Corporate Account Take Over

First identified in 2006, "corporate account take over," has morphed in terms of the types of companies targeted and the technologies and techniques employed by cyber criminals. Where cyber criminals once attacked mostly large corporations, they have now begun to target municipalities, smaller businesses and non-profit organizations. Thousands of businesses, small and large, have reportedly fallen victim to this type of fraud. Educating all stakeholders (financial institutions, businesses and consumers) on how to identify and protect themselves against this activity is the first step to combating cyber criminal activity.

An advisory was created as part of a joint effort between the United States Secret Service, the Federal Bureau of Investigation, the Internet Crime Complaint Center (IC3) and the Financial Services Information Sharing and Analysis Center (FS-ISAC) intended to provide basic guidance and resources for businesses to learn about the evolving threats and to establish security processes specific to their needs.

Download *Fraud Advisory for Businesses: Corporate Account Take Over.*

Source: Internet Crime Complaint Center (IC3)

Fed Stands Strong on Existing Debit Card Interchange Fee Regulation

As required by law, the Federal Reserve surveyed debit card issuers and processors to determine costs related to authorization, clearing and settle (ACS), and fraud for regulated issuers across the United States (those with assets over $10B). Based on this data, the Fed has determined that no changes will be made to existing debit card interchange fee regulation or fraud adjustment. The next survey takes place in two years.

Mercator Advisory Group anticipates issuers that have accepted the inevitable will continue to lobby behind the scenes to modify or eliminate the Durbin Amendment based on its impact to unregulated financial institutions. Retailers will most likely highlight parts of the release, such as:

Issuers that responded to both the 2009 and 2011 data collections typically reported ACS costs per transaction that were lower in 2011 than in 2009. Covered issuers that had average ACS costs below 21 cents in 2011 processed well over 99 percent of all reported covered transactions, the same proportion as in 2009.

The 39-page report also illuminates how the regulation has shifted network incentives, citing:

Although networks reduced payments and incentives to covered issuers after October 1,2011, covered issuers received a disproportionate share of payments and incentives (compared with exempt issuers) both before and after implementation of the interchange fee standard.

Download the report.

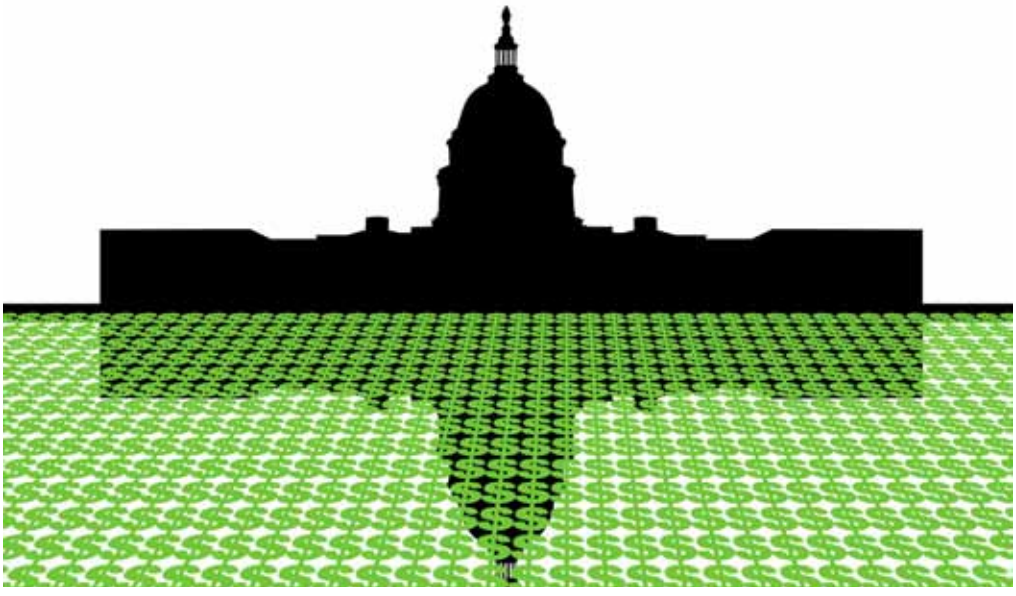
Another interesting note was the dramatic drop in ACS for prepaid card transactions:

The average ACS cost for prepaid transactions was 22 cents in 2009 and 12.2 cents in 2011.

The median fraud loss, as reported, was essentially unchanged from 2009, which will not help EMV advocates make their case; a hoped-for outcome of this survey.

Mercator will be writing more about this as we absorb the complete report, but the continuation of this survey provides a valuable glimpse into the economics of debit cards in the United States, even if, at first glance, it appears to have a net neutral effect on either side of the argument regarding the rules.

Source: Payments Journal



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