epcor®
Electronic Payments Core of Knowledge

INSIDE ORIGINATION

INSIDE: Are You Ready to Run with the 2017 *ACH Rules* Changes? ..... pg. 1
Simplify Your Payments Processing with the Small Business Payments Toolkit ..... pg. 1
What Does Same Day ACH Mean for Businesses? ..... pg. 1
IRS Scam Blends CEO Fraud, W-2 Phishing ..... pg. 2
Encourage Your Staff to Increase Savings Through Split Deposit ..... pg. 3
Why U.S. EMV Could Be Poised to Rise in 2017 ..... pg. 4
Small Business Tips: Foreign Payments, The Patriot Act, OFAC and You ..... pg. 5
Social Engineering Fraud Threat Targets Public-Sector Entities ..... pg. 6
Federal Reserve Payments Study Highlights Strong Trends in Card Use ..... pg. 8
NACHA Research Shows Direct Payment via ACH is a Valuable Donor Retention Tool ..... pg. 8
Can the Insurance Industry Get Aboard the Faster Payments Train? ..... pg. 9

Are You Ready to Run with the 2017 *ACH Rules* Changes?

As an Originator of ACH entries it is very important for you to stay current with the *ACH Rules*, including how updates and changes might impact your business.

Same Day ACH debits and Third-Party Sender Registration are the two major changes on tap for 2017; are you up-to-speed on these revisions? Download the ***2017 ACH Rules Update for Originating Companies*** for an overview of the *ACH Rules* changes that will affect companies in 2017. If you have any questions about how these changes may pertain to your existing Origination activities, contact your financial institution.

Simplify Your Payments Processing with the Small Business Payments Toolkit

The Small Business Payments Toolkit can make your work more efficient and cost effective.

What Was the Genesis of the Toolkit?

One of the five desired outcomes outlined in the Federal Reserve Bank's *Strategies for Improving the U.S. Payment System* paper is to collaborate with industry stakeholders to improve payments efficiency. This goal includes originating and receiving more payments electronically to reduce the average end-to-end costs of transactions and to enable innovative payment services for consumers and businesses.

Introducing... the Improved Small Business Payments Toolkit

The recently released Volume 2 of the *Small Business Payments Toolkit*, is a robust payments education tool for small businesses and the financial institutions who serve them. Volume 2 is chock-full of new information to further encourage electronic B2B payments and

see TOOLKIT on page 3

What Does Same Day ACH Mean for Businesses?

The same-day settlement of Automated Clearing House (ACH) payments is now a reality for businesses across the country. According to NACHA, 79 million ACH payments are made every day. In total, nearly $40 trillion is moved through the ACH network each year. These payments typically take 24-48 hours to process.

Now, thanks to a new rule that went into effect on September 23, 2016, all financial institutions must be able to accept requests for same-day settlement of ACH credit payments for transactions less than $25,000. The new rule affects virtually every player in the ACH transaction ecosystem and brings the payments industry one step closer to real-time payment capabilities.

How Does the New Rule Impact Businesses?

With global commerce continuing to grow rapidly, there is an increased need for businesses—and consumers—to get payments and information faster. Today, the only way to do a same day payment is via a U.S-based

see SAME DAY on page 2

SAME DAY continued from page 1

wire transfer—a costly and cumbersome process that is not practical for smaller payments.

The new rule evolves the payments industry by giving all organizations using the ACH network access to same day settlements. While waiting a day or two for a payment to clear may not sound like a long time, businesses today are in a hyper-competitive environment that demands every dollar be used wisely and accounts receivables management is as much of a priority as accounts payable. With same day settlement, companies will be able to both increase cash flow and improve the customer experience.

Some of the specific benefits include:

- Providing more accurate, real-time view of balance sheets, incoming payments and any potential cash shortages.
- Fulfilling emergency payroll distributions to employees for a final paycheck or to correct an error with regular payroll processing.
- Reimbursing insurance claims directly into patients' accounts, even on the same day as the procedure or appointment.

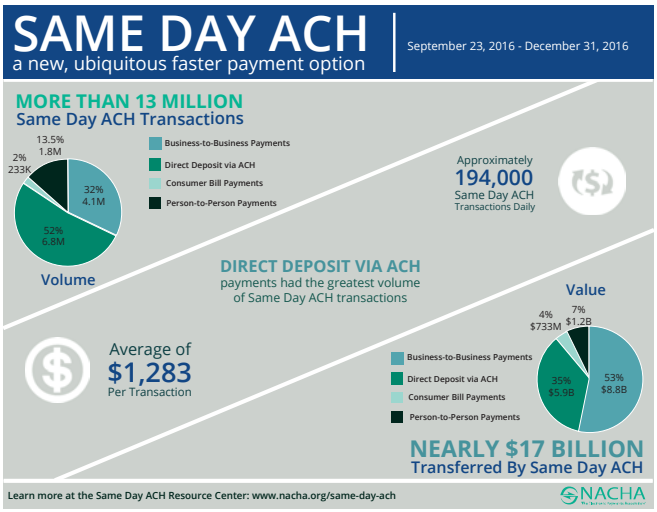
The fast and easy transfer of money will remove many of the inefficiencies from current payment and billing cycles, but companies will need to adapt. As more real-time payment channels become the norm, some businesses may need to update their existing payments systems or hire additional staff to handle more frequent payments and the resulting larger anticipated volumes.

What's Next for the Payments Industry?

Implementation of the Same Day ACH rule will occur over three phases. Following the first phase which went into effect in September 2016, this functionality will be expanded to also include ACH debit payments on September 14, 2017. By March 16, 2018, all financial institutions will be required to provide end-of-day funds availability for Same Day ACH credit payments.

Although the three phases are split up to reduce any major disturbances to the payments industry, early signs are that most financial institutions are well on their way to complying with the new rules. According to a survey conducted by NACHA, the nation's top financial institutions are already on target to offer same day ACH payments. Ninety-five percent of respondents indicated they will offer their clients same day ACH origination services by year end. One hundred percent of respondents are planning to offer same day payroll payments and 95% are planning to offer same day B2B payments, in addition to services for expedited bill pay and person-to-person (P2P) payments.

While all current payment types will continue to exist within the ACH network, the addition of same day capabilities represents an important milestone for the industry that will also help businesses run more efficiently. By providing businesses and customers with access to same-day settlement, the ACH network is setting a gold standard for global commerce, and implementation of other payment networks and technologies will soon follow. The future of commercial payments is fast approaching—it is time for financial executives, financial institutions and affiliates to get ready.



Source: Payments Essentials

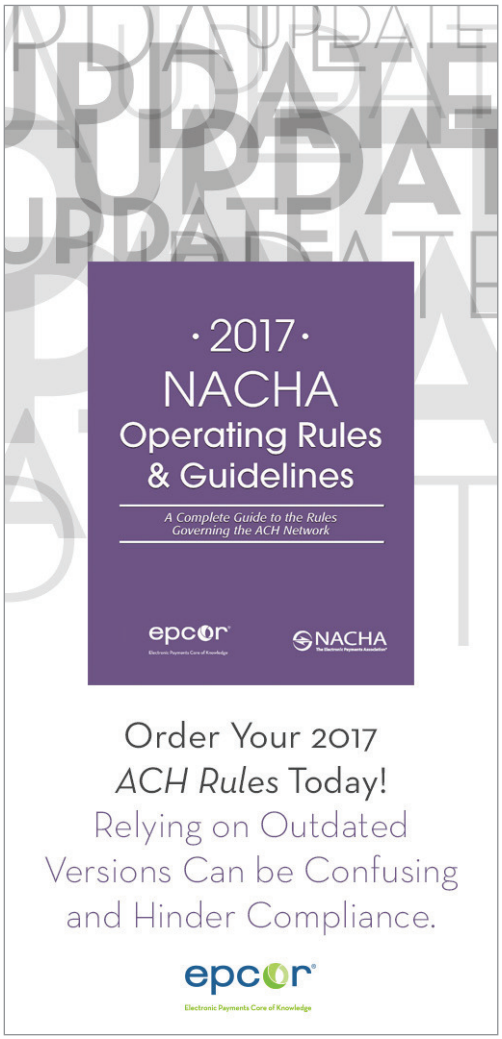
IRS Scam Blends CEO Fraud, W-2 Phishing

Most people are familiar with CEO fraud—e-mail scams in which the attacker spoofs the boss and tricks an employee at the organization into wiring funds to the fraudster. You may also have heard about W-2 phishing, in which crooks impersonate the boss and request a copy of all employee tax forms. According to a new "urgent alert" issued by the U.S. Internal Revenue Service, scammers are now combining both schemes and targeting a far broader range of organizations than ever before.

The IRS said phishers are off to a much earlier start in 2017 than in tax years past, trying to siphon W-2 data that can be used to file fraudulent refund requests on behalf of taxpayers. The agency warned that thieves also appear to be targeting a wider range of organizations in these W-2 phishing schemes, including school districts, healthcare organizations, chain restaurants, temporary staffing agencies, tribal organizations and nonprofits.

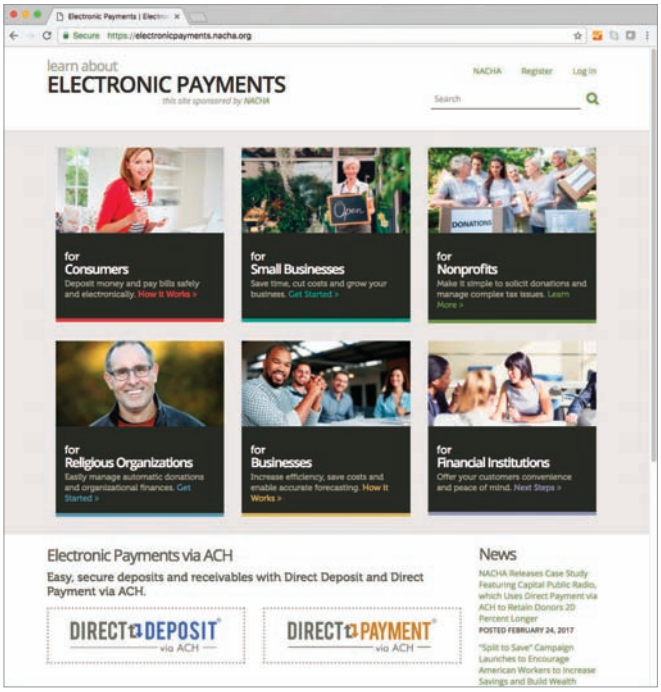
Perhaps because they are already impersonating the boss, the W-2 phishers feel like they're leaving money on the table if they don't also try to loot the victim

see SCAM on page 4



Encourage Your Staff to Increase Savings Through Split Deposit

The new "Split to Save" campaign aims to educate workers on the benefits of Direct Deposit *via ACH* and Split Deposit and how it can help increase personal savings and build wealth. Currently, 82% of the nation's workers receive Direct Deposit of their pay, but only 24% use Split Deposit—one of the easiest ways to grow savings over time.



[Watch this free webinar] initially held in February to kick off the campaign where speakers unveiled the ["Split to Save" Toolkit], which provides educational resources for building awareness about Direct Deposit and Split Deposit.

For more resources on Split Deposit, Direct Deposit and saving automatically, visit [ElectronicPayments.org].

Source: NACHA

TOOLKIT continued from page 1

remittance information exchanges by small businesses. Resources in the Toolkit include:

- **Working with Your Banker** – details on getting started with Automated Clearing House (ACH) origination.
- **Fraud Prevention and Mitigation Tips** - financial services and other mitigation strategies to help small businesses combat payments fraud.
- **What Small Businesses Should Know about EMV or Chip Cards**
- **An Introduction to Alternative Payments**
- **Business Continuity Planning for Small Businesses**
- [Vendor Forum] - a venue for collaboration and resources.
- **Understanding ISO 20022 Resource Guide**
  - General ISO 20022 Resources
  - Information on Using ISO 20022 in the ACH Network and for Wire Transfers
  - Resources Focused on Global Implementation of ISO 20022
- **B2B Directory** - provides a valuable tool enabling payors to obtain payee information easily and securely.
- **Other Resources** also include ACH checklists and forms, financial institution holidays, Regional Payments Association information, health care information and webinar links.

Financial institutions, consultants, small businesses and anyone else interested in learning more about payments can download this free resource now. We recommend bookmarking the ***Small Business Payments Toolkit*** as the **Business Payments Coalition** may continue to release new volumes.

Source: FedPaymentsImprovement.org

How Can You Get Involved in These Initiatives?

Interested in joining the Business Payments Coalition?

You will receive a welcome packet, be added to the Coalition distribution list and be invited to specific Coalition initiatives that may interest you.

REGISTER NOW!

SCAM continued from page 2

organization's treasury: According to the IRS, W-2 phishers very often now follow up with an "executive" email to the payroll or comptroller requesting that a wire transfer be made to a certain account.

"This is one of the most dangerous email phishing scams we've seen in a long time," IRS Commissioner John Koskinen said. "Although not tax related, the wire transfer scam is being coupled with the W-2 scam email, and some companies have lost both employees' W-2s and thousands of dollars."

The Federal Bureau of Investigation (FBI) has been keeping a running tally of the financial devastation visited on companies via CEO fraud scams. In June 2016, the FBI estimated that crooks had stolen nearly $3.1 billion from more than 22,000 victims of these wire fraud schemes.

First surfacing in February 2016, the W-2 phishing scams also have netted thieves plenty of victims. Some of the more prominent companies victimized by W-2 scams last year included Seagate Technology, Moneytree, Sprouts Farmer's Market and EWTN Global Catholic Network.

Scammers also are now selling 2016 employee W-2 forms that were phished or otherwise stolen from victim organizations, peddling individual W-2 tax records for between $4 and $20 apiece.

Tax refund fraud affects hundreds of thousands, if not millions, of U.S. citizens annually. Victims usually first learn of the crime after having their returns rejected because scammers beat them to it. Even those who are not required to file a return can be victims of refund fraud, as can those who are not actually due a refund from the IRS.

The IRS says organizations receiving a W-2 scam email should forward it to phishing@irs.gov and place "W2 Scam" in the subject line. Organizations that receive the scams or fall victim to them should file a complaint with the Internet Crime Complaint Center (IC3,) operated by the FBI.

Employees whose Forms W-2 have been stolen should review the recommended actions by the Federal Trade Commission at www.identitytheft.gov or the IRS at www.irs.gov/identitytheft. Employees should file a Form 14039 (PDF) Identity Theft Affidavit, if the employee's own tax return rejects because of a duplicate Social Security number or if instructed to do so by the IRS.

W-2 forms are prized by ID thieves because they feature virtually all of the data needed to file a fraudulent tax refund request with the IRS in a victim's name, including the employer name, employer ID, address, taxpayer address, Social Security number and information about 2016 wages and taxes withheld.

According to recent stats from the Federal Trade Commission, tax refund fraud was responsible for a nearly 50% increase in consumer identity theft complaints in 2015.

The FBI urges businesses to adopt two-step or two-factor authentication for email, where available, and to establish other communication channels—such as telephone calls—to verify significant banking transactions. Businesses are also advised to exercise restraint when publishing information about employee activities on their Web sites or through social media, as attackers perpetrating CEO fraud schemes often will try to discover information about when executives at the targeted organization will be traveling or otherwise out of the office.

Source: Krebsonsecurity.com

Why U.S. EMV Could Be Poised to Rise in 2017

In its January EMV update, Visa announced that chip-enabled merchants now account for 46% of the company's in-store payment volume.

The firm also saw over 800 million chip-on-chip transactions in November, up 359% year-over-year.

The numbers point to rising EMV penetration across the US, but are also significant because, as the largest U.S. card network, Visa's figures could serve as a benchmark for the progression of the U.S. EMV migration across the industry,

Rising chip transactions points to growing adoption and buy-in from consumers and merchants alike.

Consumers: Visa has now issued just under 400 million chip cards in the U.S., marking a 105% year-over-year increase. For context, that's roughly 47% of Visa's total U.S. cards. And consumers seem to be adjusting to the changes that chip cards bring, like dipping rather than swiping. A separate Visa survey found that 35% of consumers, the highest percentage in the survey, believe chip cards are the safest way to pay.

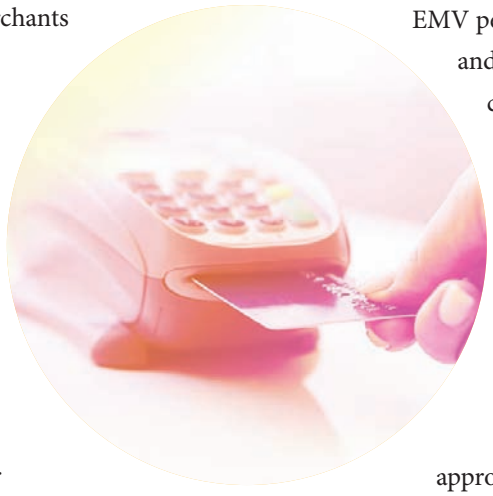
Merchants: Merchant adoption continues

see EMV on page 5

EMV continued from page 4

to rise, though it's slowing—1.75 million Visa merchants now accept chip cards, up by 110,000 since the previous quarter and over 1 million since November 2016. That's still just 38% of U.S. storefronts, but represents a significant figure of transaction volume because most major merchants accept EMV cards. As more small businesses warm to the idea of EMV and upgrade their readers, likely because of the fraud protection benefits they can reap, it's likely this figure will continue to rise steadily. However, Visa and other networks recently delayed the migration for gas stations, somewhere that cards are used regularly and locations that see high fraud, by three years, which could continue to impact merchant upgrades.

That could have a big impact on transaction safety in the U.S. The U.S. EMV migration continues to be slow going—for the year ending in second quarter 2016, just 7% of transactions overall in the U.S. were chip-on-chip, according to data from EMVCo. And though Visa's numbers point to a slowdown in both merchant and customer uptake, it's likely we'll see steady growth that will lead to another considerable jump in overall EMV penetration in late 2016 and early 2017. And that could help reduce fraud, which is still high in the U.S., and make card-present transactions as safe as possible, even as in-store retail remains popular.



Fraud cost U.S. retailers approximately $32 billion in 2014, up from $23 billion just one year earlier. To solve the card fraud problem across in-store, online and mobile payments, payment companies and merchants are implementing new payment protocols that could finally help mitigate fraud.

Source: Business Insider

The Other Side of the EMV Coin

In late 2016, **Digital Transactions reported** that slow adoption of the transition to chip and pin was resulting in merchants feeling the pain of seeing chargebacks for the first time, and to the tune of an estimated $5.8 billion price tag for the year.

Under rules in place since October 1, 2015, merchants not prepared to process EMV chip cards are now liable for fraud caused by counterfeit cards. That is meant to spur merchants to adopt EMV, but it also means fraudsters have rushed to take advantage of a dwindling opportunity while they still can.

New temporary policies by Visa and MasterCard will help cut back on the losses merchants are seeing. As more merchants finally achieve EMV compliance, the burden will start to lighten in 2017, with transactions estimated to fall to 14.2 million and dollar value to $5.6 billion.

Source: Digital Transactions

Small Business Tips: Foreign Payments, The Patriot Act, OFAC and You

Every time I find myself in the security line at the airport, I watch the folks ahead of me anticipating that someone will be pulled from the line because their name appeared on the TSA "no-fly" list. I have yet to see this happen, but I sympathize with the poor schlub whose name matches that of a known evil-doer.

Many small businesses that regularly make overseas payments to customers, vendors, or clients are unaware that they too may fall victim to a lesser-known "no-fly" list. Compliments of the USA Patriot Act, these payments, often made through bank wire transfers or International "FX" payments, are subject to similar scrutiny but via a less-publicized list of names.

The United States Treasury Department oversees the transfer of capital internationally and are charged with regulating these transfers. The Office of Foreign Assets Control administers and

see TIPS on page 7

Social Engineering Fraud Threat Targets Public-Sector Entities

NACHA issued an ***ACH Operations Bulletin*** in February, providing guidance, including steps that businesses can take to reduce vulnerability to this type of fraud.

Social Engineering Fraud

Several recent news articles have highlighted successful social engineering fraud carried out against public-sector entities that have resulted in monetary losses. Each of these reported cases has a similar fact pattern. A public-sector agency or entity, such as a municipal government agency or a public university or college, receives an unsolicited request, purportedly from a valid contractor, to update the payment information for that contractor. The update could be new routing and account information for ACH or wire payments, or a request to change the payment method from check to ACH or wire payments along with routing and account information. In these cases, the update did not come from the contractors themselves but from fraudsters. As described in the articles, the public entities that used the "updated" information actually sent payments to the fraudsters, resulting in losses to the public entities.

This social engineering scenario is similar to the Business Email Compromise (BEC) scenarios that were described by the Federal Bureau of Investigation (FBI) in 2015, and many of their recommendations are applicable to this scenario as well. The main difference is that instead of impersonating a corporate official (CEO or CFO) and ordering a payment to be made, in this scenario the fraudsters impersonate a legitimate contractor or vendor and order the change in payment information from legitimate instructions to reference a fraudulent account.

Several of the articles further suggest that the funds are being moved out of the country (China is prominently referenced). As most public-sector entities will not have the ability to initiate International ACH Transactions, other means are presumably being employed. For example, after funds are deposited via an incoming ACH credit or wire transfer, they may be subsequently wired out of the country or otherwise withdrawn.

In a statement quoted in an article on January 20, 2017, the FBI characterized one of these cases as business email compromise, and that there is "absolutely no suspicion or indication that this fraud involved the manipulation or compromising of the Automated Clearing House (ACH) banking transfer system."

Public-Sector Entities Are Being Targeted

Although any business entity could be the target of this type of social engineering attack, public-sector entities seem to be specifically targeted because their contracting information is typically a matter of public record. Fraudsters use information from such public records to more convincingly impersonate legitimate contractors.

Guidance for Businesses

Businesses should not consider these types of social engineering attacks solely as hacking, phishing or cybercrime. Be aware that the vectors for these attacks are not necessarily through Internet-based methods; while some come by email, others come as phone calls, faxes or letters in the mail.

One method to reduce the risk of falling victim to this scam is to authenticate any request to make a payment or change payment instructions to a contractor or vendor, and independently verify a change in payment instructions using out-of-band verification techniques, especially when the request cannot be authenticated. The phone number or other contact information used for this verification should not come from the communication requesting the change, but should instead be taken from a known and trusted contact list for that contractor or vendor.

For those entities that make forms available online for contractors to submit ACH or payment information, verification of a change in payment information should not rely solely on contact information provided in such forms. Additionally, entities should consider making such forms available only via secure means, whether online or offline. Entities should take seriously any call they receive from their financial institution questioning the legitimacy of a payment.

These steps are suggestions only; each business should consider the risk management practices best tailored to its individual programs and circumstances.

Source: NACHA

TIPS continued from page 5

enforces various economic sanctions programs; you may be familiar with the restrictions and embargoes that are placed on countries such as North Korea or Iran which are designed to put foreign policy pressure on those and other governments. And it is not just countries with nuclear ambitions that are embargoed, but also those considered at risk for security reasons such as terrorism and narcotics trafficking.

OFAC not only has the ability to block transactions bound for specific countries, but also maintains a list of specific individuals to whom payment can be blocked or delayed. If a person's name appears on the Specially Designated Nationals List (SDN), any payments or other financial transactions intended for them can be blocked, delayed or even confiscated. OFAC updates and publishes this list online, but is time consuming to search and, for many businesses, may be impractical to do so for every payment sent.

All US-based businesses, small and large, are responsible for complying with these regulations and a business has very little control over the policies, procedures and penalties which can be assessed for companies which violate OFAC compliance guidelines. Most banks and international payments facilitators such as PayPal and Western Union have policies and programs in effect that will help businesses to remain in compliance and enforce OFAC rules on payments sent via their systems.

Here are a few tips on what you can do to assure that you remain in compliance and to assist should you find that a transaction you initiate is flagged or held by OFAC.

1. Know How It Works. OFAC compliance is complex and the best defense is a good offense. You can learn everything you need to know on the Treasury Department website, although it can be difficult to navigate and search.

2. Check with Your Financial Institution. Your financial institution is a great place to start; have a conversation with your client manager or relationship officer and ask what you can do on your end prior to initiating a transfer. The goal is to limit the surprises that will come your way if you attempt payment to a business, or individual from one of the affected countries or to someone on the SDN List.

3. Ask for the Relevant Information. A good strategy is to request from your payees the specific personal information that OFAC may require if your payment is held. This can include information such as full and complete name, place of birth, date of birth, country of citizenship, legal residence or profession; in addition you may be asked to provide the specific purpose of the payment. It can be a delicate matter to ask for this kind of information, but most people will be happy to comply if they understand why you are asking.

4. Stay Up-to-Date. The Treasury Department regularly updates the SDN list and you can access the most current list here. Two other valuable resources provided by OFAC are a comprehensive list of FAQs, as well as information for specific industry groups.

Source: Crowdspring.com

Federal Reserve Payments Study Highlights Strong Trends in Card Use

From 2012 to 2015, credit and debit (including prepaid and non-prepaid) card payments continued to gain ground in the payments landscape, accounting for more than two-thirds of all core noncash payments in the United States, according to a recently released Federal Reserve study of U.S. non-cash payments. Automated clearinghouse (ACH) payments grew modestly over the same period, and check payments declined at a slower rate than in the past.

The ***2016 Federal Reserve Payments Study***, which presents 2015 payments data, found that the number of domestic core noncash payments totaled an estimated 144 billion—up 5.3% annually from 2012. The total value of these transactions increased 3.4% over the same period to nearly $178 trillion.

Other key findings:

- Card payments grew 19.9 billion from 2012 to 2015, led by non-prepaid debit card payments which grew by 12.4 billion, and credit card payments, which grew by 6.9 billion. Prepaid card payments grew by less than 1 billion.

see STUDY on page 9

NACHA Research Shows Direct Payment *via ACH* is a Valuable Donor Retention Tool

NACHA released a **case study** on the benefits of using Direct Payment *via ACH* for donor retention and announced the launch of a new comprehensive outreach effort. The effort is designed to increase awareness and understanding of the value of ACH payments for fundraising, and build confidence in adoption and use of these payments by charitable organizations to grow and sustain donation dollars and their donor base over time.

"Industry research clearly shows that the contributions of sustaining donors, or those that give on a recurring basis, are worth more than those from traditional donors over the life of their giving," said Janet O. Estep, NACHA president and CEO. "In addition to donating more frequently and at higher amounts than traditional givers, sustainers continue to give for many years providing for consistent and predictable cash flows and a loyal and committed donor base. Organizations that leverage Direct Payment *via ACH* for sustained giving can reduce resources spent on fundraising and devote more effort to what matters most: their missions."

NACHA's newest case study highlights the value of Direct Payment *via ACH* for donation collection. The case study features Capital Public Radio (CapRadio), which is based in Sacramento, California, and showcases how it leverages ACH for its sustaining donor program. According to CapRadio, sustaining donors that pay with ACH are responsible for more than 40% of all individual donation dollars, and they are retained for up to 20% longer than sustainers who use credit or debit cards.

Recurring Direct Payment *via ACH* results in less churn among donors because consumers' bank accounts don't have expiration dates, and consumer are far less likely to change their main bank accounts than they are with credit cards. Further, recurring ACH payments are just as easy to set up online as any other type of payment. Recurring ACH payments have been the preferred payment method for decades for other types of organizations, such as billing companies for recurring bill payments, and employers of all types and sizes for payroll Direct Deposit.

"ACH payments can be a powerful tool for charitable organizations of all sizes and types," said Estep. "It is our hope to enhance awareness and understanding of this payment method as it will go a long way in advancing the invaluable work of our nation's charitable organizations."

Source: NACHA

Can the Insurance Industry Get Aboard the Faster Payments Train?

When Hurricane Matthew's Category 5 bluster wreaked havoc on U.S. homeowners last fall, thousands were forced to seek shelter far from home only to later return and find their homes destroyed or severely damaged by the storm.

Of the displaced masses, the Consumer Federation of America expected more than 100,000 insurance claims to be filed with payouts topping $7.5 billion. And these hurricane victims needed payouts to happen quickly and easily, because delays posed potential problems as the victims attempted to get their lives back on track.

But it's not just hurricane victims and other individuals who have experienced devastation expecting fast resolution. Today's consumers increasingly expect payments to be processed quicker than ever before, and insurance companies are turning to newly introduced faster payment initiatives such as Same Day ACH to accommodate the demand.

Overcoming the Antiquated

For the insurance industry, as with other businesses, one of the biggest challenges is extending modern-day faster payment solutions through old-school legacy information technology platforms. Many companies across the insurance space are reliant on common business-oriented language (COBOL)-based platforms, which have been in existence since the late 1950s.

see INSURANCE on page 10

STUDY continued from page 8

- Remote card payments, sometimes called card-not-present payments, reached 19% of card payments in 2015, an increase of less than 4% compared with 2012. Gains in remote cards' share of total card payments were mitigated by substantial growth of in-person card use.
- Credit card and non-prepaid debit card payments nearly tied for first place in growth by number from 2012 through 2015, both growing by roughly 8% over the period.
- The number of general-purpose card payments initiated with a chip-based card increased substantially from 2012, growing by more than 230% per year, but amounted to only a roughly 2% share of total in-person general-purpose card payments in 2015, during a broad industry effort to roll out chip card technology.
- In 2015, the proportion of general-purpose card fraud attributed to counterfeiting was substantially greater as a share of total card fraud in the United States compared with countries where chip technology has been more completely adopted. Nonetheless, the total share of remote fraud is already substantial (46%) compared to its share in total card payments (19%).
- The number of ACH payments is estimated to have grown to 23.5 billion in 2015, with a value of $145.3 trillion. ACH payments grew at an annual rate of 4.9% by number and 4% by value from 2012 to 2015.
- Check payments fell at an annual rate of 4.4% by number or 0.5% by value from 2012 to 2015. For the first time since the descent began in the mid-1990s, check payments posted a slowing in the rate of decline.

"The data collected for the 2016 study was substantially expanded," said Mary Kepler, senior vice president of the Federal Reserve Bank of Atlanta, which sponsored the study.

"This reflects an increased desire within the payments industry for additional fraud-related information," she said. "A limited amount of fraud information was ready for release today, and further results will be released in 2017 as the complete data set is more fully reviewed and analyzed."

Beginning in 2017, some survey data will be collected annually, rather than every three years, to enhance the value of the study, Kepler added.

"Payment industry participation drives the quality of the study's results," Kepler said. "The Federal Reserve appreciates the industry's response in 2016 and looks forward to working with selected participants for the annual data collection getting underway in the first quarter of 2017."

As in previous studies, the estimates reported are based on information gathered in three survey efforts:

- The *2016 Depository and Financial Institutions Payments Survey* (DFIPS)
- The *2016 Networks, Processors and Issuers Payments Surveys* (NPIPS)
- The *2016 Check Sample Survey* (CSS)

The Federal Reserve partnered with McKinsey & Company on the DFIPS and CSS, and with Blueflame Consulting, of Melrose, Massachusetts, on the NPIPS. The information collected in each survey is combined with information about payments trends from previous studies and then analyzed to produce comprehensive estimates not available in other studies.

Source: FederalReserve.gov

INSURANCE continued from page 9

Chad Hauff, who oversees payment and billing operations as director of premium accounting for Safety Insurance says, "You're working with multiple systems that need to talk to one another," Hauff said. "It's tough to change a system that's been in place and working for years. I don't think anybody is averse to it. Consumers want it and insurance companies want to provide it. It's just always a lot more complicated than you really want it to be."

Despite using decades-old billing and payments systems, the insurance industry has made strides toward making both more streamlined. From mailing paper bills to receiving them online, the industry is changing head to toe—from modernizing information distribution for its customers to upgrading its payments processing machinery.

While processing payments would ordinarily take days or more than a week, faster payment offerings such as Same Day ACH have now made it possible for insurance companies to process transactions almost instantaneously.

But with many insurance companies relying on legacy systems, they are finding themselves in a position where even if their customers were able to send them insurance premiums faster, they wouldn't necessarily be able to apply them to accounts quicker.

"You have your payment systems and payment collection process, but then you have your back-end billing systems and they don't always talk," Hauff said. "The connection is becoming better between the two, so the timeframe it takes to get from collecting the money and posted to your billing account is shorter and shorter."

When looking at the payment collection-to-posting situation, insurance companies are making progress but aren't quite where they need to be yet.

Maximizing Same Day ACH Opportunities

Hauff sees Same Day ACH opportunities on the claims side of the insurance business as well. Case in point? Homeowners affected by Hurricane Matthew. When returning to their devastated properties shortly after the storm, the last thing they should have to worry about is how long it would take them to get their insurance claim check, Hauff said.

Being able to deliver funds to policyholders shortly after they request payment would be a significant accomplishment, he said. Case in point? Homeowners affected by Hurricane Matthew. When they returned shortly after the storm to their devastated properties, the last thing they should have had to worry about was how long it would take them to get to their insurance claim check.

From a non-claims perspective, Same Day ACH also presents opportunities for insurance companies to pay commissions quickly to vendors. "When you're dealing with someone—a supplier, an agency or a contractor—you're not talking about small dollar amounts," Hauff commented. "Sometimes you're talking about big dollar amounts, and they are looking to get paid, so it's important to make sure they get paid in a timely fashion."

Whether it's paying vendors or processing consumers' insurance claims following a natural disaster, speed and accuracy are critical components in both scenarios, as Hauff noted. But will legacy systems prevent companies like his from being able to make faster payments even more quickly than they are processed today?

Source: Faster Payments Tracker

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