

<b>INSIDE:</b> 2015 ACH Rules Changes That Could Impact You.....1	PayPal Hit with Large Settlement for Alleged OFAC Sanction Violation.....6
Survey Finds Many Small Merchants Unaware of Upcoming EMV Liability Shift.....1	PCI Issues New Testing Guidance.....7
PoSeidon Malware Could Sink Retailers.....2	Report Shows Companies Failing Payment Data Security Tests.....8
NACHA Releases Mobile Payments White Paper.....3	New Currency Education Resource Now Available.....9
CFPB Takes on Payday Lenders.....3	Payments Education for Small Businesses.....9
Same Day ACH and the Future of Faster Payments.....4	The Value of Green.....9
Walgreens Sets Example of Success with New Business Model.....6	

## 2015 ACH Rules Changes That Could Impact You

Several ACH Rules changes of significant impact to Originators go into effect this year. 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.

[Click here](#) to download the 2015 ACH Rules Update for Originating Companies to find out which ACH Rules changes may apply to you. Be sure to contact your financial institution regarding any questions you have in regard to how these changes pertain to your current Origination activity. 

## Survey Finds Many Small Merchants Unaware of Upcoming EMV Liability Shift

Another sign that the U.S. EMV conversion has a long way to go emerged recently when a survey of more than 990 independent business owners by Newtek Business Services Inc. revealed that 71% of respondents were unaware of the so-called EMV liability shift coming on Oct. 1. And 81% of respondents answered no when asked if they have upgraded their point of sale systems or terminals to be EMV ready and also accept Apple Pay™—in other words, contactless mobile payments, which the payment card networks hope will get a lift with the EMV conversion.

Newtek offers merchant processing, loans and other services to small businesses. Around 15,000 businesses use their merchant-processing services. The EMV survey, conducted in February, gathered data from merchants calling Newtek’s customer-service lines, including customers who don’t use Newtek’s merchant-processing services.

Only 29% of respondents said yes when asked, “Are you aware that by October of 2015, Visa and MasterCard will hold the merchant

responsible for credit card fraud if they do not have an EMV-compliant terminal?”

Barry Sloane, president and chief executive of New York City-based Newtek, likens the low level of merchants’ EMV awareness to college students who don’t do much studying until test time approaches. “There’s always a fairly significant portion of students that didn’t do anything on their lessons, and cram for their final exams,” Sloane tells *Digital Transactions News*. “I think that level of awareness will pick up.”

Come October, the party to a general-purpose credit or debit card transaction that doesn’t support EMV chip cards, be it the issuer or merchant, will bear liability for any resulting counterfeit fraud. That liability shift has issuers pumping out chip cards en masse this year, and merchants upgrading their POS systems to accept them. Big-box retailers and national restaurant chains are much farther along than small merchants.

The survey had a somewhat more encouraging other finding: 35% of the callers



**ACH Security Framework for Originators**

Learn your new requirements as an Originator  
*FREE On-Demand Course*

[Click Here to Download](#)

see SURVEY on page 2

## SURVEY continued from page 1

who were Newtek merchant-services clients had done something to prepare for EMV, Sloane says.

The big selling point for EMV mostly has been to reduce counterfeiting fraud, to which magnetic-stripe cards are quite vulnerable, and lost-and-stolen card fraud, and also to get the United States in step with most of the rest of the industrialized world where chip cards now dominate. But small-business owners have other things on their minds, says Sloane.

“They think about their revenues, they think about expenses, and they think about their risk,” he says. “Risk is a far distant third.”

The fact that only 19% of the callers claimed to be EMV-ready in February isn’t surprising. Earlier that month, a Visa Inc. executive reported at a Smart Card Alliance conference that only 78,800 merchants were wired and ready to accept EMV transactions, a small fraction of the overall United States merchant base.

Sloane predicts about 80% of his merchants will be EMV-ready by October. Newtek is ramping up its merchant-awareness efforts and running an email offer for a “significantly discounted” Dejavo Systems terminal, according to Sloane. The terminal supports EMV and near-field communication (NFC) transactions, the kind generated by Apple Pay™ and some other mobile-payments systems. 🌱

*Source: Digital Transactions; Jim Daly*

# PoSeidon Malware Could Sink Retailers

Cisco Systems is warning of a new breed of malware technology, nicknamed PoSeidon, that targets point-of-sale systems. This is bad news for retailers that are still reeling from the many data breaches of recent history, such as those that hit Target, Home Depot, Staples and Supervalu. Target is still attempting to settle a class action suit from its 2013 breach, which affected as many as 110 million customers, for \$10 million.

PoSeidon infects machines and scrapes their memory for credit card information, and then exfiltrates that data to servers—many hosted on Russian domains—where it can be harvested and likely resold, according to a post on Cisco Systems’ blog. Data exfiltration is also known as data extrusion, and it is the unauthorized transfer of computer data.

When a system is infected, PoSeidon tries to maintain “persistence” so it will survive a system reboot and avoid detection, which is an advancement in hacking technology. It then contacts a command and control server, leading to the installation of a “keylogger.”

“The keylogger is installed to pull credit card data,” said Craig Williams, senior technical leader for Cisco’s Talos Security Intelligence and Research Group. “It is not

uncommon for more sophisticated and current POS malware samples.”

The malware then scans the infected POS device’s memory for sequences of digits that could be payment card numbers, according to the blog. This leads to the payment card



information being sent to the exfiltration server. The blog post describes many technical details about the threat.

“PoSeidon is interesting because it is self-updateable,” Williams said. “It has interesting evasion technologies, and it has direct communication with the exfiltration servers, as opposed to common POS malware, which logs and stores for future exfiltration from another system.”

Cybercriminals will continue to target POS systems and use increasingly sophisticated techniques to maintain access, Caspida CEO and co-founder Muddu Sudhakar said.

“Enterprises must stop granting unfettered access to employees and third parties that are allowing cybercriminals to take advantage by installing malware like PoSeidon.

“Organizations need to be more proactive and take preventative measures by looking

at threats based on behavior and strengthen encryption.

Cybercriminals are oftentimes taking advantage of enterprises that have not rolled out basic security hygiene and security best practices that have been discussed since the Target breach was first reported in December 2013,” Sudhakar added.

PoSeidon is another in a growing number of POS malware threats demonstrating sophisticated techniques and approaches. According to Cisco, attackers will continue to target POS systems and employ various techniques in an attempt to avoid detection, and as long as POS attacks continue to provide returns, attackers will continue to invest in innovation and development of new malware families. Cisco urges network administrators to remain vigilant and adhere to industry best practices to ensure coverage and protection against advancing malware threats. 🌱

*Source: Fierce Retail*



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

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

Email [thirdpartyservices@epcor.org](mailto:thirdpartyservices@epcor.org) to find out more!



### EXPLORE EPCOR MEMBERSHIP

EPCOR has membership opportunities for companies, businesses, corporations and Third-Parties.

Explore your options by calling 800.500.0100 or visiting [www.epcor.org](http://www.epcor.org).

# NACHA Releases Mobile Payments White Paper

NACHA—*The Electronic Payments Association*® recently announced that its Payments Innovation Alliance released a white paper, “*Leveraging the Mobile Channel for ACH Payment Innovation*.”

The paper asserts that the payments industry and its embrace of mobile stand at an important crossroad. The increasing use of mobile devices by consumers and corporates, the steady introduction of new mobile point-of-sale solutions, and the advancement of the ACH Network together make mobile an important option for moving money and payment information.

“The mobile future is here,” said George Throckmorton, managing director, Advanced Payments Solutions at NACHA. “The use of mobile devices with ACH transactions is ripe for rapid adoption and further innovation given that it is a ubiquitous, low cost means of accessing payments.”

The paper explores the current landscape for mobile payments; the role of mobile in ACH transactions; and assesses the challenges and opportunities of using the mobile channel for ACH for merchants, billers, consumers and corporates.

The Payments Innovation Alliance held a members meeting March 3-5 in Los Angeles to discuss a variety of payments-related topics, including a session dedicated to providing an overview of the white paper and smaller group discussions about the issues it raises around the use of mobile devices in ACH transactions. Launched last year, the Alliance is a membership group that encourages industry dialogue and collaboration to help advance domestic and global payments.

To download a copy of the “*Leveraging the Mobile Channel for ACH Payment Innovation*” white paper, [click here](#). 📄

Sources: NACHA

# CFPB Takes on Payday Lenders

The Consumer Financial Protection Bureau (CFPB) has begun to take the first steps toward more intensive legislation of the short term, small dollar borrowing space—also known as payday lending.

Last week, the Federal consumer watchdog announced that it is considering a proposal that would require lenders to take additional steps to ensure consumers have the ability to repay these loans. The proposed rule would also restrict payment collection methods that apply fees “in the excess.”



“Today we are taking an important step toward ending the debt traps that plague millions of consumers across the country,” CFPB Director Richard Cordray remarked at a Field Hearing on Payday Lending in Richmond, Virginia. “Too many short-term

and longer-term loans are made based on a lender’s ability to collect and not on a borrower’s ability to repay. The proposals we are considering would require lenders to take steps to make sure consumers can pay back their loans. These common sense protections

see CFPB on page 5

# Same Day ACH and the Future of Faster Payments

The financial industry is working to make payments better, more efficient, simpler—and faster. Many Americans are particularly invested in efforts to achieve this last improvement. A recent Federal Reserve study found that 69% of consumer payers and 75% of business payees prefer instant or one-hour payment speed. The key question for all users is what functionality will be required to meet Americans' needs: validation of good funds, settlement of funds, or actual funds availability in a user's bank account?

The automated clearinghouse (ACH) network sits at the epicenter of this dialogue. As the backbone for electronic payments, it supports over 80 million ACH payments each day, including direct deposits and direct payments. It also enables settlements for credit and debit card transactions and ATM transactions. By speeding up processes within this ubiquitous foundational system, the needs of the industry can better be met.

NACHA, which serves as the administrator of the ACH network, identified the need for faster payments six years ago when it implemented Secure Vault Payments. SVP is an online and mobile payment system that leverages the ACH Network and offers a real-time guarantee of good funds, 24 hours a day and seven days a week. Although the technology already exists to meet the demand for faster payments, not all financial institutions have adopted it. We have seen time and again that ubiquity is critical for any change in our vast ecosystem. So when the Federal Reserve cited the lack of a real-time payments system as an issue in their September 2013 paper, NACHA agreed.

But real-time payments are only one part of the solution. While there are some unmet consumer and corporate needs that would benefit from real-time payments, there are many other needs that can be met by same-day payments. Expedited bill payments, payroll applications and many

ad-hoc business payments, for example, would benefit greatly from Same Day ACH. Same Day ACH would allow the network to move payments faster and provide additional functionality that meets the industry's needs for faster payments.



To that end, NACHA is working toward a phased implementation approach that will move the ACH network from next-day settlement to same-day payment processing during three different settlement windows. This would be available for virtually any transaction and provide greater certainty about fund availability, thereby improving the efficiency of hourly payroll disbursements and last-day tax or bill payments. All of this provides a solid foundation on which to build other innovative services.

NACHA's work as a rulemaker for many types of payments and standards has demonstrated the benefit of continually working to bring parties together to identify solutions that balance the needs of various entities. Today's work on Same Day ACH is an industry effort that will serve as a first step to moving payments faster.

Over the past several months, NACHA has methodically collected and analyzed feedback on this approach from financial institutions, businesses, and payments service providers in an effort to identify a workable path forward in advance of formal rulemaking on Same Day ACH. This step will help all parties to think carefully about the rules, tools, and technology that can help

create a bridge from today's payments to those of the future.

## Industry Support for Initiative

The Clearing House, the only private-sector ACH Operator in the country, welcomed NACHA's proposal for same day ACH. "This comprehensive proposal is a significant step forward in continuing to better meet consumer and business needs," said Dave Fortney, Senior Vice President for Product Development and Management at The Clearing House. "Adoption of Same Day ACH settlements will complement TCH's real-time payment system initiative. Together with today's already efficient ACH, Same Day ACH and real-time payments will provide distinct payment options for customers. Consumers and businesses will be able to choose the speed and features required for a broad range of use cases."

## Same Day ACH Goes to Ballot

NACHA – *The Electronic Payments Association* released the Same-Day ACH Settlement ballot on Monday, April 27. The final ballot is substantially similar to what was presented in the Request for Comment issued earlier this year. The changes include: a reduction in the interbank compensation fee; minor changes to the ACH Operator deadline and settlement times for the morning same-day window; a one week change in the effective date for Phase 1 implementation; the addition of an optional, standardized description for Originators' use in identifying files intended for same-day settlement; clarification regarding ACH transactions with invalid or stale Effective Entry Dates; clarification related to processing of return items and contingent effective dates based on a the Federal Reserve Board's path to support the rule. The ballot period closes on May 18th at 5 PM ET. 

Sources: *American Banker*

are aimed at ensuring that consumers have access to credit that helps, not harms them.”

## What Are The Proposed New Payday Lending Rules?

The new protections would apply to all forms of short-term loan products and longer-term credit products that are said to target the most financially “vulnerable” consumers—such as high interest installment loans. If the rule change is made, the CFPB would require lenders to implement one of two options to make sure that borrowers do not end up in an unending cycle of debt.

The first option is called debt trap prevention, and would require lenders to determine, at the outset of a lending process, whether a consumer could repay the loan and all fees on time, without defaulting or re-borrowing.

The second option would require lenders to offer affordable repayment options as well as limit the number of loans per borrower within specific time frames. For longer-term loans, this would mean applying either an interest-rate (and application fee) cap, or limiting monthly payments to equal a maximum of 5 percent of the borrower’s gross monthly income.

## Why So Popular?

As *The Washington Post* put it, “Basically, it mandates the kind of underwriting that payday lending characteristically avoids. This could go a long way toward ending, or at least reducing, payday-lending horror stories.”

And the horror stories are well known—a borrower goes in for a relatively small (couple of hundred dollars) loan, and through partial payments, falling behind, extending the loan and perhaps even taking out supplemental payday loans to pay the first – the borrower ends up paying thousands of dollars in fees after months and sometimes years, before defaulting entirely.

According to a study of 12 million payday loans, one in five borrowers eventually defaulted on their short-term loan and nearly two-thirds ended up renewing it. According to the report, some of those borrowers renewed their loans up to 10 times, turning a “short-term” loan into something they were paying on for a long time. In three-fifths of the cases studied, the fees ended up exceeding the original amount of the loan.

## Unintended Consequences

Research shows again and again the majority of these types of loans are used to cover recurring expenses—food, utilities, rent, mortgage, etc.

It seems that consumers need these loans to get them to their next payday. They may not be able to pay them off at the time, but that doesn’t actually change the reality of the initial need.

Moreover, this leads to a question about harms—and where the most serious risks of harm occur to consumers who regularly make use of short-term loans.

“All of the market is going after people who can’t pay them back? That’s ridiculous,” Nathan Groff, chief government relations officer for Florida-based Veritec Solutions LLC told MPD CEO Karen Webster. “If they don’t get paid back or lose money, it’s not a success.”

It does seem an implausible assumption to make that an entire industry is built upon a business model that plans on consumers defaulting on the loans they are making.

Groff noted that being in the business of giving away money is easy. Being in the business of lending money and getting it back is not easy—which is why subprime borrowers pay so much for their money. At the end of the day, a short-term lender is like any other lender—they need to mitigate their risk.

“Every day we see people who are innovating in lending,” Groff observed. “They say, ‘we’re going to Facebook to use their

data points, we’re going to fine-tune our risk metrics.’ And that’s great—but at some point, when you strip everything away, the fees have to get somewhat close to the risk the lenders are taking.”

And those fees are high, and on average rolled out across an entire year. The harm payday lenders face in this scenario is paying far more than an average borrower would—and that is a real harm especially for the 57 percent of borrowers who earn less than \$35K a year.

However, that harm has to be weighed against the harm of not paying a utility bill on time—which can result in lights being switched off and the possibility of expensive turn-on fees and deposits for continued use. Unpaid traffic tickets or unmade car repairs can both result in loss of transportation, which then risks continued employment. Generally speaking, not eating is a not a good idea—and most payday lendees don’t actually qualify for food stamps.

Overpaying is a harm; starving, losing housing, losing power, losing a job or getting a debt beat out of one are worse harms and ones that are at least risked when one makes the business of short-term lending unpalatable for businesses, if not outright illegal.

There are no easy answers here.

“We gotta be careful. There are people who say there has never been a problem with the product, and there are also people saying anyone who takes [a payday loan] out is in a cycle of debt,” Groff told Webster.

And it’s surely the case that there are bad payday lenders who do need to be cleaned out. However, if any attempt to curtail the payday lending industry is hailed a “progress” merely because the industry is itself evil—well, that should be a concern. Taking away lenders will not take away the need for their loans, and a solution that doesn’t solve for that probably isn’t a real solution at all. 🍌

Sources: PYMNTS.com

# Walgreens Sets Example of Success with New Business Model

Once upon a time, Walgreens' strategy was to build up physical storefronts on the corner of main streets in an effort to ensure consumers had fewer miles and less time to travel to find a location.

Today, Walgreens' director of its mobile innovation program Joe Rago said, the drugstore's strategy is more or less the same, only the retailer aims to reach consumers with the fewest amount of clicks, as opposed to steps.

Rago recently headed a presentation at the Evans Data Developer Relations Conference to discuss Walgreens' transition from physical storefront to physical storefront plus mobile storefront. It's a crucial strategy, too, as Walgreens' mobile customers spend

six times as much as their retail-store-only counterparts, Rago said. Consumers that visit the physical store and the online store, without going mobile, still spend 3.5 times as much as physical-only shoppers.

To put it into perspective, Rago said that in 2009, less than 1 percent of consumers connected and interacted with Walgreens through a mobile device. Today, more than 60 percent of all online traffic that leads to Walgreens began with a smartphone.

That's not to say, however, that Walgreens has abandoned its physical storefront strategy. According to Rago's presentation, two-thirds of people in the U.S. live within three miles of a Walgreens store. But as the number of shoppers with

a smartphone has exponentially increased over the years, so have Walgreens' efforts to capture that audience.

Walgreens' app currently holds third place for today's leading retail mobile apps, Rago's presentation showed, surpassed only by Amazon and Groupon.

Looking ahead, Rago said that Walgreens will look to further integrate its greatest assets across all digital and mobile platforms to take the most advantage of the digital commerce shift. The strategy is especially helpful for Walgreens customers using the mobile prescription refill and the digital photo printing ordering services. 📱

Sources: PYMNTS.com

# PayPal Hit with Large Settlement for Alleged OFAC Sanction Violation

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has announced a \$7,658,300 settlement with PayPal, Inc. (PayPal) to resolve potential civil liability for 486 alleged violations of the Iranian, Sudanese, Cuban, Global Terrorism and Weapons of Mass Destruction Proliferators (WMDP) sanctions programs. OFAC alleged that, for several years up to and including 2013, PayPal failed to employ adequate screening technology and procedures to identify the potential involvement of U.S. sanctions targets in transactions that PayPal processed; consequently, PayPal did not screen in-process transactions in order to reject or block prohibited transactions; even when PayPal instituted automated interdiction filtering that initially identified account holders as potential matches to OFAC's

List of Specially Designated Nationals and Blocked Persons (SDN List), PayPal Risk Operations Agents improperly dismissed alerts after failing to obtain or review documentation corroborating the identity of the SDNs; and PayPal processed hundreds of transactions involving individuals on the SDN List that gave economic benefit to such persons and undermined U.S. sanctions programs. Although all of the transactions at issue totaled only \$43,934 in value, OFAC found some of PayPal's conduct to be egregious and assessed its apparent liability at \$17,018,443.

OFAC cited the following facts as supporting its view that PayPal violated the sanctions regulations:

- PayPal acknowledged that its automated interdiction filter had not been not "working properly."

- After PayPal's filter was corrected, and it appropriately flagged certain transactions involving an SDN's account, separate PayPal Risk Operations Agents dismissed the alerts without requesting additional information to clear the potential SDN name matches (conduct that PayPal asserted did not comply with its internal policies and procedures).
- Even where PayPal's interdiction filter properly flagged an SDN's account as a potential SDN List match, and a PayPal Risk Operations Agent followed procedures by restricting the SDN's account and obtaining additional information from the customer, the Agent mistakenly dismissed the match despite the information showing a date and place of birth that were identical to those on the SDN List.

see **PAYPAL** on page 7

## PAYPAL continued from page 6

The total value of the 486 transactions at issue was only \$43,934. Nonetheless, OFAC determined that the total base penalty for all of the alleged violations was \$17,018,443. In arriving at that amount, OFAC considered the following factors in concluding that PayPal's actions, although deemed to be non-egregious violations of the Iranian, Cuban, Sudanese and Global Terrorism sanctions programs, constituted an egregious violation of the WMDP sanctions regulations:

- PayPal demonstrated reckless disregard when its software failed to identify the SDN as a potential match to the SDN List for approximately six months and when, even after the filter flagged the account-holder as a potential SDN match, employees cleared name matches against the SDN's account on six separate occasions prior to appropriately identifying and blocking the account.
- Multiple PayPal Risk Operations Agents engaged in a pattern of reckless conduct by repeatedly ignoring warning signs about potential matches to the SDN List, and by failing to adhere to PayPal's policies and procedures pertaining to SDN match escalation.

- PayPal's actions provided economic benefit to the SDN and undermined the integrity and objectives of the WMDP sanctions program by operating an account and processing transactions on behalf of an SDN for approximately three-and-a-half years.
- PayPal's management and supervisors knew of the conduct giving rise to the apparent violations, and demonstrated reckless disregard for U.S. economic sanctions requirements in deciding to operate a payment system without implementing appropriate or adequate controls to prevent processing of transactions in apparent violation of OFAC regulations.

Somewhat offsetting these aggravating factors, OFAC found the following to be mitigating factors:

- Following its initial missteps, PayPal's interdiction filter flagged the SDN's account, and PayPal appropriately blocked the account and voluntarily reported it to OFAC.
- PayPal hired new management within its Compliance Division, identified OFAC-related issues with regard to its payment system in 2011, and undertook

- various measures to strengthen its OFAC screening processes and measures, including steps to implement more effective controls.
- PayPal had not received a penalty notice or Finding of Violation in the five years preceding the earliest date of the transactions giving rise to the apparent violations.
- PayPal voluntarily self-disclosed its violations to OFAC and substantially cooperated with OFAC's investigation by submitting relevant documents, responding to OFAC information requests, and entering into a statute of limitations tolling agreement and extension.

OFAC's announcement of its settlement with PayPal is significant. Whereas much of the publicity surrounding the agency's recent enforcement actions has been focused on financial institutions that have stripped identifying information from fund transfer documents to avoid detection of transactions involving persons in sanctioned countries, OFAC's settlement with PayPal may indicate a new, heightened focus on the payments industry and payments processors. 🌱

Source: Davis Wright Tremaine, LLP

NEED TO LEARN MORE ABOUT WHAT OFAC REQUIRES OF YOUR BUSINESS?  
**CLICK HERE FOR OFAC COMPLIANCE 101.**

## PCI Issues New Testing Guidance

New [guidance](#) from the PCI Security Standards Council specifies how businesses should use penetration testing to identify network vulnerabilities that could be exploited for malicious activity.

But while one payments security expert says the guidance could help ensure ongoing compliance with the Payment Card Industry Data Security Standard and improve card security, another says the guidance doesn't go far enough.

Penetration testing is a critical tool for verifying that segmentation is appropriately in place to isolate the cardholder data environment from other networks, the council states in its March 26 guidance release.

"Penetration testing is a critical component of the PCI-DSS," says Troy Leach, chief technology officer of the council. "It shines a light on weak points within an organization's payment security environment which, if unchecked, could leave payment card data vulnerable."

The guidance includes insights about:

- Understanding the different components that make up a penetration test;
- Determining the qualifications of a penetration tester, whether internal or external, through experience and certifications;
- Defining methods used for penetration testing that address the pre-test, test and post-test findings;
- Developing a comprehensive penetration test report.

see PCI on page 8

## A Missing Element?

One payments security expert says the guidance comes up short. “Unfortunately, the PCI Council did not go far enough to require that penetration testing be a manual process, rather than allowing automated penetration-testing tools to be used,” says the payments expert, who asked not to be named.

Manual penetration tests are random tests waged against a network by a skilled network tester, rather than an automated tool. Manual testing is well-suited to evaluating vulnerabilities from many different vantage points, or attack vectors, the expert contends. In contrast, automated penetration tools from vendors can only test limited vantage points, he says.

“Clearly, these vendors were successful in lobbying the council to temper its requirements for penetration testing,” the expert adds.

## A Positive Step?

But Charles Henderson, vice president of managed security testing at security and forensics investigation firm Trustwave, says the new guidance should encourage more businesses to check and test network segmentation. Inadequate segmentation has led to many card data compromises, apparently including the Target breach.

Henderson says most businesses only test vulnerabilities on systems and networks that hold card data. But if these are not properly segmented, hackers can access them through attacks that invade any point on the network, he adds.

“Inadequate segmentation is far more likely to be uncovered under the new guidance, and businesses must test their segmented networks thoroughly to help ensure their data is secure,” Henderson says. “The guidance should also help businesses segment off a smaller cardholder environment.”

When helping businesses achieve security and PCI-DSS compliance, Trustwave often finds that businesses have unnecessarily large cardholder environments—meaning they are

storing card data on more systems than they realize or that their network is not properly segmented, he says.

“A smaller target is easier to protect,” Henderson adds. “It doesn’t directly eliminate the problem, but it does make businesses take segmentation more seriously.”

## Exploiting Vulnerabilities

The new guidance requires that businesses actually attempt to exploit the vulnerabilities they identify. It’s not enough to identify a vulnerability and fix it; businesses must wage simulated attacks against their networks by exploiting the vulnerabilities they find to help determine the level of risk, Henderson says.

And while exploitation requirements were already noted in version 3.0 of the PCI-DSS, Henderson says many businesses have been reluctant to exploit vulnerabilities during a test. “The new guidance makes it crystal clear—penetration testers must identify and exploit vulnerabilities,” he says. 🟢

*Source: Tracy Kitten, BankInfo Security*

# Report Shows Companies Failing Payment Data Security Tests

According to a recent report put out by Verizon Communications, four-fifths of companies fail interim compliance assessments for payment card data security.

For brands that handle payment card data—like the type that come from Visa and MasterCard—the Payment Card Industry Data Security Standard (PCI DSS) functions as the essential rules of the road. The standard exists to protect data by trying to ensure, ahead of an attempted breach, that institutions have a method by which they safely store, process and transmit payment information.

However, by reverse engineering from previous data breaches over the last 10 years, Verizon’s forensics team was not able to find a single breached firm that had been in compliance with all 12 PCI requirements at the time their data was lifted.

The good news out of the report is that between 2013 and 2014, compliance was on the rise in every measurable area except testing security systems. The telecom firm also noted that businesses need to minimize the number of openings into their system though which sensitive data can be extracted through the use of techniques such as network segmentation and data masking.

While most firms are not short on security procedures, Verizon notes, small changes within an organization can often cause systemic effects that damage security in ways that are not immediately obvious.

“We’re in such a constantly changing environment, actually keeping up with the way the architecture and services change, compliance is going to be a snapshot at a point in time,” said Mark Hughes, president of U.K.-

based BT Security, part of BT Global Services.

However, given the ever-changing demands of security, coupled with the fact that full compliance often means increased (and increasingly expensive) infrastructure, data security is rarely seen as a revenue generator and consequently doesn’t always generate maximum enthusiasm.

Moreover, even if an institution nails down PCI compliance, they still have a long ways to go when contemplating keeping all financial data secure.

“If regulations are the beginning and end of your security strategy, you need to rethink your strategy,” a report released Thursday by Forrester Research Inc. says. “Compliance-based strategies have narrow controls that are of limited use to the entire enterprise.” 🟢

*Source: PYMNTS.com*

## ORDER YOUR 2015 ACH RULES TODAY!

RELYING ON OUTDATED  
VERSIONS CAN BE CONFUSING  
AND HURT COMPLIANCE.

CURRENTLY TAKING ORDERS IN THE  
ONLINE STORE AT [WWW.EPCOR.ORG](http://WWW.EPCOR.ORG)



# New Currency Education Resource Now Available

The Federal Reserve Bank's new [Know Your Money](#) educational brochure is now available in 23 languages, including Spanish, Russian and Vietnamese. *Know Your Money* is a comprehensive guide that includes technical information on the security and design features of the current \$5, \$10, \$20, \$50 and \$100 notes. *Know Your Money* can be used to train cash handlers on how to quickly authenticate U.S. currency.

Even with the most technologically advanced security features, it is the educated user of U.S. currency who continues to be

the first and best line of defense against counterfeiting.

Remember, the best way to determine whether a banknote is genuine is to rely on the security features in the note. Protect your money by watching this [short video](#) discussing the design and security features of U.S. currency. Links on this page provide [free training tools](#) to download.

The goal of the currency education program is to provide information on the design and security features of Federal Reserve notes to users worldwide. 

## Payments Education for Small Businesses

The Federal Reserve recognizes that improving the efficiency of their payments processes is not the primary focus of most small businesses. Thus, the Fed has released a [toolkit](#) intended to educate small businesses interested in learning more about payments. The toolkit was produced by the Remittance

Coalition, a group of organizations and individuals volunteering to promote greater use of electronic business-to-business (B2B) payments and electronic remittance data exchanges. (The term "remittance" refers to details about a payment, such as what the payment is for and variances between

the amount billed and amount paid.) It is intended to be used by small businesses and the bankers and advisors who serve them in order to encourage the adoption of electronic B2B payments and remittance information exchanges by small businesses. 

## The Value of Green

April is PayItGreen month. What does that mean to your business? [PayItGreen](#) is an environmental initiative dedicated to providing information that will help businesses and consumers make the switch from paper to electronic payments, statements and bills.

PayItGreen offers a variety of tools and resources that help businesses convert their customers to paperless transactions—an initiative that has both

environmental benefits—and a positive financial impact to your bottom line. The

PayItGreen Seal of Approval identifies your business as one that's dedicated to preserving the environment through reducing the amount of paper used for financial transactions

Wouldn't you like for your organization to be able to proudly display the PayItGreen Seal of

Approval? By taking a quick, FREE survey

your organization can quantify your "green efforts" and earn your Seal. Displaying this seal clearly demonstrates to your customers and your community that your organization has been acknowledged for positively impacting the environment by 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 assessment survey. You can also measure your organization's financial paper footprint using their [Paper Footprint Calculator](#). 





Electronic Payments Core of Knowledge

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

The mission of EPCOR is to provide financial institutions with reliable payments and risk management education, information, support and national industry representation.



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

© 2015, EPCOR. All rights reserved.

[www.epcor.org](http://www.epcor.org)

3100 Broadway Blvd., Ste. 555, Kansas City, MO 64111

800.500.0100 | 816.474.5630 | fax: 816.471.7665