


<b>INSIDE:</b> ACH Rules Update for Originating Companies.....	pg. 1
Global Cost of Data Breaches Increases by 15%.....	pg. 1
FREE Checklist Helps Companies with ACH Rules Security Requirements.....	pg. 2
Disaster Preparedness Toolkit for Small Businesses.....	pg. 3
CFPB Platform Empowers Customers to Publicly Voice Financial Product Complaints.....	pg. 3
FTC & CFPB Ask Court to Overturn Ruling in Debt Collection Notification Case.....	pg. 4

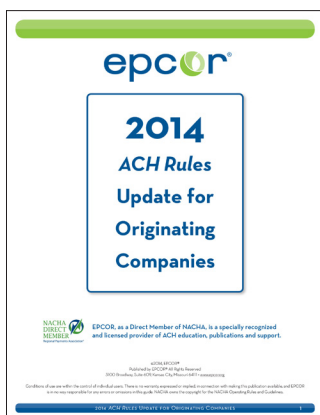
What's New in the World of NFC Terminals?.....	pg. 4
Is the Cloud an Alternative to More Expensive Transaction Processing Options?.....	pg. 6
Federal Reserve Banks Complete Final Phase of Research to Inform Payment System Improvements.....	pg. 7
Are You Prepared? Record Number of Cyber Attacks Target Small Business.....	pg. 7
Small Companies are Susceptible to Export Control Enforcement Actions.....	pg. 9
CMS Issues FAQs on Providers' Rights Regarding Healthcare EFT Standard.....	pg. 9

## ACH Rules Update for Originating Companies

Several 2014 ACH Rules changes of significant impact to Originators went into effect on September 19. How have you been keeping up with this year's changes? As an Originator of ACH entries it is important to stay up-to-date with the ACH Rules, including updates and changes as they arise.

Need a refresher? [Click here](#) to download the 2014 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. 



## Global Cost of Data Breaches Increases by 15%

Ponemon Institute has released its ninth annual *Cost of Data Breach Study: Global Analysis*, sponsored by IBM. According to the study of 314 companies spanning 10 countries, the average total cost of a data breach increased 15% in the last year to \$3.5 million. The study also found that the cost incurred for each lost or stolen record containing sensitive and confidential information increased more than 9% to \$145.

The ninth annual study involved the collection of detailed information about the financial consequences of a data breach. For purposes of this research, a data breach occurs when sensitive, protected or confidential data is lost or stolen and put at risk. Ponemon Institute conducted 1,690 interviews with IT, compliance and information security practitioners representing 314 organizations in the following ten countries: United States, United Kingdom, Germany, Australia, France, Brazil, Japan, Italy, India and, for the first time, the Arabian region (a consolidation of organizations in the United Arab Emirates and Saudi Arabia).

“The goal of this research is not just to help companies understand the types of data breaches that could impact their business, but also the potential costs and how to best to allocate resources to the prevention, detection, and resolution of such an incident,” said Dr. Larry Ponemon, Chairman and Founder of Ponemon Institute. “This year’s *Cost of Data Breach Study* also provides guidance on the likelihood an organization will have a data breach and what can be done to reduce the financial consequences.”

All those interviewed are knowledgeable about their organization’s data breach and the costs associated with resolving the breach. All participating organizations experienced a data breach ranging from a low of approximately 2,400 to slightly more than 100,000 compromised records, which identifies the individual whose information has been lost or stolen in a data breach.

“Clearly, cybersecurity threats are a growing concern for businesses, especially when we consider how persistent data has become in the age of cloud and mobility,” said Kris Lovejoy, General Manager, IBM Security

**see GLOBAL COST on page 2**

## GLOBAL COST continued from page 1

Services Division. "A data breach can result in enormous damage to a business that goes way beyond the financials. At stake is customer loyalty and brand reputation."

The following are key takeaways from the global *Cost of Data Breach Study*:

- Root causes of data breaches differ among countries and affect the cost of the breach. Countries in the Arabian region and Germany had more data breaches caused by malicious or criminal attacks. India had the most data breaches caused by a system glitch or business process failure. Human error was most often the cause in the UK and Brazil.
- The most costly data breaches were those caused by malicious and criminal attacks. The U.S. and Germany paid the most at \$246 and \$215 per compromised record, respectively.
- A strong security posture was critical to decreasing the cost of data breach. On average, companies that self-reported they had a strong security posture were able to reduce the cost by as much as \$14 per record.
- The involvement of business continuity management reduced the cost of data breach by an average of almost \$9 per record.
- The appointment of a Chief Information Security Officer (CISO) to lead the data

breach incident response team reduced the cost of a breach by more than \$6.

- The probability of a company having a data breach involving 10,000 or more confidential records is 22% over a two-year period.

Consistent with previous *Cost of Data Breach* studies, the most common cause of a data breach is a malicious insider or criminal attack. In this year's study, we asked companies represented in this research what worries them most about security incidents, what investments they are making in security, and the existence of a security strategy.

Following are some of the key findings:

- The greatest threats to the companies in this study are malicious code and sustained probes.
- Only 38% of companies have a security strategy to protect its IT infrastructure. A higher percentage (45%) has a strategy to protect their information assets.
- Malicious code and sustained probes have increased the most. Companies estimate that they will be dealing with an average of 17 malicious codes each month and 12 sustained probes each month. Unauthorized access incidents have mainly stayed the same and companies estimate they will be dealing with an average of 10 such incidents each month.
- The majority of companies (50%) have

low or no confidence that they are making the right investments in people, process and technologies to address potential and actual threats.

- Ideally companies would like to invest \$14 million over the next 12 months to execute their organization's security strategy. However, in the next 12-month period, companies anticipate having an average of about half that amount, or \$7 million, to invest in their security strategy.

**Ponemon** also released *The Economic Consequences of an APT Attack* study sponsored by Trusteer, an IBM company. This newly released report is part of a larger research study entitled, *The State of Advanced Persistent Threats*, published in December 2013. This original research of 755 U.S. IT security practitioners supports the findings of *The Cost of Data Breach Study*, wherein targeted criminal attacks are considered by a majority of respondents to be their organization's greatest threat. Another corroborating fact is a finding that reputation damages represent the most costly component or consequence of criminal attacks, and especially those involving the theft or misuse of information assets. Respondents in this study estimate an average cost to restore reputation as much as \$9.4 million. 🟢

Source: Wireless Design & Development

## FREE Checklist Helps Companies with ACH Rules Security Requirements

The *ACH Rules* require Originators to establish, implement and (as appropriate) update security procedures relating to the initiation, processing and storage of entries. The *ACH Security Framework Checklist* provides examples of how to handle, move and destroy ACH data in a secure manner. Also included are considerations to help

protect ACH data and additional resources.

[Click here](#) to download the Checklist.

For details on the ACH Security Framework Rule that went into effect September 20, 2013 please refer to the [2014 ACH Rules Update for Originating Companies](#). 🟢

A graphic for the ACH Security Framework for Originators. It features a blue header with the text "ACH Security Framework for Originators". Below the header, it says "Learn your new requirements as an Originator FREE On-Demand Course". At the bottom, there is a button that says "Click Here to Download". The background of the graphic shows a close-up of a computer keyboard with a key that has a shield icon and the word "SECURITY" on it.

**ACH Security Framework for Originators**

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

[Click Here to Download](#)

# Corporate User ACH Quick Reference Cards

Get fingertip access to critical information for the correct handling of ACH Returns, Dishonored Returns, Standard Entry Class (SEC) Codes, Transaction Codes and Notifications of Change (NOC).

**ORDER NOW IN THE ONLINE STORE!**



# Disaster Preparedness Toolkit for Small Businesses

Knowing what to do before, during and after disruptions or large-scale disasters is critical. A small investment of time now can help alleviate major challenges, and costs, in the future.

To assist you, The Federal Emergency Management Agency (FEMA) has collected some leading resources so you can quickly

find what you need. Whether you have a few hours to get started with a few of the basics or time to invest in implementing a full business continuity plan, there is something here for every small business.

[Click here](#) to access the FREE Toolkit. 📄

Sources: FEMA

# CFPB Platform Empowers Consumers to Publicly Voice Financial Product Complaints

The Consumer Financial Protection Bureau (CFPB) has created a new tool to empower consumers to publicly voice their complaints about consumer financial products and services. When consumers submit a complaint to the CFPB, they have the option to share their account of what happened in the CFPB's public-facing Consumer Complaint Database. Consumer narratives provide important context to the complaint, helping the public detect specific trends in the market, and aiding consumer decision-making to drive improved consumer service.

"The consumer experience shared in the narrative is the heart and soul of the complaint," said CFPB Director Richard Cordray. "By publicly voicing their complaint, consumers can stand up for themselves and others who have experienced the same problem. There is power in their stories, and that power can be put in service to strengthen the foundation for consumers, responsible providers and our economy as a whole."

The CFPB accepts complaints on many consumer financial products, including credit cards, mortgages, bank accounts, private student loans, vehicle and other consumer loans, credit reporting, money transfers, debt

collection and payday loans.

When consumers submit a complaint to the Bureau, they fill in information such as who they are, who the complaint is against and when it occurred. They are also given a text box to describe what happened and can attach documents to the complaint. The Bureau forwards the complaint to the company, allows the company to respond, gives the consumer a tracking number and keeps the consumer updated on its status.

The CFPB's Consumer Complaint Database is the nation's largest public collection of consumer financial complaints. It includes basic, anonymous, individual-level information about the complaints received, including the date of submission, the consumer's zip code, the relevant company, the product type, the issue the consumer is complaining about and the company's response.

## Narratives Add Significant Impact to the Consumer Complaint Database

The CFPB contends the narratives are the most insightful part of a complaint. They provide a first-hand account of the consumer's experiences and the problem they

see **COMPLAINTS on page 4**



# What's New in the World of NFC Terminals?

Most of the largest retailers have moved to EMV-based systems (EMV is short for Europay, MasterCard and Visa, sometimes referred to as chip and PIN), but smaller businesses are well behind. And of those that have embraced the chip card standard, most also are including Near Field Communication (NFC) chips in the terminals, executives at terminal manufacturer VeriFone Systems Inc. noted during a fiscal third quarter earnings call with analysts in September.

The question is, are the EMV or NFC functions activated? In all likelihood, they're not. "Most Tier 1 retailers already have EMV in place," VeriFone CEO Paul Galant said "It's really about turning the system on as opposed to putting in terminals."

In the U.S., about 30 percent of terminals thus far are equipped to accept EMV cards, Galant noted on the call. That leaves millions of terminals remaining that must be converted so merchants can avoid taking on liability should they not be able to accept a presented EMV card starting in October 2015.

Most EMV terminals VeriFone is shipping include NFC chips, Galant noted. "What we shipped in the third quarter, almost every EMV terminal had an NFC chip in it. It's not a terribly expensive piece of equipment, and it kind of safeguards you from future opportunities," he said.

More than 80 percent of VeriFone's products shipped in the United States during the quarter were EMV-capable, up from approximately 70 percent in the first quarter, Galant said. Also during the period VeriFone upgraded 14 top retailers to its MX 900 series of EMV devices, including an order from one of the world's largest retailers for

see **TERMINALS** on page 5

## COMPLAINTS continued from page 3

would like resolved. The benefits of sharing the narratives include:

- **Providing context to the complaint:** Including the consumer's narrative increases the level of detail available to consumers, consumer groups and companies in the market for services. Describing the circumstances can provide vital information about why the consumer believes they were harmed, and the impact that harm has had on the consumer.
- **Spotlighting specific trends:** Not only does the narrative provide context to the individual complaint, it provides context to the marketplace, enabling detection of trends across the consumer experience. For example, reviewers may see that a number of consumers are starting to receive a \$10 mystery charge from a particular company. Or they may see that more and more companies are failing to meet their student loan servicing obligations. Without the narrative, the public cannot fully connect the dots.
- **Helping consumers make informed decisions:** Consumers often go online to research products before they make a decision to purchase. Including the details of a complaint would help inform consumers who are considering

a particular product or service.

Databases with narratives, such as the Consumer Product Safety Commission's SaferProducts.gov or the National Highway Traffic Safety Administration's SaferCar.gov, have helped inform consumers about a range of products from cribs to cars. The CFPB aims to empower consumers with the same kind of information. Reviewers could use the narrative to decide for themselves if the problems experienced by other consumers would stop them from purchasing the same product or service.

- **Spurring competition based on consumer satisfaction:** With these powerful stories readily available to the public, companies may have additional incentives to address potential shortcomings in their businesses that could have negative impacts on consumers. In the end, the narratives may encourage companies to improve the overall quality of their goods and services and more vigorously compete over good customer service.

Complaints are listed in the database only after the company responds to the complaint or after it has had the complaint for 15 days, whichever comes first. 📌

Sources: CFPB

## FTC & CFPB Ask Court to Overturn Ruling in Debt Collection Notification Case

A recent Urban Institute analysis of the credit files of nearly 7 million Americans revealed that 35% have a debt so far past due it had been referred to a collection agency. And this has led to a strong market for debt-collection agencies, not all of which have operated in accordance with the law.

In some cases, collectors may have failed to give proper notice to indebted consumers when trying to collect, in violation of the Fair Debt Collection Practices Act, or FDCPA.

Last week, the Federal Trade Commission (FTC) joined with the Consumer Financial Protection Bureau (CFPB) in filing a friend-

see **RULING** on page 5

## TERMINALS continued from page 4

40,000 MX 900 units, he said. None of the 14 retailers were in the hospitality industry or quick-service restaurants, though Galant said VeriFone believes they will be coming aboard with EMV soon.

“It’s important to note that a similar percentage of our terminals in the United States included embedded NFC chips, and the migration to EMV will certainly significantly increase the installed base of NFC terminals and the potential for the use of NFC in payment and commerce, moving forward,” Galant said.

This is playing an even more significant role with the Apple’s recent introduction of the new iPhone 6 and iPhone 6 Plus.

In the United States, the increased focus and importance of EMV and security is also driving demand for VeriFone’s Payment-as-a-Service offering, which incorporates EMV terminals with a simplified certification process. It also includes so-called end-to-end encryption to protect cardholder data at the device level and at the back end to reduce the scope and cost of maintaining PCI compliance.

Driving interest in the service are merchants, acquirers and integrators that are becoming increasingly interested in secure devices and an easier path to enabling EMV acceptance, managing the intensifying risk posed by cyber-criminals and reducing the burden of compliance obligations, Galant said.

The bottlenecks to EMV migration have been certifications, Galant adds. “It is quite a cumbersome process to certify the EMV terminals across the very large landscape of issuers, of card networks and of acquirers,” he said. “We’ve been, at VeriFone, working to help the acceleration so that our merchants can get their environments up and running and reduce their exposure to the cyber criminals. So, it’s really been a lot of work, a grassroots effort, a lot of innovation on the technology side.” 🟢

Sources: *Pymnts.com*

## RULING continued from page 4

of-the-court brief in a case that concerns interpretation and enforcement of that law as it pertains to such notifications. The fact they did so illustrates the importance they see in clarifying the law, as the most complaints they receive are about collection practices related to credit card, mortgage, health care and other debts.

In the case, a federal judge granted summary judgment to a law firm, Williams Zinman & Parham P.C. (WZP), who was sued by Maria Hernandez, who complained the debt-collection letter she received from the firm violated the FDCPA because it didn’t properly advise her that in order to dispute the debt she would have to do so in writing. The law firm contends it didn’t have to comply because Hernandez received the initial debt-validation notice requiring such information earlier from another collection agency, Thunderbird Collection Specialists.

According to the summary judgment ruling, WZP contends that Hernandez’s complaint rests entirely upon her false assumption that its letter also must comply with the FDCPA as a debt-validation notice. However, because its letter to Hernandez was not the “initial communication” with respect to the debt, WZP contends that its letter did not need to comply with the FDCPA as a debt-validation notice.

Though the courts are divided as to whether both the initial debt collector and each subsequent debt collector must provide a debt-validation notice in their initial communication with a consumer, the judge ruled in WZP’s favor because its notice was not the original one Hernandez received.

“Under the FDCPA, it is “the” initial communication with the consumer that triggers the mandatory debt validation notice requirements,” the court ruled. In the district court’s view, regardless of whether the initial debt collector sent a notice that complied with the act, a subsequent debt collector like WZP had no obligation to comply with the provision.

In their amicus brief, the FTC and CFPB argue that each debt collector that contacts a consumer, not just the first debt collector that attempts to collect a particular debt, must send a notice that complies with the act’s notification provision. As such, they are asking the Ninth U.S. Circuit Court of Appeals to reverse the U.S. District Court’s March ruling granting summary judgment to WZP.

The brief asserts that harmful debt-collection practices remain a significant concern, as the bureau and FTC receive more complaints about debt-collection practices than any other issues. By imposing the written-notification requirement on “a debt collector,” Congress indicated that each debt collector that attempts to collect a debt from a consumer must provide the required notice, the agencies contend.

The district court, however, “impermissibly narrowed the law’s reach to only the first of what is often many debt collectors that handle a particular debt,” the FTC and CFPB noted. “That narrow interpretation has no basis in the statute’s text or purposes”.

Last November, the CFPB took its first step toward considering consumer-protection rules for the debt collection market when it began collecting information on a wide array of issues, including the accuracy of information used by debt collectors, how to ensure consumers know their rights and the communication tactics collectors employ to recover debts. The Bureau also added consumer complaints about debt collections to its public Consumer Complaint Database.

“For decades, many consumers have reported various unacceptable practices in the debt collection industry,” CFPB Director Richard Cordray said in announcing the changes. “We want to ensure that all players in the industry are working with correct information, that consumers are fully informed, and that consumers are treated fairly and with dignity.” 🟢

Source: *FinCEN*

# Is the Cloud an Alternative to More Expensive Transaction Processing Options?

Many companies are starting to turn to enterprise resource planning (ERP) initiatives to help streamline their supply-management, B2B (business-to-business) invoicing and other business operations.

In a recent blog post, Joshua Morrison, whose company Tradeshift operates a cloud-based transactional business, noted that ERP software is becoming more common for handling transaction processing, specifically within accounts payable and purchasing. “Many United States companies have made significant

capital investments in corporate ERP software to manage these transactions and look to leverage the ERP as much as possible to maximize the value from their associated costs.”

While acknowledging why they do so, given that the average ERP implementation across all industries costs nearly \$10 million, and even more for manufacturers where the average costs reach almost \$11.5 million, he suggested they could benefit from using a third party’s cloud-based Software as a Service (SaaS) to support their transaction processing.

“There remains not only a heavy reliance on company ERP platforms for transaction processing, but also a high cost to manage the platforms and to change providers as well,” he noted. “While processing financial transactions directly within the ERP was once

considered the best solution to centralize company data, many businesses now struggle to maintain their ERPs, to stay current with release updates and patches, as well as take advantage of best practices and new technologies in the industry.”

Moreover, Morrison noted, as business becomes more global and geographic restrictions continue to dissolve, “it becomes more imperative for businesses to employ a solution that will provide a consistent, controlled, cost-effective and fluid approach to managing financial transactions. This is where SaaS can help.”

In his own ZDNet commentary responding to Morrison’s “hybrid approach,” technology consultant Joe McKendrick notes he raises points worth considering as companies weigh what enterprise applications to run in-house versus off-site.



“Morrison proposes a hybrid approach that leaves analysis and reporting work in on-premises ERP systems, and offloads transaction processing to a [SaaS] provider,” he said. “Cloud offers a lot of functionality for small to medium-size businesses that usually can’t handle the costs of ERP systems. This may not involve sensitive, internal corporate financial data, but data that is shared between trading partners.”

Morrison contends SaaS will not replace the ERP. Instead, it would complement it through the integrated exchange of transactional data to feed ERP and support enterprise

planning, reporting and analytics.

“Remember planning, reporting and analytics? This is what ERP was intended to do, not to handle transaction processing!” he wrote. “Knowing this, major ERP providers are taking steps to move into the cloud SaaS space through acquisition and portfolio expansion. However, I expect that they will be slower to adapt to customer demands and bring new deliverables to market given their large and segmented structures.”

There has been, however, a significant increase of third-party SaaS provider offerings to address this space, Morrison wrote. “It is becoming a best practice to migrate the processing of financial transactions with supply chain partners outside of the ERP and into the cloud,” he said. 🟢

*Source: Pymnts.com*

# Federal Reserve Banks Complete Final Phase of Research to Inform Payment System Improvements


The Federal Reserve Banks have spent the last year conducting an extensive program of research and input gathering designed to inform an initiative to improve the speed, efficiency and security of the United States payment system. The effort began last fall with release of the “Payment System Improvement – Public Consultation Paper” which solicited comments on gaps and opportunities in the payment system. The paper described desired outcomes, strategies and tactics to shape the future of U.S. payments, as well as the Federal Reserve’s role in implementing the strategies and tactics. In addition to the consultation paper, the Federal Reserve also completed a number of research initiatives designed to inform future plans for payment system improvements.

One of these research efforts explored the needs related to faster retail payments, one of the consultation paper’s desired outcomes, and included insights on end-user demand for specific payment attributes and a consultant-led assessment of alternatives for speeding United States payments. A second initiative involved identifying gaps and opportunities related to payment system

security. Finally, an analysis of the business case to adopt the ISO 20022 international payment standard for the U.S. payment marketplace was conducted in collaboration with three other industry organizations: The Clearing House Payments Company, NACHA – *The Electronic Payments Association* and the Accredited Standards Committee X9. The results from these key research efforts were shared via a number of industry forums hosted by the Federal Reserve in June 2014 at various locations across the country. Summaries of these work efforts and stakeholder input received can be found at [FedPaymentsImprovement.org](http://FedPaymentsImprovement.org).

“Stakeholders from all corners of the payment industry have demonstrated great enthusiasm for working together to identify and implement needed payment system improvements,” said Gordon Werkema, First Vice President of the Federal Reserve Bank of Chicago with responsibility for industry relations for Federal Reserve Financial Services. “The tremendous participation in our research initiatives and attendance and engagement at our forums is a testament to the focus and energy around these critical payment issues.”

The Federal Reserve plans to use research conclusions and stakeholder feedback to prepare and share in the coming months a roadmap for payment system improvements. “Staff and leaders from around the Federal Reserve System are working diligently to craft a thoughtful and effective path forward,” commented Narayana Kocherlakota, president of the Federal Reserve Bank of Minneapolis and chair of the Financial Services Policy Committee. “The Federal Reserve remains committed to its mission of payment system integrity, efficiency and accessibility, and we look forward to ongoing collaboration with stakeholders this year and beyond to improve the ability of the U.S. payment system to meet evolving end-user needs for speed, efficiency and security,” said Kocherlakota.

For more information on these opportunities and to subscribe to strategic direction updates from the Federal Reserve Banks, visit [FedPaymentsImprovement.org](http://FedPaymentsImprovement.org). 

Source: NACHA

## Are You Prepared? Record Number of Cyber Attacks Target Small Business

If you think your business is too small to be an attractive target for cyber criminals or you don’t have anything worth stealing, think again: The [2012 Data Breach Investigations Study](#) by Verizon shows that in 855 data breaches they examined, 71 percent occurred in businesses with fewer than 100 employees. Verizon’s 2013 Report shows attacks on small business increasing in record numbers as well.

The report has been intently reviewed by Vikas Bhatia, a New York-based security expert who heads Kalki Consulting, a company that helps organizations identify and prevent security related risks. His team supports organizations of all sizes, but he reports that the level of unpreparedness and naivety in small businesses, in particular, is an epidemic.

To address this chronic issue Bhatia’s company recently published a How-To-Guide on Cyber Security for the NYC program that is available to all. [Click here](#) to see the presentation.

To address the growing and chronic issue of cyber security and small businesses, there are some surprisingly simple things that can be done to alleviate or even eliminate the lion’s share of the small business’ risks.

see **ATTACKS** on page 8



## ATTACKS continued from page 7

Bhatia shared some interesting stories. A three-person upstart company located in downtown Manhattan recently fell victim to the theft of its three Mac Air computers, when a petty thief managed to walk the three machines out the door. Where was their business data? You guessed it. On the company laptops. No backup. In an instant, the business lost a year and a half of research and development.

Other cases emerge where entrepreneurs think their data is safe because it's been stored "in the cloud." "Where is the cloud?" Bhatia asks. "Do they know? Are they paying attention?" He points to a number of recent cases where cloud services for sensitive data such as electronic medical records have been breached.

Another recent incident Bhatia reports: An employee in a small business had taken data she shouldn't have had access to from the company's owner. When Bhatia's team investigated, however, they found something even more alarming: over a three month period there had also been three and a half thousand scurrilous attempts to enter the company's website from locations all over the world.

"Who is designing and setting up your company's website?" Bhatia asks. "We see all of these small businesses working with service providers spinning up sites for them on platforms like WordPress, but is the developer of the site or the group helping protect you from the risks that exist for these platforms, or are they even aware?"

As Bhatia asks these questions of customers, he says he's increasingly accustomed to the response he gets in most cases: a blank stare.

"We used to think the primary cybersecurity threats were coming from adult websites," he said. "But not anymore. Legitimate sites you visit – such as Dr. Smith's dental practice, to check for opening hours—can be affected with malware that looks for your credit card numbers, social media passwords, Excel files, QuickBooks files—if I'm a bad guy who's

financially motivated (as 70 percent of cyber criminals are) I'm honed in on how to obtain enough details to open up a credit card in a person or a company's name."


Bhatia mentioned another risk most small businesses are entirely naïve to: What do you advertise about the clients you work with?

"It is a common practice for a small business to advertise their client list," Bhatia tells me. "But what they don't realize is that cyber criminals are viewing you as a stepping stone into your client's organization as well. If they find out your company works with 'Global Investment Bank,' for example, you become a potential target, because the criminal knows you have at least email communication with the people in that organization, and potentially even more."

In the course of conducting your business do you store client information or intellectual property of any kind? Product designs? Customer lists for campaign fulfillment? All of this information presents a cyber-security risk.

Recently a young entrepreneur was hacked. What happened exactly? In his case, the attack began innocuously enough when his Facebook password was compromised. Fortunately for him, he was watchful enough to realize that within minutes his Instagram and Twitter accounts were also being targeted and that the effort was being orchestrated in an effort to affect his business.

"I realized I was making my business vulnerable by having similar passwords on my various social media accounts," the executive said. He quickly addressed the issue by buying a software program called LastPass that allowed him to create and manage more secure passwords on all of his bank accounts and business services as well as his social media accounts. "It was just \$12 a year and packed with features," he said. "This was a quick and simple step I'd recommend to anyone." Bhatia recommends five easy steps for small businesses that can make a substantial difference in their protection from cyber-attacks, as follows:

- 1. Use different passwords for every account and be sure they are strong.** "If your password can be found in a dictionary it can be hacked in 30 seconds," he says. Use different passwords for email, social media and business accounts. Consider using password managers such as LastPass to help you manage and store password information securely.
- 2. Conduct regular backup of business data, and be sure the backed up data is located off site and that you periodically test the data restore.** "I speak to so many small business owners, including those who were affected by Hurricane Sandy, and ask 'Did you make a backup? And where is it?' And we discover the backup drive or computer is in the same room and was affected by the disaster as well."
- 3. Keep your antivirus software up to date, and stay abreast of all software patches and updates.** "Any antivirus or malware software provider expects your software to be downloaded and installed; if you don't update the program, you may as well not have it," he says. He also debunks the myth that Macs can't be attacked or affected by Malware. They can.
- 4. Be conscious of the personal information you share.** "How much information do you share willingly?" All it takes is enough pieces to allow the criminal to create a collective picture and they have access not only to you, Bhatia says, but potentially to everybody you are connected to in your business or social networks as well.
- 5. Know where your cloud-based data is stored.** "What do you have and where is it? Within the city, the state, within the United States or offshore? How is it being secured? What is the provider's liability for protecting your data? If you are using low cost or free outsourced providers, as many small businesses are, these are important questions to ask." 

Source: *Forbes.com*



# Small Companies are Susceptible to Export Control Enforcement Actions

A recent United States Office of Foreign Assets Control (OFAC) enforcement action illustrates how small businesses are not immune from government investigations and enforcement actions for alleged violations of export control laws. According to an [OFAC press release](#), a small tech company settled the enforcement action by paying \$504,225 for alleged violations of export control laws when its distributors re-exported broadband wireless goods to Iran.

The action involved a small tech company with a little over 100 employees. The action involved the company's distributors in the United Arab Emirates and Greece, which obtained broadband wireless goods pursuant to its distribution agreement with the small company. The distributor in turn re-exported the equipment to Iran. In determining the

penalty amount, OFAC considered the fact that the small company did not have a compliance program in place and did not voluntarily disclose the alleged violations when it knew or had reason to know of the alleged violations, among other findings. OFAC's determinations highlight the dangers that small businesses face as they expand to the global market without insight into the various complex export control laws regulating the business.

Here are the takeaways from the enforcement action:

- Small companies are just as susceptible to government investigations as large companies for alleged violations of export control laws, such as ITAR, EAR and those laws enforced by OFAC.
- A compliance program is crucial for

companies conducting international business.

- A company's executives and upper management must actively "buy in" to a compliance program and enforce it. All of a company's employees, distributors and agents must know of and understand the compliance program.
- Foreign distribution or dealer agreements should contain representations, rights and obligations to help United States companies mitigate the risk of violating export control laws.
- Companies should investigate their distributor's background and audit their practices. 🟢

*Source: Joaquin M. Hernandez, Schwabe, Williamson & Wyatt, Attorneys at Law*

## CMS Issues FAQs on Providers' Rights Regarding Healthcare EFT Standard

In response to industry questions regarding health plans or their vendors' ability to charge providers a percentage of the transaction value to receive the healthcare EFT standard (CCD+Addenda), Centers for Medicare & Medicaid Services (CMS) issued [FAQ 9778](#) that states that a health plan may not:

- Delay or reject an EFT or ERA transaction because it is a standard
- Charge an excessive fee or otherwise give providers incentives to use an alternative payment method to EFT via the ACH Network

Providers who choose not to use the ACH Network may continue to receive payments by check, Fedwire and other payments networks.

For any payment method, CMS recommends that providers carefully review the agreement for any added fees.

NOTE: CMS has been requested to define "excessive fees" and is currently reviewing the term in relation to HIPAA violation reports that have been filed. The definition of excessive fees and health plans charging providers to deliver the healthcare EFT standard (CCD+Addenda)

was also a topic of discussion at the National Committee on Vital and Health Statistics (NCVHS) Subcommittee on Standards hearing in June. Several panel participants requested that NCVHS prohibit health plans from charging providers to deliver the healthcare EFT standard or require them to have a free healthcare EFT option available and published for providers. 🟢

*Source: NACHA*



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.

© 2014, EPCOR. All rights reserved.

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

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

800.500.0100 | 816.474.5630 | fax: 816.471.7665