BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVII NUMBER 10

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.

This issue went to press on October 19, 2017

From the Frontline to the Boardroom

CyberSecure Your Bank

by Teri Wesley

Ghosts, goblins, witches, and demons will soon be roaming the streets in search of tasty treats on Halloween night. Cyber attacks, data breaches, BEC (business email compromise) scams, and wire transfer fraud are just a few of the evil forces that haunt bankers every night throughout the year.

The 14th annual National Cyber Security Awareness Month (NCSAM) – an initiative co-founded and led by the National Cyber Security Alliance (NCSA) and the U.S. Department of Homeland Security (DHS) to promote online safety and increase national cyber resiliency – is underway this month. Held every October, the NCSAM promotes specific themes each week. The first week highlighted simple steps for consumers to take for online safety. The second week focused on cybersecurity in the workplace, and the remaining weeks cover securing new and emerging technologies, building the cyber workforce, and promoting cybersecurity in critical infrastructure. Results of a recent survey conducted by security training firm MediaPro revealed that seventy percent of respondents lacked some degree of security and privacy awareness. Other notable findings from the study include:

- Nearly a quarter (24%) of employees surveyed took potentially risky actions when presented with scenarios related to organizational physical security, such as letting strangers in without identification.
- A lack of awareness related to safe social media posting, choosing risky actions such as posting sensitive employer information on their personal social media accounts was reported by 20% of employees.
- An alarming number (19%) of respondents take risky actions related to working remotely, i.e., connecting their work computers to an unsecured public WiFi hotspot.
- Many respondents (12%) failed to recognize common signs of malware when presented with real-life examples, such as a sluggish computer or anti-virus software unexpectedly switching off.

(continued on next page)

Bank Regulator Breaches

by Teri Wesley

In the wake of several high-profile breaches, government agencies and federal regulators are under scrutiny for their own cyber inefficiencies….and many of them are falling short. In conducting recent audits, the Office of Inspector General (OIG) found that information security fell short across 24 reviewed agencies in the areas of network authorization and security management protocols. The OIG reported that the Federal Deposit Insurance Corp (FDIC) suffered more than 50 data breaches between January 2015 and December 2016. The OIG reviewed 18 of 54 suspected breaches that jeopardized personally identifiable information (PII) of U.S. citizens, and found that the FDIC failed to perform impact assessments or communicate with the Data Breach Management Team within the designated timeframe for 13 of the 18 reviewed breaches. It was about 288 days from the discovery of a breach before the FDIC informed impacted individuals, and about 67% of the reviewed breaches took more than the 72-hour timeframe required for initial investigator actions. It took the agency, which did not have an incident response coordinator, an average of 21 days to complete these tasks. The bank regulator has until September 2018 to correct the issues the OIG highlighted.

CyberSecure Your Bank
(continued from front page)

A new initiative was launched this year titled "CyberSecure My Business." The program's interactive training is based on the NIST Cybersecurity Framework. Hosted in partnership with the FTC, with support from the FBI and DHS, the initiative includes workshops and webinars providing guidance on integrating cybersecurity practices, and incorporates content from federal and industry partners, including recent threat data. The same principles this comprehensive program is founded on can be applied to CyberSecure Your Bank. In addition to training your staff from the frontline to the boardroom, the framework provides the following steps you can take to better guard your institution's backdoor against cyber threats:

Identify: Conduct an inventory of your most valuable assets – those of greatest importance to your business and of most value to criminals – such as employee, customer and payment data.

Protect: Assess what protective measures you need in place to defend your institution as much as possible against a cyber incident.

Detect: Have systems in place to alert you if an incident occurs, and the ability for employees to report problems.

Respond: Make and practice an incidence response plan to contain an attack and maintain vital operations in the short term.

Recover: Know what to do to return to normal business operations after an incident or breach.

In today's volatile cyber landscape, it's not a matter of "if" but "when" a cyber incident will occur. When your turn comes around to respond to a cyber incident, make sure all the Ts are crossed, the Is dotted, and the ducks are in a row to comply with data breach laws and regulations. This month and throughout the year, treat your staff to ongoing cybersecurity education and training to arm them with the knowledge and tools to uncloak bad actors disguised as friendly ghosts who come knocking on your backdoor with nefarious tricks up their sleeve.

At this year's Bank Security Conference, on Day 2 of the two-day conference, Jeff Spivey, CRISC, CPP, PSP, President of Security Risk Management, Inc., will present "*Current Trends In Cyber Security and What Security Managers Can Do"* with insight into emerging cybersecurity trends putting your institution at risk.

IN THE *News*

Payday Loan Rule Finalized – Finally!

Following five years of debates, feedback (more than one million comments from lenders, borrowers and consumer advocates) and amid much controversy, the long-awaited final rules for payday lending were finalized by the Consumer Financial Protection Bureau (CFPB) on October 5. The new rules will require lenders (and banks) to verify the ability of borrowers' to repay a loan, limit loan flipping and cap automatic debit attempts. The rule is designed to protect consumers who find themselves in need of quick cash, which often leads to predatory lenders and consumers trapped in loans they can't afford. The rule primarily applies to two types of loans (with some exceptions): short-term loans with terms of 45 days or less (including 14-day and 30-day payday and vehicle title loans), and longer-term (more than 45 days) loans with balloon payments. One of the key requirements under the new rule is a reporting requirement. Companies may become designated as "registered information systems" by the CFPB. Lenders making short-term loans and longer-term balloon-payment loans will need to furnish loan information to such a registered information system, and will also be required to obtain and review a consumer report from a registered information system, prior to making either a covered ability-to-repay loan or a conditionally exempt loan. The provisions of the Final Rule related to the registration of information systems will become effective 60 days after publication in the Federal Register, and the rest of the Final Rule will become effective 21 months after publication in the Federal Register.

Following the release of the CFPB's final rule, the OCC rescinded its Guidance on Supervisory Concerns and Expectations Regarding Deposit Advance Products, which addressed the OCC's expectations regarding the offering of deposit advance products. The OCC's Recission notes that its previous guidance overlaps with the CFPB's new rule, resulting in potentially inconsistent regulatory guidance for banks.

Less Regulatory Burden…What He Said!

In remarks presented at a recent conference for midsize bank risk officers, OCC's Acting Comptroller Keith Noreika had some optimistic words for banks feeling the weight of regulatory burden. Recalling the words of former Acting Comptroller John Walsh that a "healthy bank is a safe and sound one," Noreika said "that means banks must be able to function in ways that satisfy their intended purposes of lending and meeting the banking needs of the consumers, businesses, and communities they serve. We can't create a system so risk averse that we squeeze opportunity out of that system." Noreika discussed proposals to minimize regulatory inefficiency, "right-size" regulation, the Volcker rule, and the Dodd-Frank Act as regulatory fixes. The CFPB's final arbitration rule was mentioned too. Noreika pointed out that harmonizing other regulatory activity is also important. Often multiple regulators overlap in unhelpful ways, which can lead to confusion and conflicting regulatory guidance. Noreika suggested creating "…a system of regulatory "traffic signals" to better coordinate activity of multiple regulators at a particular institution." Yeah, what he he said!!

The Journey to Improved Payments

Kenyan photojournalist and activist Dan Eldon said, "The journey is the destination." For the past two years, the Federal Reserve and payment stakeholders have been paving the way toward an improved, safer and more streamlined U.S. Payment system. While significant steps have been taken and much progress has been made, the journey to implement safe, ubiquitous, real-time payments and create a safe, efficient, and resilient payment system is still underway.

The Federal Reserve recently released a paper that outlines the strategies and next steps the agency plans to follow, in collaboration with industry stakeholders and the Faster Payments Task Force, to reach the ultimate destination in the payments improvement journey. The paper outlines the Federal Reserve's next phase of work, including its plans to address Faster Payments Task Force recommendations and suggestions emanating from the Secure Payments Task Force.

A copy of the full paper is available for download at:
https://fedpaymentsimprovement.org/wp-content/uploads/next-step-payments-journey.pdf

Statistics, *Facts & Such*

■ U.S. consumers are ready to use a digital drivers license, with 80% having interest in a mobile driver's license app.
ATM Marketplace, *8/28/17*

■ Consumers (70%) report they would be interested in renewing their drivers license through their mobile phone.
Ibid.

■ The average credit card interchange fee today is about $1.00. Credit card interchange, which hit $33.8 billion at the end of last year, surpassed overdraft revenue ($33.3 billion) in 2016 for the first time.
CU Times, *9/29/17*

■ Nearly two-thirds (66.2%) of banks charge $30 or more per overdraft item, while 50.7% of credit unions charge less than $30.
Ibid.

■ While debit cards create 76% more volume than credit cards, credit card interchange fees are 250% greater.
Ibid.

■ Since the financial crisis, more than 10,000 branches have closed (3/day average). In the first half of 2017 alone, 869 brick-and-mortar locations shut their doors.
CU Times, *9/29/17*

■ The rate of spam hit 55% in September, (up from 54% the first half of the year).
Security Week, *10/6/17*

■ New variants of Locky ransomware contributed to the increase in spam rates, with six massive runs of the malicious malware detected during mid-September.
Ibid.

■ One in nine users had at least one malicious email sent to them during the first six months of 2017.
Ibid.

■ In July, phishing hit a 12-month peak at one in 1,968 emails. There were 2,644 phishing emails reported in September.
Ibid.

■ Malicious email attachments accounted for 74% of phishing emails in the first half of 2017.
Ibid.

Tech *Update*

Banks Must Face Increasing Third Party Cyber Risk

by Will Durkee, CISSP, ITPM

Amid the backdrop of September's Equifax, SEC and Deloitte breach revelations, the recognition that banks of all sizes need to address cyber risk grows. A key focus within that effort is the requirement to address third party cyber risk. Regulators such as the Federal Financial Institutions Examination Council (FFIEC) and the Office of the Comptroller of the Currency (OCC) are increasing demands on banks, including greater board oversight of outsourced relationships, hiring of information security officers, and proof that the large number of third party vendors now frequently involved in critical activities are being assessed, monitored, and managed.

More than half of companies have experienced a data breach involving a vendor but meanwhile the average number of third parties with access to confidential or sensitive information has increased by 25 percent, according to the Data Risk in the Third-Party Ecosystem survey released by Ponemon/Opus in September. With its largest segment of respondents from the financial services sector, fewer than half said managing outsourced relationship risks is a priority in their organization and 57 percent said they are not able to determine if vendors' safeguards and security policies are sufficient to prevent a data breach.

A Way to View Third Party Cyber Risk

The numbers demonstrate that as core business functions become decentralized and critical dependencies expand beyond the sphere of banks' control, they must posture themselves in a way that allows them to minimize both their susceptibility to and the impact of cyber threats.

Although the services and products of third parties fall outside of what an organization has direct control over, banks do have the ability and the responsibility to influence – to shape the security environment in a manner that protects their organization from risk. By identifying aspects of third parties' security posture that align with or are in conflict with a bank's security, they shift from viewing third parties as a potential vulnerability, to recognizing them as an active participant in the improvement of their security posture and lowering potential risk across the enterprise.

With competing priorities and limited resources, banks need help to assess vendor risk for compliance, score risk, and monitor vendors' performance. There are economical solutions in the marketplace that meet these needs in an efficient and scalable manner, mapped to the necessary standards and regulatory requirements. TSC Advantage is a risk management firm that can help you wade through these solutions and develop a comprehensive solution that is tailored to your needs.

Will Durkee, CISSP,ITPM, is the Director of Security Solutions at TSC Advantage, a cybersecurity assessment and consulting firm that provides cyber risk solutions to fortune 500 companies, federal agencies, and global insurance underwriters.

COMING *Up*

23rd Annual Bank Security Conference!

New Name! New Location!
Same premium conference dedicated to security personnel
Attend Live or via Remote Streaming
The Hyatt Regency Crystal City, Washington, DC, October 25-26, 2017
(optional Basic Security 101 workshop October 24)
There is Still Time to Register!! Get the agenda, all the details and register today!
@ www.bolconferences.com/bsc/

ASIS INTERNATIONAL

ASIS Assets Protection: Principles of Security (APC 1)
Orlando, FL, March 12-15, 2018
Info: (703) 519-6200
www.asisonline.org

ACAMS
Association of Certified Anti-Money Laundering Specialists

ACAMS 23rd AML & Financial Crime Conf
Hollywood, FL, April 9-11, 2018
info: www.acams.org

BOL CONFERENCES

BSA/AML TopGun Conference
Scottsdale, AZ, Feb 27-28, 2018
Info: (888) 229-8872 ext 87
www.bolconferences.com/topgun18/

TRAINING
PAGE

Safety & Security Coordinators – The Untapped Resource

by P.. Kevin Smith, CPP

The Bank Protection Act of 1968 requires annual robbery training, the Bank Secrecy Act has a training requirement for Suspicious Activity Reports, and there are several other regulations around customer privacy and Know Your Customer (KYC) that require (or suggest) some type of initial and/or periodic training. At the same time, the economy has the banking industry cutting costs wherever possible, which usually means cutbacks in support functions like Security, Compliance, HR, and Contingency Planning. While many believe the best way to prevent crime in the financial services industry is through a combination of systems and training, most organizations fail miserably when it comes to training because they typically lack the resources for a continuous education program. What are we to do when it comes to meeting the regulatory training requirements and keeping losses in check?

One solution we recommend is to establish a safety and security coordinator (SSC) program, which is designed to take advantage of existing resources to create and maintain a security conscious attitude among all staff members throughout the organization. Corporations have used this cascading communication model for years, which is an effective way to address these regulatory training challenges in a cost cutting environment.

Ambassadors for Security

The SSC program is really quite simple. One person from each branch, facility, or department throughout the organization is designated as the Safety & Security Coordinator, and they are charged with establishing and maintaining a security conscious attitude among all staff members in their respective areas. SSCs may be compensated in a variety of ways (a cash stipend, compensation time, annual gatherings, etc), but most companies simply reward these dedicated employees by acknowledging their efforts through the annual performance review process. More often than not, the employees are simply happy to be involved with a proactive role in making the office a safe place to work.

The SSC should have a dotted line relationship to someone in the Corporate Security Division, typically a Security Training Manager or the Chief Security Officer depending on the size of the organization, and it's important to keep the SSC informed about all security issues. If security is planning to add equipment at a branch, the branch SSC should be involved with the design, selection, and installation of the equipment to be installed. SSCs aren't expected to be familiar with the various security technologies, but they will offer valuable input from the end user's perspective. Perhaps more important, they are excellent resources when it comes time for equipment installation and maintenance. The important thing is to make them part of all security projects in their area of responsibility. It's the only way they will feel like a part of the security team.

Using communication tools, such as security alerts and a monthly security newsletter, the SSC will serve as a conduit to the front line staff on matters related to crime prevention, policy revisions, or customer and employee safety. Given proper instruction (and resources), these dedicated employees become excellent ambassadors for your security program, and they perform a valuable role that is widely accepted by examiners and internal auditors. Having the SSC hold a 15-20 minute gathering each month to discuss a security topic becomes a very powerful ritual, and when you have them submit a monthly certification for security training, you've created an excellent, auditable training program. The key is to centralize the message to be conveyed, and structure the information in a concise, meaningful, and, above all interesting format.

Bankers' Hotline is a Valuable SSC Resource

Most organizations employing the SSC concept rely on a newsletter to serve as the primary training resource and communication tool. The newsletter is very similar to the Bankers' Hotline publication. In fact, the editorial staff has structured the Hotline with the SSC concept in mind. Each issue contains the most up-to-date news on technology and security trends, a training page, statistics, and anecdotal stories, so security, compliance, and training managers can use this valuable information in their in-house training programs. When developing a bank or company newsletter, information from the Hotline can be incorporated as long as attribution is given to Bankers' Hotline with a disclaimer: "This article first appeared in Bankers' Hotline Newsletter, published by Bankers' Hotline Copyright © {insert year article was published} Bankers' Hotline."

We know of one financial services company who has mirrored the Bankers' Hotline publication, and modified their own monthly security newsletter to include examples of great work on the part of front line staff. This "kudos section" acknowledges security excellence on the part of staff members by listing their names, where they work, and a brief description of what they did to enhance the security program. The security director says, "Our employees love to see if they know someone in the kudos section. We move it and the cartoon around every issue, so readers will learn something as they search the pages". Another bank includes a security trivia question in its newsletter each month, where they award a company trinket to the winner.

The concept of an SSC program isn't new. Fire Wardens have been used in schools and corporations for years to ensure the orderly evacuation of buildings. And, communication trees have long been the staple of a good business resumption strategy and a means to convey weather emergencies. The challenge in the banking industry is to establish the program and maintain interest through the involvement of front line staff members. Regardless of the size of your organization, the SSC program is a simple, cost effective way of creating and maintaining a security conscious attitude among everyone in the company.

Thanks to Bankers' Hotline, you already have the monthly communication tool to make your program successful. And, we've made access to the Hotline easier than ever! Last year, we went all-digital to keep subscription rates low in light of rising printing and mailing costs. A priceless feature we offer is the ability for your additional staff members to have their own online access to the newsletter (at no additional charge) by simply registering using their bank email. We at Bankers' Hotline are here to help you achieve your security mission!

Global Cyber Guidance for FI

Cyber incidents are increasing in scale and sophistication. As part of their objective to improve the cyber resiliency within the financial sector, the Group of Seven (G7) – foreign and U.S. democracies – meet annually to discuss international security and other global matters. On October 16, in response to the exponential growth in emerging cyber threats and the vulnerabilities which they exploit, the G-7 Cyber Expert Group (CEG) published the "G-7 Fundamental Elements of Cybersecurity for the Financial Sector (G7FE)" to provide cyber security best practices within private entities, public authorities and the financial sector. The report outlines five "desirable outcomes" with respect to cyber security practices at financial institutions, as well as recommendations for promoting effective cyber security assessments. The guidance is designed to be tailored to different jurisdictions, and to firms of different sizes and levels of maturity. In a statement about the report, Treasury Secretary Steve Mnuchin noted that "a secure, safe, and strong financial sector is essential to promote real growth within the U.S. economy and across the world. Cybersecurity, particularly in the financial sector, is a top priority for the United States, and we are pleased to work with the members of the G-7 to advance a common approach that enhances resiliency." The G-7 Cyber Expert Group, established in 2015, is chaired by the Treasury Department and the Bank of England. Get a copy of the full report at https://www.treasury.gov/resource-center/international/g7-g20/Pages/g7.aspx

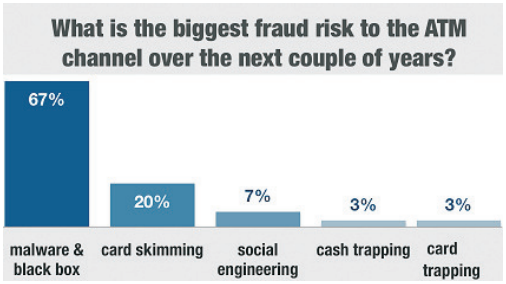
AI-Assisted Banking

In the beginning, computers spoke only computer language…today they not only speak human language, they perform helpful tasks, such as telling time, setting an alarm, playing music, and even requesting an Uber ride or ordering a pizza. Leading financial technology company NCR has upgraded its Digital Insight solutions with Amazon's Alexa cloud-based voice service to provide consumers with access to bank account information with simple voice commands. NCR is piloting the technology with banks and credit unions across the country to provide Alexa-assisted banking.

Focus *on Fraud*

Skimming, Malware, and Black Box – Oh, My!

With the same mindset as the infamous Willie Sutton who robbed banks because "that's where the money is," criminals are increasingly targeting ATMs for the lucrative cash payout - literally. Security firm Kaspersky Lab has discovered a new malware that is a bank's worst nightmare. Known as ATMii, the malicious malware deploys nefarious tactics to access ATMs remotely via the network or physically through USB ports to upload infected files coded to compromise the ATM and dispense cash to the criminals. A recent EAST ATM fraud risk survey found that malware and black box attacks are the biggest threats targeting ATMs, followed by card skimming, social engineering , and cash/card trapping. Oh, my!



ATM Marketplace, 10/6/2017

For today's security professionals, navigating ATM security and the evolving risk landscape can be just as a scary as walking through a dark forest. You never know what characters you might come across on your way! Follow the yellow brick road (live or via remote streaming) to the 2017 Bank Security Conference October 25-26, where Chris Carney, President of CJC Security & Risk Consulting Associates, will present a session during day one of the two-day conference on ATM Security and emerging ATM crime, recent trends and methods of attack, and how to confront these challenges.

Pink Collar Crime Awareness

During the month of October, women across the nation "Go Pink" for breast cancer awareness and many financial institutions participate in breast cancer fundraisers – a worthy cause! A risk that all financial institutions should be aware of and take steps to eradicate is Pink Collar crime. Last month, a former female credit union employee in western Pennsylvania pleaded guilty to stealing $180,000 from an upstate New York credit union that she managed for 20 years. Over a five-year period, the CU manager embezzled funds, made false business entries and altered financial statements to cover the thefts. Her actions and the losses incurred by the credit union led to the credit union's closure. The former employee faces up to 30 years in prison and a $1 million fine when she's sentenced in December. A recent Pew Research study revealed that nearly half (40%) of women are the primary breadwinners in their household. The additional pressures put on today's female workers can lead to an increase in embezzlement by women who are often employed in financial firms with access to funds, which may account for the stark increase in female embezzlement over the past ten years. On day 2 of the Bank Security Conference, renowned "pink collar" crime expert Kelly Paxton, CFE, will provide tips on identifying "pink flags" that are common among female embezzlers to help spot what could be a pink collar criminal within your institution.

Early Fraud Detection Tools

With card fraud all the craze in criminal circles and a growing challenge for card issuers, early detection is the key to mitigating the risks and losses when physical cards or card data is stolen. Global payments provider Mastercard has launched an Early Detection System that alerts card issuers when cards or accounts are exposed to data breaches or security incidents. Financial institutions who offer customers the My Mobile Money app can now offer mobile fraud protection for their debit cardholders. Ondot Systems and Elan Financial Services have added real-time fraud alerts to the My Mobile Money app for early fraud detection.

From the Editor

A Passion for Hiring Protocol

by P. Kevin Smith, CPP

People often ask me, "Why do you get so worked up about workplace ethics and background investigations?" Well the simple answer is that I believe the greatest threat to any organization is the enemy within. If you let a crook get through your door and you fail to establish a workplace ethics program, it's not a question of will they do something nefarious, it's simply a matter of when. I've had some rather interesting debates on this topic with Human Resource (HR) professionals, Information Technology folks, Auditors, Lawyers, and Compliance Officers, but the latter three don't count because they are typically only worried about checking a box on the next exam form. More often than not, they all fail to recognize or acknowledge the risks of hiring a dishonest employee…until it's too late.

HR professionals think that outsourcing the background investigation (BI) process is "good enough" because they insist on criminal record checks. The reality is that investigations conducted by most third party BI firms are fraught with holes and oversights because they simply don't have any skin in the game. In a recent Security Management article, Sandra Stibbords, owner and President of Camelot Investigations notes that vetting potential employees and conducting background checks is where many private companies go wrong. According to Stibbords, most companies outsource the BI process to a third party agency who claims to do a national criminal search, when really they are simply running a name through a database that has access to on-line court records. There is little information about which state, county, and local governments actually have their criminal records on-line, but I'd be willing to bet the number is south of 50%. Furthermore, if history is any indicator, those that do have records on-line are behind in their data entry by 6 months to a year. I agree with Stibbords when she says, "To really be aware of the people that you're getting and the problem with the human element, you need to have somebody who specializes in solid investigative research and you need to invest money in doing proper background checks."

Technology folks think that internal theft may be prevented through solid system architecture. They claim they can keep unauthorized personnel out of any system, but I disagree. You can build a nice mouse-trap to help identify a thief, but that is usually after the fact. I chuckle when information security folks tell me that a secure system infrastructure will prevent unauthorized access to customer information. Heck, 90% of bank employees have legitimate access to customer information. It's their job!!! Look up the account to see what we can sell them next. I settled that argument with one information security "expert", when I asked him to join me on a physical security penetration test one evening. We walked into the company's operations center at around 10:00 pm, and the first office area we entered had stacks and stacks of computer printouts filled with customer names, birthdates, addresses, social security numbers, and account numbers on top of the filing cabinets. Sure the printouts were behind a locked building door and locked office door, but a cleaning lady had to move them to dust the tops of the cabinets. The information security expert said with a chuckle, "well at least the cleaning lady couldn't get into my system."

In the same article, Chris Inglis, former deputy director and senior civilian leader of the NSA during the Edward Snowden leaks, addressed the importance of creating an ethical culture. As a contractor, Snowden was treated as a commodity, and he never attended the typical new employee orientation program. He was expected to report for duty on day one and get to work immediately. So on Snowden's first day he was not taken to the NSA museum like other employees and told about the meaning of the oath that new employees take. Instead, according to Inglis, "contractors were expected to sit down, shut up, and color within the lines".

While some internal theft cases are crimes of opportunity, most of the dishonest employees I've encountered over the years (and there have been hundreds), had a checkered past that was never discovered during the hiring process. Make no mistake, a thorough background investigation and a mandatory workplace ethics program are your greatest defenses against internal theft. If you are not passionate about that concept and you fail to sell it to senior management, you should keep your resume current.

WAR *Stories*

Can I Catch a Ride… Officer?

Sometimes the story writes itself…and the crime solves itself. Tristan Paul Mitchell, 28, walked into The Columbia Bank in Hagerstown, MD, wearing all black, demanding money placed in a black bag he carried, and fled the bank on foot. Apparently he forgot to bring a getaway vehicle, so he flagged down a car driving by. When Mitchell spotted the driver of the unmarked vehicle wearing a raid vest with "sheriff" on it, he attempted to flee. The deputy apprehended Mitchell, who had the exact amount of cash stolen from the bank on him. The ride to his next destination was pre-arranged.

It's Not Me

Bank robbers aren't the only ones who are a few fries short of a Happy Meal. A fast food restaurant in East Baton Rouge, LA was robbed at gunpoint by a man wearing all black with a black ski mask covering his face. When the suspect held a gun to one of the victims and demanded money, they recognized Cleveland Willis by his voice and facial features that were visible through the holes in the mask. When one of the workers said, "Cleveland, is that you?" the suspect replied "No, it's not me." Turns out, Willis was a former employee at the restaurant, and fled in the same silver Nissan Altima he drove when he worked there. With that easy ID, police arrested Willis and charged him with armed robbery.

Should Pick an Older Car

Car dealers have begun using GPS devices to keep track of cars they finance if the buyer defaults on payments. Lucky for the police, not so much for thieves. Brothers Evan Housley and Aaron Housley held up three banks in the Indianapolis area, wearing disguises and carrying high-powered weapons. In one of their heists, they drove a 2017 Nissan Murano. Armed with a partial license plate number, FBI discovered the car was stolen from a local dealer. The Murano is equipped with a GPS mapping device that allows remote "pinging" of the car. - a handy feature that led FBI agents to the car, with both suspects inside – along with two AR-15 rifles, a tactical vest, latex gloves and a handkerchief. The brothers were arrested and one confessed to the robberies. Police won't need to track down the other one.

QUESTIONS & *Answers*

Q. What are industry thoughts on banks changing domains from .com to .bank? With all of the listed benefits, it would seem that financial institutions would be wanting to transition sooner rather than later. Also, other than to prevent fraudsters from being able to register an illegitimate .com web address for spoofing purposes, what are the added benefits for a community bank?

A. We consulted with two of our expert board of advisors regarding .bank domains. Following is their feedback.

The Pros for .bank domains are: Better security comes to the top of the list. Applicants for .bank gTLD (general top level domain) urls will be vetted by a financial industry consortium, fTLD Registry Services, which includes the ABA. Applicants will have to prove their eligibility, conform to a strict name selection policy, and implement security requirements intended to make it harder for crooks to scam consumers with fake websites. There's also recertification every two years. Theoretically at least, "branding" should be more intuitive.

There are cons for going with a .bank domain. It could be a challenge to come up with the ideal address, given the strict parameters and the huge numbers of similarly-named institutions (how many First National Banks or First Banks do you suppose there are?) The process of approval won't be as speedy as applying for a .com address.

There will be costs of transitioning from your old name to your new one. These include education of account holders and updating all your company letterhead variations, email addresses (and signature blocks, in come cases), digging though all your print material to see where you've used the old url (and reprinting those materials, updating print and broadcast advertising. The track record for earlier attempts to create "vanity" TLDs is mixed. How many times have you seen the extensions .aero, .tel or .biz lately?

Thanks to John S. Burnett, Executive Editor, BankersOnline.com, for his response

The ".bank" internet address has been around several years now and while many banks secured a new address, the more common ".com" is still the go-to internet address. I do know some banks are actively using the ".bank" address but I've yet to see it advertised by any in my market or on TV. If a bank wanted to use the address, I would believe to make it cost effective the bank should promote it continuously and tout the security aspects of the address in the wake of Equifax, malware attacks and other data breaches. It's a little more security but it doesn't provide any guarantees. If the bank is all about apps on a smartphone, the branding of ".bank" may not provide the full benefits as ".com" is better for an advertisement to get a person to your website, and then sell them on the convenience and security of the internet banking phone app. At the end of the day, if the money is spent the bank should use and promote it.

Thanks to Andy Zavoina CRCM, BankersOnline.com, for his response.

Q. With regard to Reg. E's reference to "Opt-in" and "Opt-out" for an "overdraft service," is this tied into the same distinction between an Overdraft Protect Program (ODP) and ad-hoc payments? When a customer opts-in or opts out under 12 CFR 1005.17, is that always in connection with an ODP, or does it cover any transaction where a bank covers a negative balance and charges a fee for processing a ATM withdrawal or a one-time debit card transaction? When a customer opts-out by indication on the Reg. E disclosure, does that prohibit a bank from assessing a fee when an ad-hoc overdraft decision is made or does the bank consult with a borrower to help make a decision on how they want to treat such transactions?

A. The Reg E opt-in requirement provides that a bank cannot charge a consumer account for an overdraft triggered by an ATM or one-time debit card transaction unless the bank:

(1) has an automated overdraft program that could permit the consumer to overdraw the account with an ATM or one-time debit card transaction;
(2) makes a disclosure concerning its overdraft program as required by section 1005.17;
(3) gives the consumer an opportunity to opt-in to coverage of ATM and one-time debit card transactions;
(4) receives such an opt-in from the consumer; and
(5) confirms the consumer's opt-in and reminds the consumer that the opt-in can be revoked by the consumer at any time. Because of the nature of ATM and debit card transactions, an ad hoc OD program would not provide overdraft service for ATM and one-time debit card transactions.

Thanks to John S. Burnett, Executive Editor, BankersOnline.com

Q. We are familiar with ATM skimming and physical attacks targeting ATMs. What are network-based ATM attacks and how can we mitigate this type of ATM fraud?

A. Bandits have held up bank branches and launched physical attacks at ATMs longer than most of us have worked in the banking industry. Banks and ATMs remain high-value targets for fraudsters. What has changed with the times is the MO used by today's crafty criminals and their ability to steal cash without physical access to the bank or an ATM. The European Union Agency for Law Enforcement (Europol) and security firm Trend Micro recently issued a joint report alerting banks to a rise in ATM attacks that infiltrate bank networks to infect ATMs and dispense cash to money mules standing by ready to collect the ill-gotten gains. The report recommends that financial institutions take more stringent steps to secure their ATM networks by deploying multiplying security layers. Like any other network, ATM networks must be closely monitored for suspicious activity and unauthorized access. To help mitigate network-based attacks, banks should update operating systems, and ensure that ATMs are programmed not to reboot from external media, such as a CD or USB, install firewalls AVsoftware, and intrustion detection programs

WHAT DO *other* BANKERS *do?*

Going Pink for Cancer

October is breast cancer awareness month – a disease that hits home for many families, communities, and even impacts the workplace. **Financial Plus Credit Union** in Flint, MI has a personal stake in raising funds to help local patients battling breast cancer. The CU began participating in Hurley Medical Center's Breast Cancer Patient Navigator Program after one of their own began fighting breast cancer. In 2016, the CU joined forces with Hurley Medical Center on an annual "Pink Night Palooza" event. Since 2007, nearly $370,000 has been raised for breast cancer patients through more than 100 events and sponsorships, including the original Pink Night and an annual Pink Night Palooza fundraiser.

Stepped Up to the Plate

A total of sixteen teams with players from local businesses across Franklin, NH stepped up to the plate and participated in **Franklin Savings Ban**k's 24th annual charity softball tournament in September. This year's event raised over $6,000 that will go to local D.A.R.E ., and other youth drug prevention programs. D.A.R.E. is a comprehensive K-12 education program that is taught in classrooms across America and in 52 countries. The program focuses on drugs, violence, bullying, internet safety, and other high risk circumstances affecting our youth. Since 1997, the FSB annual Charity Softball Tournament has raised over $79,000 for countless charities throughout the Central Lakes Region.

Educational Support for Vets

In partnership with a local nonprofit, **Citizens Community Bank** in Idaho is helping its residents and veterans further their education. The POW*MIA Awareness Rally Corp is a non¬profit organization dedicated to the public awareness and financial support of POW*MIA and other veteran issues. The bank is matching opening deposits for checking accounts Oct 23-27, and establishing two scholarships for veterans in need. Working with representatives from veterans groups throughout Southeast Idaho, the bank will donate up to $2,500 at Idaho State University and up to $2,500 at the College of Eastern Idaho to provide support for their programs and Veterans education needs.

Wildfire Relief Funds

Residents in California and surrounding regions can help those who have been affected by the raging wildfires. **Savings Bank** Mendocino County is accepting monetary donations on behalf of local nonprofits. Donations for the Mendocino County Disaster Fund can be made payable to the Community Foundation. For those in Lake County, payments can be made to North Coast Opportunities, with "Lake County fire relief" in the check memo. Contributions can be dropped off at the bank or mailed to Savings Bank, P.O. Box 3600, Ukiah, CA 95482. The MTN Montana Wildfire Relief Fund has raised over $450,000 from local nonprofits and other contributions to help those affected by the region's devastating wildfires.

AND IN *Conclusion*

"That was someone from tech support offering to fix a computer problem that I was not even aware I had!"

BANKERS' Hotline

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.

BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVII NUMBER 7

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.

This issue went to press on July 20, 2017

Robbery Response: Follow the Money

by Teri Wesley

Back in the days of John Dillinger and Slick Willie Sutton, ruthless bank robbers would burst into a bank, force a manager to open the vault, and flee with sacks full of loot (lots of it!) amidst gun battles with local authorities. As times changed and bank security evolved, many thieves have resorted to verbal or written demands at the teller window, escaping with less cash (in many cases), and often getting away with it. In today's high-tech world, robbing banks may sound a little old-fashioned, but it remains a present-day threat that continues to take a toll on financial institutions and communities across the nation. The FBI has had a primary role in bank robbery investigations since 1934 when it became a federal crime to rob any national bank or state member bank of the Federal Reserve. Through their Bank Crime Statistics (BCS) reporting, they provide a nationwide view of bank robbery crimes based on statistics contributed by FBI field offices responding to bank robberies or data provided to the FBI from local and state law enforcement.(NOTE: Since not all bank robberies are reported to the FBI, the actual numbers involving bank robberies in the U.S. is actually higher.)

On July 5, the FBI released the 2016 Bank Crime Statistics Report for January 1 – December 31, 2016. There were 4,185 bank robberies committed last year, 65 burglaries and 1 larceny, involving 4,900 perpetrators (336 of which were female suspects – a growing trend). That means, on average, more than 348 bank robberies take place every month, nearly 10 incidents per day on average. The highest number of robberies took place on a Friday (913) and the most popular time of day for robberies committed last year was 9am-11am (1004). The types of institutions hit most often were branch offices (3.978), financial institutions located in commercial districts (2,725) and those in Metropolitan areas (1.997). Acts of violence were committed during 146 of the total incidents last year. These acts included 43 that involved the discharge of firearms, 72 instances involving assaults, and 31 hostage-related instances – during which there were 43 injuries, 8 deaths, and 59 persons taken hostage. While demand notes were the most often used modus operandi in last year's robberies, in 2,361 (more than half) of the robberies, the threat of some type of weapon was made. Firearms have historically been the weapon of choice for bank robbers, but an alarming trend that is on the rise is the use (or threat of) explosive devices, with 110 recorded incidents involving the threat of explosives last year.

(continued on next page)

OCC Fintech Guidance

by Teri Wesley

Financial institutions are increasingly turning to fintech providers to meet consumers' growing demands for digital products and services. To provide guidance for regulated entities and address due diligence concerns when partnering with third-party providers, the OCC has issued a supplement to its "*Third-Party Relationships: Risk Management Guidance*." The OCC notes that if a fintech company performs services or delivers products on behalf of a bank or banks, the relationship meets the definition of a third-party relationship and should therefore be included in bank's third-party risk management process. The supplement addresses frequently asked questions concerning these third-party relationships and risk management practices related to fintech firms as well as other non-bank vendors.

Bank Robbery: Follow the Money
(continued from front page)

On a positive note, bank robberies have declined (down from more than 7,500 incidents in 2004 to less than 4,000 in 2014). One contributing factor in the decrease could be sophisticated security measures banks have put in place to deter criminals, such as alarms, locks, vaults, CCTV, and bullet-resistant glass . These methods will deter some thieves, but others are willing to take the risks for the high payout they expect to get. As the growing trend toward the threat of explosive devices continues, these methods become less effective.

To date, 2,537 of the 4,900 persons involved in last year's incidents have been identified. That's over 2,300 who are still out there! Security vendor 3SI Security Systems recommends tracking devices to catch and put these criminals behind bars, and recover the bank's losses. According to 3SI, the national average for recovering stolen cash is less than 15%, but banks that use their tracking systems average over 70% recovery. In May, 3SI's GPS Tracking solutions helped arrest at least 82 criminals and recover over $665K in stolen cash and assets. In just one example, the use of a 3SI Cash Tracker™ led to the arrest of a robber in Portsmouth, VA and the recovery of $35,000. When a lone suspect entered a bank and demanded cash from the teller, a Brinks employee, who was in the bank at the time, knew that the Portsmouth Police and Comm Center phone systems were down. He flagged down and alerted a police officer who in turn notified 3SI. 3SI's Tracking Support Center immediately communicated the tracking information to the Virginia Beach Police Department, who contacted the Portsmouth Police. The suspect was subsequently taken into custody and all of the bank's money was recovered.

Join us in Washington, D.C. in October for the 23rd annual Bank Security Conference where you can meet and talk with 3SI Security System reps, and get more information about their tracking devices. You can also hear firsthand from a former career criminal who will provide insight into the mind of a bank robber. You'll also hear from the security director of a bank that experienced a traumatic kidnaping incident. She will share details of the kidnaping, internal notification and response, law enforcement investigation, and the impact on employees and bank operations. Check out all the details for this year's event and register before the Early Bird deadline for additional savings at www.bolconferences.com/bsc

IN THE *News*

Banks Subject to Discrimination Lawsuits From Cities

Banks who willfully target minority communities with predatory lending practices that result in foreclosures and vacancies, and ultimately lead to reduced property values and diminished property tax revenue, may face lawsuits from cities adversely affected. The Fair Housing Act (FHA) protects people from discrimination when they are renting, buying, or securing financing for any housing. The prohibitions specifically cover discrimination because of race, color, national origin, religion, sex, disability and the presence of children. The FHA allows any "aggrieved person" to file a civil action seeking damages for a violation of the statute.

Following federal lawsuits that the City of Miami brought against two of the nation's biggest banks, the Supreme Court ruled that cities can sue banks under the federal anti-discrimination in housing law. The city alleged that Bank of America and Wells Fargo intentionally targeted predatory practices at minorities with excessively high interest rates, unjustified fees, teaser low-rate loans that overstated refinancing opportunities, large prepayment penalties and unjustified refusals to refinance or modify loans in the face of default. The city asserted that the banks' actions led to a disproportionate number of foreclosures and vacancies in minority neighborhoods and hindered the city's efforts to create integrated, stable neighborhoods, reduced property values and diminished the city's property tax revenue while increasing demand for municipal services.

The Court held that a city qualifies as an "aggrieved person" under the FHA and that cities may assert claims under the FHA against banks that are engaging in unlawful discriminatory lending practices. The Court concluded that such alleged damages are within the "zone of interests" designed to be protected by the FHA, and the city had the right to assert its claims. The Court also concluded that although the alleged damaging consequences of the banks' alleged discriminatory lending practices were foreseeable, that, alone, was insufficient for the city to establish proximate cause under the FHA, as required. The case was remanded to the trial court for that court to establish the parameters for sufficiently demonstrating proximate cause.

FINRA's Fintech Initiative

With the proliferation of fintech and banks partnering with fintech providers to remain competitive, the Financial Industry Regulatory Authority (FINRA) has launched an Innovation Outreach Initiative in an effort to better understand how the latest fintech innovations impact the financial industry and to track fintech developments. FINRA's new Office of Emerging Regulatory Issues will be responsible for carrying out the initiative. Part of the agency's initiative includes a website with resources to help financial professionals understand emerging fintech areas, such as distributed ledger and other digital technologies. Other initiative goals include:

- Creating a Fintech Industry Committee to facilitate discussion on fintech developments and how FINRA's rules and programs interact with technology innovations.
- Conducting regional roundtables to provide a forum for market participants (including FINRA members and nonmembers) to discuss fintech topics.
- Developing timely publications on fintech topics, such as the increased adoption of regulatory technology applications.
- Enhancing existing internal processes to effectively communicate with the industry.
- Increasing collaboration with other regulators, in the U.S., and other countries.

Disaster Recovery Season

Summer heat waves and stormy weather are impacting regions across the country. Tornadoes, hurricanes, and other weather-related events can wreak havoc on your bank's operations and cause a great deal of stress for your staff and customers. The July issue of BOL's free Security Spotlight provided tips to prepare your institution for these and other catastrophic events: having a specific designated meeting place for staff, keeping non-perishable food and supplies stocked in your branches, and more The Federal Reserve Board has an Ops Stop site with helpful operational resources, including business continuity tips and resources, including a National Business Continuity Guide, and the FRB's operational status as well as other important notifications. The best time to review your disaster recovery plans and share those plans with your staff is now – before a major event impacts your operations.

Statistics, *Facts* & Such

■ Credit union membership is on the rise. At the end of the first quarter this year, credit unions had 109.6 million members, up from 105 million a year ago.
Credit Union Times, *5/25/17*

■ About 1.4 million members joined credit unions in the first three months of 2017, the largest quarterly gain on record, with 592,000 new members joining in March alone.
Ibid.

■ A survey of 8,000 millennials in December found both older millennials (age 26-36) and Gen Xers (age 37-51) in the U.S., U.K., Germany and other countries are more likely to use regional banks as their primary financial institutions.
Credit Union Times, *6/1/17*

■ Older Millennials and Gen Xers conduct about 75% of their banking activities online or via mobile.
Ibid.

■ About two-thirds of senior millennials and about half of Gen Xers are planning at least one major life event in the next two or three years that will have a financial impact.
Ibid.

■ Primary reasons for choosing financial providers included simplicity, digital payments and mobile payments.
Ibid.

■ By the end of 2016, the number of EMV payment cards in global circulation increased 1.3 billion year over year to a new total of 6.1 billion.
ATM Marketplace, *6/5/17*

■ More than 52% of all card-present transactions conducted globally between January and December 2016 used EMV chip technology, up from 35.8%t for the same period in 2015.
Ibid.

■ The EMV chip card adoption rate for the U.S. Is at 52.2% (up from 26.4%); Europe Zone 1 chip card adoption is 84.9% (up from 84.3%), Europe Zone 2 63.7%, up from 52.3%. Canada chip card adoption is 75.7% (up from 71.7%)
Ibid.

Tech *Update*

Authentication Changes on The Horizon

In a recent white paper, Vasco, a leader in the field of transaction authentication, claims that online banking, ACH transactions, ATMs, branch services, mobile banking applications, customer communication and bank operations can all be made more convenient, more accessible and more secure through the innovative use of strong authentication technology. Strong authentication in its traditional way has developed into a standard procedure for online banking applications and has become, well...kind of boring. Tokens, key fobs, mobile tokens, SMS codes, phone calls certainly do their job to confirm a customer's identity and combat cyber-attacks. But now is the time for a "strong authentication overhaul". While the cryptography of many such solutions has been available for years, the actual application methods were far from convenient. However, the outlook has changed quite a bit with the expansion of consumer-friendly tools such as mobile smartphones, Bluetooth and Quick Response Code technology. To illustrate how this one-time dream is approaching reality, Vasco experts point to ATM transactions.

ATMs lose $8 billion a year to skimming fraud, according to the U.S. Secret Service. The introduction of EMV Chips and constant security improvements still leave a security gap. The biggest problem is that the ATM card PIN never changes. The demands of mobile-minded consumers play a role too as mobile phones become more valuable possessions than wallets. "Scan QR or Tap Your Phone to Get Cash." VASCO security experts suggest that a card-less ATM is not a dream. Here too, mobile phones could be used to make ATM transactions more secure and more convenient. Instead of the traditional use of a bank card and PIN to validate a transaction, ATM customers would use their phones to either scan a quick response (QR) code or tap and transmit using built-in NFC technology. In both cases, encrypted information would be read off the ATM and then verified by the mobile phone user to initiate the transaction. Even an intercepted and copied QR code will not present a fraud risk as it is only valid for one transaction for a specific user.

Last year a study conducted by IOActive Labs has found that 90% of mobile banking apps from top banks have serious security vulnerabilities that could potentially compromise sensitive user data. To minimize those risks, most banks simply restrict functionality to minimize the risk. That does not make customers happy. Vasco urges financial institutions to stop and take a fresh look at how strong authentication can serve banks in areas they never thought of using it. For a copy of the complete Vasco white paper, visit their website at https://www.vasco.com/images.

COMING *Up*

23rd Annual Bank Security Conference!
New Name! New Location!
Same premium conference dedicated to bank security personnel
Attend Live or via Remote Streaming
The Hyatt Regency Crystal City, Washington, DC, October 25-26, 2017
(optional Basic Security 101 workshop October 24)
Get the agenda, all the details and register by 9/30 for Early Bird Specials!
@ www.bolconferences.com/bsc/ !

ASIS INTERNATIONAL

Security Risks and Mitigation Strategies for Financial Institutions
Dallas, TX, Sept 24, 2017
ASIS International 63rd Annual Seminar and Exhibits
Dallas, TX, Sept 25-28, 2017
Info: (703) 519-6200
www.asisonline.org

ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)

ACAMS 16th Annual AML & Financial Crime Conference
Las Vegas, NV, Sept 25-27, 2017
ACAMS 23rd AML & Financial Crime Conf
Hollywood, FL, April 9-11, 2018
info: www.acams.org

TRAINING
PAGE

Social Media and Background Checks

by P. Kevin Smith, CPP

In today's world, the importance of a solid background check cannot be overstated. I learned the importance of a thorough background investigation many years ago when I received a call from a supervisor at a satellite operations center. The supervisor stated that the FBI was on-site, asking to see the workstation of a 4-year employee (let's call him Billy Jones) who had abandoned his job just a few days before the FBI visit. I asked to speak with the agent, and explained that we were happy to cooperate, but unfortunately the work station had been cleaned out because Mr. Jones had abandoned his job just a few days ago. The FBI agent explained that Jones hadn't abandoned his job. Instead, he had been picked up by the FBI three days ago on his way to work, and charged with running a major identity theft ring. He said Billy Jones was really another person who had stolen Jones' identity five years ago. In other words, we had an identity thief in our employ, operating under an assumed name for over four years. Imagine our embarrassment and the fallout from this identity thief, who had access to customer records.

According to a recent publication on backgroundchecks.com, background checks are needed to help keep your clients, your employees and your business safe. Lack of background checks, or poorly done background checks, can lead to horrific crimes. The sad fact is that people rape, people murder, people steal. You don't want anyone to experience that, but you have a responsibility to protect your clients and your employees. Protection of your employees is imperative in any business. A 2005 survey found that 2.3% of all businesses experience some form of co-worker violence, ranging from .6% to 8.1% for businesses with up to 250 employees and up to 34.1% for businesses with 1000+ total employees. In addition, a 2006 survey discovered that 13% of all workplace fatalities were caused by assaults and violent acts. This includes homicides, which accounted for 9% of all workplace fatalities.

Another very important factor is the protection of your customers. In an article appearing on bnet.com, the Journal of Business and Entrepreneurship, the author cited a case in which an unnamed company hired Jesse Rogers as a home healthcare aide without running a background check. Rogers, who had a number of larceny convictions, killed the 32-year-old quadriplegic and 77-year-old woman he was supposed to be caring for in an attempt to cover up additional thefts.

The big debate in the worlds of security and human resources is, "How much is enough?" While HR practitioners are typically satisfied with verification of education, prior employment, and (in most cases) criminal history, security practitioners want to know anything and everything you can possibly get your hands on. Unfortunately, the latter can get you in trouble, if the inquiries are not handled properly. In this regard, social media should be treated as "recruiting minefield".

A recent publication in CareerBuilder indicates that 60 percent of employers used social media to research job candidates in 2016, a 500 percent increase since 2006. The same survey found that of the 59 percent of hiring managers who used search engines to research candidates, nearly half discovered information that negatively impacted the candidate, including provocative or inappropriate photographs or videos (46 percent), information about candidate drinking or using drugs (43 percent), and discriminatory comments related to race, religion and gender (33 percent).

Financial Institutions would be wise to codify their social media use policies, including the manner in which social media may be used in the recruiting and hiring process. By having the proper policies and procedures established in regards to social media interactions, it helps prevent legal risks.

There is no doubt that social media will be used in the investigative process, but here again, a written policy will reduce the risks associated with this practice. Policies should include the following basic principles.

- Inform candidates of your social media searching policy. Some of the information that is found on social media sites may not be reliable, so make sure to inform the candidate of your social search practice and confirm that their profile and data is indeed authentic.
- Any social media investigation should be restricted to publicly available information. Employers shouldn't demand an applicant's passwords for social media accounts. This is specifically prohibited in many states, and employer requests for such information also could violate the Stored Communications Act in all 50 states. Never attempt to force, persuade or coerce a candidate to provide access to their social media site. Accessing the candidates social private data should not be required as part of their application.
- Social media background investigations should be restricted to those who know how to use the information. Hiring managers and future supervisors shouldn't be involved in any social-media-driven screening processes. Instead, the social media background investigation should be left to trained individuals in the HR Department or Security Division within an organization. If those resources are limited, a third party background investigation firm may be considered. Social media background check vendors insulate internal managers from liability. They will truncate protected class information and only show focused information that an employer chooses and is job-related. Hiring managers should not be privy to social media investigations.
- Verify the accuracy of information obtained from internet screening media.
- Document the findings of your investigation. For now, the courts have ruled that employers are entitled to disqualify applicants exhibiting dangerous, harassing or illegal conduct on their public social media sites. Employers should document and store such information, however, in case an applicant later asserts discrimination.

The definition of "social media screening" is open to interpretation. But given the regulatory climate and trends, 2017 will be the year in which smart organizations with active risk management strategies get proactive. We can expect to see more developments on formal policies for executing searches, who is responsible for conducting them, and how the information will be reviewed.

Latest ATM Fraud Update

The European ATM Security Team (EAST) released its second Fraud Update for 2017. Of the 21 SEPA (Single Euro Payments Area) countries and 5 non-SEPA countries reporting, ten countries experienced payment fraud issues. Fifteen countries reported ATM malware and logical security attacks. Two of the 15 countries reported ATM malware and 14 reported the use of black box devices (5 of those for the first time). Nineteen countries reported skimming at ATMs. The use of M3 category (card reader internal skimming) devices that are placed inside the motorized card reader, behind the shutter, continues to spread, with nine countries reporting this type of attack. International skimming-related losses were reported in 49 countries and territories outside of SEPA and in 9 countries within SEPA. The top three locations for such losses were the U.S., Indonesia and the Philippines.

Ram raids and ATM burglaries were each reported by nine countries. Most alarming is that six countries reported the use of solid explosives in attacks. The increase in these attacks is of growing concern to the industry due to the risk it poses to life and the significant amount of collateral damage to equipment and buildings.

Same Day Updates and Testing

The Federal Reserve Banks (FRB) have announced new updates to their Same Day ACH resource center. New information posted to the resource center includes a schedule for Phase 2 of Same Day testing that will be conducted in four waves during June, July, August and September. Those falling in the first and second waves should have already received detailed instructions via email from the FRB. The resource center also posted an update from the FRB Atlanta Same Day ACH Readiness Forum (Phase 2) conducted on May 17, 2017. The agenda (pdf format) and presentation slides from NACHA® and Federal Reserve Financial Services presenters are available for viewing. The FRB encourages banks to review the Same Day FAQs and to visit the resource center regularly for updates.

Focus *on Fraud*

Cyber Response Exercise

In Marvel Comics' most popular superhero series, Spider-Man, Peter Parker's character has evolved exponentially since the first movie was released in 2002, wherein "Uncle Ben" cautioned the webbed superhero that "with great power comes great responsibility." Technology and the Internet have empowered the financial industry and other sectors to branch out and provide services on a global scale. But it has also provided criminals the same tools to use for nefarious gain. As fraud and cyber attacks become the norm rather than the exception, financial institutions have an inherent responsibility to take effective measures to mitigate these threats and defend their networks. The Financial Services – Information Sharing and Analysis Center (FS-ISAC) is providing its members and regulated financial institutions an opportunity to practice their processes, plans and resources in response to a simulated attack. The FS-ISAC's seventh annual Cyber-Attack Against Payment Systems (CAPS) is a virtual two-day tabletop exercise that simulates an attack for participants to practice – or even challenge – their institution's response plan. The exercise, open to all FS-ISAC members and regulated financial institutions, is free. Two identical sessions for North American banks are available on September 12-13, 2017, and September 19-20, 2017. The exercise only takes about two hours each day. Get more information and register for the CAPS exercise at www.fsisac.com

No Fraud Too Finite to Report

With the increased popularity of the Internet and online auction sites, such as eBay, check scams are on the rise. Forged cashier checks are often sent to online sellers, whose bank doesn't discover that the document is counterfeit (which could take weeks in some cases) until after the seller has sent the item off to the buyer. Another popular scam occurs when an individual sends an email to another about a check he wants the recipient to deposit. The person who sends the email says that, in exchange, all the recipient has to do is transfer funds to the sender from her own account. The document the recipient gets from the scammer can look very real, but is worthless.

To help banks mitigate these losses, the FRB issued a reminder to its bank customers on June 15 on the importance of reporting fraudulent check activity to law enforcement, regardless of the dollar amount. While law enforcement agencies may not pursue every single report of check fraud, smaller value items may be part of a larger fraud scheme and, in aggregate, can amount to values that law enforcement agencies will find to be of interest. When reporting to the law enforcement agency in the jurisdiction where the fraudulent check was negotiated, financial institutions may want to confirm whether that agency will pass the information along to the Federal Bureau of Investigation (FBI) or whether the institution should assume that responsibility. Reporting fraudulent check activity to local law enforcement does not negate any applicable Suspicious Activity Report (SAR) filing requirement under FinCEN regulations.

Remind your customers that to avoid check fraud scams they should never cash checks from individuals, banks or businesses they don't know. If they know the issuing bank, they still should verify that the address and other contact information on the check are correct before cashing or depositing it.

Mortgage Closing Scams Heating Up

The temperatures outside are rising and the housing market is heating up. That's good news for banks and lenders. The bad news is that mortgage closing scams are sprouting up along with those home sales. Scammers are hacking the email accounts of real estate agents and consumers to discover closing dates of upcoming home sales. Then they send an email to the buyer posing as a real estate agent or a title company. The email instructs the buyer that their closing costs will have to be wire transferred instead of being brought to the closing, and provides an account for the wire to be sent that is controlled by the fraudsters. Once the scammers' victim takes the bait and sends the money, it's often too late…their account is cleaned out. In response to this alarming trend, the Consumer Financial Protection Bureau issued an alert for banks to warn consumers about these mortgage closing scams, particularly when closing dates are approaching. The alert includes a link to tips provided by the FTC, FinCEN and the FBI, and advice on how to avoid email phishing schemes.

From the Editor

Look Me in the Eye

by P. Kevin Smith, CPP

It's a well-known fact that body language is a key indicator during the interview or interrogation process, and some of the best investigators will tell you that the eyes are the most expressive area of a person's entire body. Truthful people generally look at the interviewer when they are answering a question. Deceptive people will generally break eye contact at the instance of the answer. If there is a #1 rule in the interpretation of non-verbal human behavior, it is to look for breaks in eye contact. Perhaps William Shakespeare said it best…. "The eyes are the windows to the soul."

Looking someone in the eye is also a powerful persuasive technique. Research shows, for example, that motorists are more likely to stop for a hitchhiker who looks them in the eye than one who looks away. Eye contact appears to make pedestrians more likely to take a brochure and allow people asking for money to collect more cash more easily. In short, if you want to ask someone a favor, eye contact is more effective than an email or phone conversation. But does eye contact or the prospect of someone watching promote moral behavior? Research psychologist Melissa Bateson and colleagues carried out the following experiment to test this theory.

The employees of a business were required to place money in a pot when they made a cup of coffee or tea. However, payments were slim because many of them didn't pay if no one saw them at the machine. The researchers wanted to know if they could improve payment behavior by applying a simple intervention. First they hung a large poster with a picture of flowers at eye level above the money pot. Every two weeks they replaced the poster with a different floral print. Payment behavior remained unchanged. Then the researchers changed tack: every other week they hung a different poster with a photo of a pair of eyes. On one occasion they were a man's eyes, another time a woman's. On one occasion the person appeared friendly, another time rather tense. In all cases the eyes appeared to be looking directly into the eyes of the person getting a cup of coffee. What did the results show? The sum in the money pot rose, by no less than 275 percent.

According to the researchers an image of eyes gives people the feeling that they are not alone, and that their behavior is being observed. Another study shows that even the idea of someone watching has this effect. Research among three-year-old children shows that when they were told that there was an invisible princess in the room, they were less inclined to behave secretively. Students told that the ghost of a dead student had been observed in the examination room cheated less in their exam than students who were not told this. Study participants required to write sentences which made them think of God subsequently behaved far more altruistically than when they had not done this (regardless of whether or not they were religious).

When viewed in the context of video surveillance, one can see the benefits of using multiple cameras as a deterrent to crime. I've had many video sales people try to sell me on the concept of less equipment is better. You know, one camera to cover 2-3 teller stations. Or, "We have this new 360 degree camera that will cover the entire branch. You can save money and improve the aesthetics of your branch with this single dome camera in the center of your lobby." It all sounds great, but put yourself in the bank robber's shoes, or consider the perception of the identity thief who's waiting patiently in line to cash a counterfeit check. When they walk into a branch, they are casing the room for security equipment and/or personnel. Wouldn't you rather have them see an entrance camera as soon as they walk through the door? Or, how about one on one teller cameras, several cameras throughout the lobby and office areas. Top it off with a sign on the front door that says, "video cameras record all activity in this office," and you've got a strong deterrence package. Comparatively speaking, multiple camera systems are not much more expensive than those fancy little dome units in the center of the lobby. I believe video surveillance cameras are some of the best crime prevention tools we have at our disposal, so don't skimp on their use.

WAR *Stories*

Up in Smoke

Without "formal training," bank robbers are left to figure out how to pull off a job using their own knowledge and resources – which doesn't always work out in their favor. Such was the case when two obviously inexperienced thieves from Everett, WA tried their hand at stealing from an ATM machine. The two men used a blazing blow torch to get through the durable metal barrier designed to protect the ATM's treasure trove of cash. But once the blowtorch penetrated the machine's casing, the men were surprised to discover just how quickly and easily paper currency catches fire. The ATM and the bills inside went up in smoke as the suspects fled the scene.

If At First You Don't Succeed...

As the old saying goes, "If at first you don't succeed, try, try again." Alex Garcia, 38, took that idiom literally when he attempted (and failed) to rob six Manhattan banks – on the same day. After successfully holding up an Apple Bank branch in Manhattan one week before, tellers recognized Garcia when he tried his luck again at that bank. He took off when employees tripped the alarm. Two hours later he showed up at Valley National Bank, where he left empty-handed. Fifteen minutes later Garcia tried his luck at a Capitol One branch, 30 minutes later an HSBC, followed by two different Chase banks, also in Manhattan. At his last five stops, Garcia fled when the tellers refused to give him cash. Garcia is still on the loose…but if history repeats itself, he'll be back.

Locked Out

Bank branches are outfitted with sophisticated equipment to deter and catch thieves, i.e. bullet proof glass, CCTV, alarm systems, and in some cases armed guards. In Guadalajara, Mexico, the actions of a quick-thinking bank employee, armed only with a door key, prevented a potentially dangerous robbery. When the employee saw three masked men approach the bank, he walked over and locked the inner doors to prevent them from entering. Video that has gone viral on social media shows the three foiled bandits standing in the locked vestibule, looking at each other, confused as to what to do next, before they exit the bank – with the bank employee on the other side of the door watching them as they go.

QUESTIONS & *Answers*

Q. We have an elderly customer who has come into our branch on a regular basis to make cash withdrawals on a regular basis in the neighborhood of $3,000-$4,000. He claims that it is payment for home care services provided by a nurse. We believe that he may be the victim of a home medical care scam or that a caregiver may be taking advantage of him. We've asked him for permission to speak with a family member, but he has basically told us to mind our own business. How far can we go in terms of notifying a family member of our concerns?

A. This is a very tricky situation. The right to financial privacy basically prohibits anyone from discussing financial records of an individual with any third party, so you run the risk of a privacy violation if you decide to contact another family member. One possible solution would be to file a suspicious activity report. What you describe sounds like a crime, so a SAR may be in order. The safe harbor clause (which may be found on the back of every SAR) states in part, "Federal law (31 U.S.C. 5318(g)(3)) provides complete protection from civil liability for all reports of suspicious transactions made to appropriate authorities, including supporting documentation, regardless of whether such reports are filed pursuant to this report's instructions or are filed on a voluntary basis. Specifically, the law provides that a financial institution, and its directors, officers, employees and agents, that make a disclosure of any possible violation of law or regulation, including in connection with the preparation of suspicious activity reports, shall not be liable to any person under any law or regulation of the United States, any constitution, law, or regulation of any State or political subdivision of any State, or under any contract or other legally enforceable agreement (including any arbitration agreement), for such disclosure or for any failure to provide notice of such disclosure to the person who is the subject of such disclosure or any other person identified in the disclosure. As you know, once a report is filed, you have the option of calling an investigating agency to make them aware of the situation, especially where it may be time sensitive. Of course, you may want to run this idea by your legal team, but we feel this would be an acceptable solution to your problem. Good luck.

Q. We have some rather cumbersome safe deposit box procedures at our bank. We must verify and record the identity of each customer who wants access to their box, and we must compare signatures upon each visit. Isn't there a simpler way to expedite that process?

A. Safe deposit box policies and procedures are extremely important because they establish "ordinary care" standards that will be the key issue in any lost or stolen property claim filed against a bank. Ordinary care is that degree of care that may reasonably be expected from a person in the party's situation. Generally, in those cases involving claims from the safe deposit box customers in which property is missing from the lessee's box, either through a burglary attack or a mysterious disappearance, the defendant-bank is required to prove that it used a reasonable degree of care in the safe deposit box operation. The defendant bank's failure to show that it used ordinary or reasonable care to protect the plaintiff's missing property could result in a finding of liability on the bank's part. A safe deposit operation should never be in a position of being negligent in its daily operating procedures. Negligence can result from inadequate and outdated security equipment; use of improperly trained or inexperienced personnel; and the failure of bank management to provide adequate and proper procedures and supervision. To that end, written policies and procedures, which are followed (and documented) in every transaction without fail are absolutely critical to reducing liability risk. The ABA and BAI have suggested policies and procedures for safe deposit box operations.

Having said the above, there are several new technologies out that are designed to streamline the safe deposit box process. For example, video technology might replace the need to manually record a driver's license number. Similarly, fingerprint technologies may replace the need for signature verification. Check with your safe deposit box supply partners for the latest technologies.

Q. My boss has asked me to explore a certification program for bank security. Is there a bank security specific certification program available for bank security officers?

A. Kudos to your boss for raising the issue. The Bank Protection Act requires "periodic training and re-training of officers and employees in their responsibilities under the [bank's] security program," and a certification program is the best way to demonstrate compliance with security officer training. The American Bankers Association (ABA) sponsors a certification program designed exclusively for security officers at banks and other financial institutions by the Institute of Certified Bankers (ICB). According to the ABA, the Certified Financial Services Security Professional (CFSSP) program is intended to:

- Establish a meaningful standard of knowledge and competency in financial institution security
- Give formal recognition to the bank security officer when prescribed standards of knowledge, experience, and performance are met
- Enable management to more readily identify the requisite experience and competencies needed to direct and administer the security function
- Promote continuing professional education and development in financial institution security.

The CFSSP advisory board has determined that a competent financial services security professional's expertise includes the following knowledge areas: Written security programs, Security devices, Crimes, Investigations, Life Safety, and Other Laws and regulations (e.g. applicants should have a general knowledge of the Bank Protection Act, Bank Secrecy Act, and privacy legislation). Applicants must meet specific experience, education, ethics and examination requirements determined to be competency measures for financial services security professionals. To qualify for the CFSSP designation, an applicant must be employed by a financial institution with at least 50 percent of work time dedicated to security responsibilities or be appointed by the Board of Directors as the organization's Security Officer.

WHAT DO *other* BANKERS *do?*

Housing Homeless Youth

Visions and Pathways, a nonprofit agency that helps families and youth in crisis throughout New Jersey received generous support from the **Financial Resources Federal Credit Union** (FRFCU). FRFCU presented the agency with a $10,000 grant to support its Outreach and Prevention program. A portion of the donated funds will go toward efforts to assist homeless college students who have aged out of foster care but do not have a place to live during the summer or other breaks from school. The agency helps them find short-term housing and jobs.

Uniting for the Community

Through a collaborative and community-based effort, the United Way of Bucks County (PA) is investing more than half a million dollars into the communities it serves in 2017 as part of the non-profit agency's larger investment strategy which totals roughly $2.6 million of programs, goods, and services in Bucks County. The agency has formed teams to focus on five key areas including education, assistance for senior citizens, referral services, emergency needs, hunger, and housing and homelessness. **QNB Bank** in Quakertown, PA presented a donation of $7,500 to the United Way of Bucks County to support their efforts in serving the community.

Legacy of Love Donation

The Beacon House in Marquette, MI provides an affordable place for patients and families to stay before and after surgeries, and while loved ones are in the hospital. The charitable organization was given two acres on the new hospital campus. To kick off the Beacon House's "Legacy of Love" campaign to construct a new fully ADA-compliant facility, **River Valley Bank** presented the non-profit with a $100,000 donation. The campaign is scheduled to go for the next two years, with construction beginning and as soon as they reach their goal.

Habitat Gets a Helping Hand

Avidia Bank reached out with a helping hand for local community members to receive new housing. The Avidia Charitable Foundation donated $1,000 to Habitat for Humanity MetroWest/ Greater Worcester to assist with the renovation of two homes into four condos in Northborough, MA.

Purple For a Purpose

More than 5 million Americans are living with Alzheimer's, a devastating disease that attacks the brain and causes dementia.. By 2050, this number could be 16 million. During the month of June, **GCS Credit Union** employees went purple with a purpose for Alzheimer's Disease Awareness and Caregivers Month to raise $1,095.00 for the Alzheimer's Association. To help raise awareness and funds, GCS employees participate in Jeans Day on Fridays and Saturdays during June in exchange for a donation of $15 or more.

The credit union's employees took the donation one step further to create a GCS Walk To #ENDALZ team at the upcoming Walk to End Alzheimer's event on September 23, 2017 at Southern Illinois University of Edwardsville.

AND IN *Conclusion*

"Is water damage included in your disaster recovery plan?"

BANKERS' *Hotline*

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.

BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVII NUMBER 5

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.

This issue went to press on May 26, 2017

The Blockchain-Bank Connection

by Teri Wesley

When cryptocurrency hit the financial marketplace, Bitcoin quickly became an oft-used buzzword. Today Blockchain – the distributed ledger technology for recording electronic transactions that underpins Bitcoin – is all the rage within the industry as the potential applications for the innovative technology are being explored by banks and industry focus groups. Blockchain was one of the primary topics at the FTC's third FinTech Forum Series held in March, which focuses on the consumer implications of emerging financial technologies, a.k.a. fintech. Fintech is redefining all areas of financial services – on the industry side and the consumer side. Technology is driving the way consumers borrow, spend, share and manage their finances and the way banks provide financial services and products. Blockchain is being hailed as fintech's latest and greatest innovation in the payments market, with proponents of the technology extolling the benefits of making global payment transactions more efficient and, more importantly, more secure. In 2015, an estimated $659 billion worth of goods and services were traded between the U.S. and China, a figure that is expected to experience continued growth. Businesses spend billions of dollars in payment processing fees for traditional wire transfers that can take several days to process. That's billions of dollars worth of opportunities for blockchain-based payments that can reduce both the time and cost of traditional B2B payments.

As with any new technology, there are concerns and potential consumer protection challenges. At the FTC's fintech forum, Deputy Director of the FTC's Bureau of Consumer Protection Daniel Kaufman stressed that innovation and consumer protection must go hand-in-hand. Blockchain is touted as one of the most secure digital capabilities available, based on nearly unhackable cryptography that secures the records in a transaction. Each transaction is tied (or linked, like a chain) to previous transactions or records. The transaction records are distributed among and viewable by all participants of a blockchain distributed ledger. For a hacker to tamper with the data would require changing all the previous records in the blockchain. Additionally, blockchain transactions are validated by algorithms on the nodes (computers in the network of participants in the distributed ledger). A single entity cannot create a transaction. The ability of each participant to monitor the transactions at any time provides open transparency. Blockchains can be set up as public (viewable by all) or private (limited number of trusted participants). The technology has been rigorously tested in pilots by many governments, companies and financial institutions that have found the technology to be incredibly secure.

According to a recent survey by Deloitte Consulting, 12 percent of financial services executives report they are in the beginning stages of blockchain deployment, with 24 percent of those planning to go live with some type of blockchain solution this year. More than 60 global banks and financial institutions are researching, experimenting or working on blockchain-enabled applications. The Bank of England conducted a proof-of-concept (PoC) to identify blockchain's potential. The bank has since confirmed that an upcoming version of its main interbank payments system will be compatible for settlements in blockchain-distributed ledgers. Qatar's Commercial Bank teamed up with banks in various other countries to test blockchain for processing international transfers. They reported the pilot resulted in increased transactional security as well as accuracy, and that they plan to extend the network to banks in additional countries.

(continued on next page)

The Blockchain-Bank Connection
(continued from front page)

Patent filings related to blockchain and distributed ledger technology are on track to see a significant increase. More than 350 blockchain-related patents were pursued by companies last November, with Bank of America, Goldman Sachs and Mastercard among the largest financial firms that applied.

Blockchain innovation groups have formed to increase awareness and promote the many benefits of the distributed ledger technology for its use in various industries. Founded in 2014, R3 is a distributed database technology company which leads a consortium of over 80 top global financial institutions from all areas of financial services, including clearing houses, exchanges, market infrastructure providers, asset managers, central banks, conduct regulators, trade associations, professional services firms and technology companies. The consortium is dedicated to developing industry standard solutions that will be the building blocks of a new financial services infrastructure.

Global financial messaging network SWIFT recently announced its blockchain proof-of-concept trial for real-time, cross-border payments and the reconciliation of banks' nostro accounts, which enable international transactions for the global banking system. The blockchain PoC trial has several primary banks already on board to participate (Wells Fargo, RBC Royal Bank, BNY Mellon, to name a few) with an additional 20 banks expected to join the program later in latter stages of the trial to validate and test the concept. If successful, the program will become part of Swift's gpi (global payments innovation) service which offers clients fast, transparent and traceable cross-border payments. According to SWIFT, nearly 100 banks have already signed up for the service which launched in February, with twelve banks sending several hundreds of thousands cross-border payments around the world presently.

In addition to facilitating payments, blockchain technology is also beneficial for biometric identity verification. While biometric security is already used for ID authentication in some banking channels, including ATMs, the applications operate on centralized servers which are vulnerable to intrusion. Blockchain's decentralized storage of sensitive data provides greater security and convenience, with faster authentication and more accurate results.

IN THE *News*

Fintech, Regtech, and an Upset

When the OCC announced plans to accept applications for charter from eligible fintech providers, the regulatory agency opened Pandora's Box. The OCC's proposal was met with strong opposition from banking groups, consumer advocacy groups, Congress, and even some fintech companies. The Conference of State Bank Supervisors (CSBS) took its objections all the way to the U.S. District Court for the District of Columbia when it filed a lawsuit, declaring the OCC's proposed nonbank charters to be unlawful and in violation of the Administrative Procedure Act.

The heated debate surrounding the OCC's plans to offer fintech charters is cooling down a bit following the departure of leading advocate and now former OCC director Thomas Curry. Before hanging up his OCC hat, Curry spoke at two recent events – Northwestern University's Kellogg School of Management and the Institute of International Bankers' (IIB) Annual Washington Conference. Curry addressed the current state of fintech innovation and the regulatory agency's efforts to encourage responsible innovation within the federal banking system. He also discussed the importance of maintaining safeguards to protect the federal banking system, and the value of international collaboration and professional bank supervision.

And the beat goes on….as a new wave of startups follow fintech, known as "regtech." Regtech (regulatory technology) refers to the application of information technology for regulatory monitoring, reporting and compliance. Curry stressed to IIB attendees that a greater level of collaboration between fintech providers and financial institutions could lead to enhanced innovation and growth in the regtech market.

The efforts to regulate fintech or regtech may hinge on former President Ronald Reagan's observation of the U.S. government's view on regulation: "If it moves, tax it. If it keeps moving, regulate it. And if it stops moving, subsidize it." In reality, the future of fintech and regtech may depend on the government's role in fostering fintech and steering it in the direction of sustainable growth.

CFPB Delays Prepaid Account Rule

Just as there are two sides of a coin, many of the laws and regulations put in place to protect consumers are a toss-up, with one side (proponents) calling heads and the other (opponents) calling tails, and it's anyone's guess where the coin lands. The Consumer Financial Protection Bureau's (CFPB) final Prepaid Account Rule, scheduled to go into effect in October, has been delayed for six months with a revised effective date of April 1, 2018. During this time-out period, the Bureau says it will revisit at least two substantive issues in the rule: the linking of credit cards to digital wallets and error resolution and limitations on liability for unregistered prepaid accounts. The CFPB and proponents of the regulation say the rule will regulate financial products, e.g., loadable debit cards and digital payment services, and provide consumers who use those products with the same protections and disclosures as checking accounts, as well as mitigate the use of those products for shady business practices and fraud. Opponents argue that online fraud has decreased over the past five years, and that the prepaid accounts rule will leave consumers with less access to financial tools, more fees, and fewer innovative products.

Reduce Risk and Build Relationships

In its May issue of FedFocus, the Federal Reserve Banks (FRB) featured valuable tools available to its clients to help mitigate payments risk and strengthen business banking relationships. Two toolboxes for hammering risk and cementing business account relationships include the Risk Management Toolbox and the Business Banking Toolbox (available in Acrobat format). The Risk Management Toolbox has tools to assist operational risk, compliance and audit staff in measuring and managing operational risks, monitoring internal and external compliance or audit obligations, and building a strong risk management program. The Business Banking Toolbox contains tools to assist treasury/cash management and business banking staff increase the flow of information to customers, reduce payment risk for the institution and its customers, and offer services that will enhance client relationships. Get the FRB's free resources at www.frbservices.org

Statistics, *Facts & Such*

■ Nearly 1.4 billion records were compromised in 2016 as a result of roughly 1,800 data breaches.
Security Week, *3/28/17*

■ The number of compromised records increased by 86% compared to the previous year. The report also shows that more than 1,000 incidents (59% of the total) involved theft of identity information, and nearly 30% involved financial and account data.
Ibid.

■ Malicious hackers were behind 68% of data breaches, while 19% were the result of accidental leaks, and malicious insiders accounted for 9% of breaches.
Ibid.

■ In March, the number of U.S. consumer Visa chip card transactions topped 1 billion for the first time (a 330% increase from March, 2016).
ATM Marketplace, *4/25/17*

■ There are now more than 421 million Visa chip cards in the U.S.
Ibid.

■ Counterfeit fraud was down 58% at chip-enabled merchants in December 2016, compared with the previous year.
Ibid.

■ Employees (1 in 3) are willing to share sensitive or confidential information under some circumstances. A third said it's common to take confidential data when leaving a company.
Credit Union Times, *4/25/17*

■ Four in five employees in financial services (81%) would share confidential information.
Ibid.

■ Employees often access, share and store data in unsafe ways. Of those surveyed, 24% say they do so to get their job done.
Ibid.

■ Other unsafe behaviors include: using public Wi-Fi to access confidential information (46%), using personal email accounts for work (49%), or losing a company-issued device (17%).Some 45% of employees use email to share confidential files with third-party vendors or consultants
Ibid.

Tech *Update*

Corporate Espionage Prevention

Research Electronics International is pleased to announce the ANDRE™ Advanced Near-field Detection Receiver, a hand-held broadband receiver that detects and assists in locating nearby RF, infrared, visible light, carrier current and other types of transmitters. Access to eavesdropping and electronic bugging devices is becoming easier and more affordable. Broadband receivers, like the ANDRE, provide mobile RF search capability to help locate these and other transmitters quickly and discretely.

The ANDRE detects signal activity in its vicinity and displays changes in signal strength over time, allowing users to quickly locate the source of transmissions. The ANDRE's frequency counter provides quick frequency information of the strongest signal and outputs additional information to an automatic signal list generator. Antenna probes included with the ANDRE can be used to sweep rooms and objects in search for known, unknown, illegal, disruptive, or interfering transmitters from 10 kHz to 6 GHz.

A 3.5-inch touch screen displays all of the operation controls and frequency activity. The frequency chart provides advantages over other RF detectors by showing rising and falling signal strength over time. Eight displayed time intervals can be selected ranging from 5 seconds to 24 hours. This helps identify pulsing signals and shows historical peaks, to ensure nothing will be missed. Manual and automatic threshold settings notify the user when a signal exceeds defined strength levels with haptic, audible, and visual alerts.

The ANDRE automatically recognizes connected probes and displays the appropriate frequency band on the time chart. A built-in frequency counter registers the strongest signal and displays the frequency. Output from the frequency counter can automatically generate a signal list with additional details such as received signal strength, attenuation and gain settings, and information about the communication band classification. Band identification will help classify detected signals based on the FCC frequency allocation the signal falls within.

As the signal list builds, stronger signals rise to the top of the list and weaker signals fall within the list. The signal list displays the frequency, date/time and the option to designate the signal as Friendly; Threat; or Unknown. The ANDRE also has the option to capture and store screen shots of any of the screens and audio files. A USB port and cable provides the means for transferring files and recharging batteries in the unit.

RF investigators will find the ANDRE a valuable asset and affordably-priced to complement advanced analysis equipment, like the OSCOR spectrum analyzer. It can also be used independently to acquire quick, non-alerting RF detection and location. Commercial and corporate applications include performing site surveys, installing and maintaining RF systems, and emissions detection of illicit transmitters.

COMING *Up*

23rd Annual Bank Security Conference!

New Name! New Location!
Same premium conference dedicated to bank security personnel
Attend Live or via Remote Streaming
The Crystal City Hyatt, Washington, DC, October 25-26, 2017
(optional Basic Security 101 workshop October 24)
Save the Date! More details coming soon!

ASIS INTERNATIONAL

ASIS 27th New York City Security Conference
New York, NY, June 7-8, 2017
ASIS International 63rd Annual Seminar and Exhibits
Dallas, TX, Sept 25-28, 2017
Info: (703) 519-6200
www.asisonline.org

ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)

ACAMS 5th Annual AML Risk Mgmt Conf
New York, NY, June 9, 2017
ACAMS 16th Annual AML & Financial Crime Conference
Las Vegas, NV, Sept 25-27, 2017
Info: www.acams.org

TRAINING **PAGE**

The (in)Security of (im)Perfect Passwords

by P. Kevin Smith, CPP

Did you know that Thursday, May 4th was "world password day" for 2017? At first I thought that Hallmark had done it again, but it turns out that "password day" is a legitimate moniker for the day that is set aside to bring awareness to strengthening personal passwords and password policies at companies throughout the world. Security researcher Mark Burnett first encouraged people to have a "password day," where they update important passwords, in his 2005 book Perfect Passwords. Inspired by his idea, Intel Security took the initiative to declare the first Thursday in May World Password Day in May 2013. Intel created the event as an annual reminder that, for most of us, our password habits are nothing to celebrate. World Password Day is a good time to ditch "qwerty" and "123456" – two of the most popular passwords – and beef up your password protocols.

A recent article written by Megan Squire, Professor of Computing Sciences at Elon University, is applicable for everyone, including end users throughout the financial services industry. We encourage you to consider the followings tips on password security from Ms. Squire when reviewing and updating your institution's password policy.

Predictable Passwords

The purpose of the password is to limit access to information. Having a very common or simple one like "ABCDEF" or "letmein" or even normal words like "password" or "dragon" is barely any security at all. It's like closing a door but not actually locking it. Hackers' password cracking tools take advantage of this lack of creativity.

Many savvy users who choose a less common password might still fall prey to what is called a "dictionary hack". The cracking software tries each of the 171,000 words in the English dictionary then the program tries combined words such as ("qwertypassword"), doubled sequences ("qwertyqwerty"), and words followed by numbers ("qwerty123").

Blind Guessing

Only if the dictionary attack fails will the attacker reluctantly move to what is called a "brute force attack", guessing arbitrary sequences of numbers letters and characters over and over until it matches. Mathematics tells us that a longer password is less guessable than a shorter password. That's true even if the shorter password is made from a larger set of possible characters. For example, a six-character password made up of the 95 different symbols on the standard American keyboard yields 735 billion possible combinations. That sounds like a lot but a 10 character password made from only lowercase English characters yields 141 trillion options. Of course a 10 character password from the 95 symbols gives 59 quintillion possibilities.

That's why some websites require passwords of certain lengths and with certain numbers of digits and special characters. They're designed to thwart most common dictionary and brute force attacks. Given enough time and computing power though any password is crackable. And in any case humans are terrible and memorizing long unpredictable sequences. We sometimes use mnemonics to help, like the way "Every Good Boy Does Fine" reminds us of the notes indicated by the lines on sheet music. They can also help us remember a password like, "freQ!9ty!juNC", which at first appears to be very mixed up. Splitting the password into three chunks, "freQ!", "9tY!", and "juNC" reveals what might be remembered as three short, pronounceable words: freak, ninety, and junk. People are better at memorizing passwords that can be chunked, either because they find meaning in the chunks or because they can more easily add their own meaning through mnemonics.

Don't Reuse Passwords

Suppose we take all this advice to heart and resolve to make all our passwords at least 15 characters long and full of random numbers and letters. We invent clever mnemonic devices, commit a few of our favorites to memory and start using those same passwords over and over on every website and application.

At first this might seem harmless enough, but password thieving hackers are everywhere. Recently big companies including Yahoo, Adobe and LinkedIn have all been breached. Each of these breaches revealed the usernames and passwords for hundreds of millions of accounts. Hackers know that people commonly reuse passwords, so a cracked password on one site could make the same person vulnerable on a different site.

Beyond The Password

Not only do we need long unpredictable passwords but we need different passwords for every site and program we use. The average Internet user has 19 different passwords. It's easy to see why people write them down on sticky notes or just click the "I forgot my password" link.

Software can help! The job of password management software is to take care of generating and remembering unique, hard to crack passwords for each website an application. Sometimes these programs themselves have vulnerabilities that can be exploited by attackers. And some websites blocked password managers from functioning. And of course, an attacker could peek at a keyboard as we type in our passwords. Of course, no system is perfect, and these tools do create a single point of failure if they're ever compromised. And if you use multiple computers, you have to have them loaded onto each machine. Still, they do offer a secure, efficient way to keep a long list of passwords.

Multi factor authentication was invented to solve these problems. This involves a code sent to a mobile phone, a fingerprint scan or a special USB hardware token. However, even though users know the multi factor authentication is probably safer, they worry it might be more inconvenient or difficult. To make it easier, sites like Authy.com provide straightforward guides for enabling multi-factor authentication on popular websites.

If you missed out on World Password Day this month, it's not too late to jump on the bandwagon now, deploy multi-factor authentication and encourage employees to use a password manager, and put World Password Day on your training schedule every May. And remind your employees that, as the saying goes, passwords are like underwear. You should change them often (okay, maybe not every day). Don't leave them out for others to see (no sticky notes!). Don't share…keep them private.

Password management should be an integral part of your institution's network and corporate security policies.

Banks Responding to Consumer Complaints

The CFPB has released its *2016 Consumer Response Annual Report*, providing an overview of consumer complaints the Bureau received last year. The consumer watchdog agency handled 291,400 complaints from consumers in 2016 (a 7% increase from the prior year). The top three complaint categories were debt collection (30%), credit reporting (19%), and mortgages (18%). Bank accounts or services offered by banks, credit unions and nonbank companies ranked fourth (10%) of all complaints. The most common type of bank account and service complaints related to opening, closing, or managing accounts. Overdrafts remain a common complaint, including those related to transaction ordering and occurring because of confusion over availability of funds. Overdraft fees amounts, insufficient fund fees, extended overdraft fees and monthly maintenance fees were also among the complaints. Error resolution procedures for deposit accounts, including time lines for investigation and provisional credit for disputed transactions, were another hot topic. On the plus side, the Bureau reports that 97 percent of the complaints sent to financial companies in 2016 received timely responses from recipients.

'Tis the Season for Same Day ACH Testing

While some parts of the country are experiencing fluctuating and atypical seasonal weather, we are entering Memorial Day weekend – and summer is just around the corner. For ACH Network participating banks, the September 15, 2017 implementation date for Phase 2 of Same Day ACH is not far off. In preparation for going live in September, the FedACH Services will be conducting ACH file testing (sending and receiving test files to validate back end processing) in a series of waves throughout the summer. Eligible customers will be notified by email approximately 45 days in advance of their scheduled testing windows.

More information and supporting documents to prepare for Same Day ACH are located at FRB's website https://www.frbservices.org/resourcecenter/sameday_ach/

Focus *on Fraud*

New Cyber Executive Order

On May 11, President Trump signed a much-anticipated cybersecurity Executive Order (EO) designed to shore up the nation's cybersecurity defenses. The EO includes an initiative to reduce the threats posed by botnets – networks of compromised computers designed to spread malware and banking trojans – that have been a growing threat to the financial industry. The EO also directs federal agencies to improve the cybersecurity of federal networks, and to follow the framework for cybersecurity set forth by the National Institute of Standards and Technology (NIST). Federal agencies will be required to review the state of their cybersecurity and submit a risk management report to the Department of Homeland Security within 90 days.

ID Theft is a Booming Business

In the war on cybercrime, the financial industry and other sectors have taken some hard hits already this year. According to a newly released Q1 2017 Cybercrime Report from digital identity company ThreatMetrix, 130 million fraud attacks were detected in the first 90 days of this year. Identities are the most sought-after cyber bounty, with sophisticated new techniques and loopholes in emerging fintech platforms helping criminals successfully launch their attacks. Another recent study released by Javelin Strategy and Research revealed that cyber criminals stole more than $16 billion from more than 15 million U.S. consumers last year.

The University of Texas at Austin Center for Identity developed a risk assessment tool – the Identity Threat Assessment and Prediction (ITAP) – which provided unique insights into data collected from more than 5,000 incidents that occurred between 2000 and 2016. Some of the key ID theft risk factors the researchers identified from their assessment of the data collected include:

- People make mistakes, and human error is a major factor in ID theft as hackers exploit vulnerabilities created by mistakes people make.
- Impact is more localized than global. Over 99% of the cases studied were limited to either a local geographic area or a particular type of victim.
- The ITAP model identified four different types of loss experienced by victims: Emotional distress (72%); financial (57%); property (56%) and reputation (41%).
- Insiders are a primary risk. One-third of the incidents involving compromised PII originated from company employees or victims' family members.
- Over half of the incidents studied were linked to non-cyber related crimes, e.g., Magnetic stripe ($28.9m); ATM pin ($24.2m); fake ID data ($15.1m).

Good Guys-1, Bad Guy-27

The expression "chalk it up" originated when it was customary for a business to write a customer's outstanding charges on a chalkboard. Today, it's used to give credit where credit is due. In an unprecedented case – and a "chalk one up for the good guys!" – a Russian hacker who stole 2.9 million card numbers and defrauded banks at least $170 million was extradited to the U.S., tried and convicted of 38 counts related to hacking, and sentenced to 27 years in prison – a record sentence handed down to a hacker in this country. Roman Seleznev hacked into point-of-sale (PoS) systems and installed malware that pilfered credit card numbers from more than 500 U.S. businesses and impacted approximately 3,700 financial institutions. He sold the stolen card numbers to criminals on underground websites. Calling Seleznev's criminal enterprise "sophisticated and expansive, with transnational implications," the U.S. Secret Service praised law enforcement agencies for holding accountable those who perpetrate such crimes.

Billion Dollar BEC Scams

On May 4, the FBI issued a PSA update to previous Business Email Compromise (BEC) announcements to provide new data as of December 31, 2016. It's important for banks to keep up-to-date on these scams, as techniques used in the Email Account Compromise (EAC) component of BEC targets those who perform wire transfer payments. The FBI reports that these scams have evolved to include the compromising of legitimate business email accounts and requesting Personally Identifiable Information (PII) or W-2 forms for employees, and may not always include funds transfer requests. The agency reports a 2,370% increase and billions of dollars in identified exposed losses. Get the full updated PSA at www.ic3.gov.

From the Editor

Security's Place

by P. Kevin Smith, CPP

I usually try to avoid political issues in this column, but the recent flap over the firing of FBI Director James Comey offers a valuable lesson about security's role in any organization. According to the White House, Mr. Comey was fired by President Trump for two issues. The first is Comey's unprofessional handling of the Hillary Clinton email investigation, where he first decided not to prosecute her over the mishandling of classified information and then subsequently revealed to the public that the investigation had been reopened shortly before the election, possibly influencing the outcome. This is a serious matter, as Comey broke with precedent by going public with details of bureau investigations that normally are considered confidential. The second issue raised is Comey's inability to "effectively lead the Bureau" given what has occurred since last summer. That is a legitimate concern. When the Clinton investigation was shelved, there was considerable dissent in the bureau, with many among the rank-and-file believing that the egregious mishandling of classified information should have some consequences. It would be safe to say that FBI morale plummeted as a result of the Clinton e-mail investigation.

Of course, not everyone believes that Comey was fired for poor performance. A recent survey by Statistico indicates that 34% of Americans believe that Comey was fired because of his handling of the current investigation into the Trump administration's relationship with Russia and their alleged attempts to influence the presidential election. I believe that the simplest explanation for Comey's firing is that Donald Trump doesn't like him much and doesn't trust him at all. Regardless of your political affiliation or beliefs, the Comey situation offers some valuable insight into the importance of organizational structure as it relates to the security function. While it is convenient to believe that the FBI director operates independently from the politicians who run the country, the reality is that he or she works for the attorney general, who in turn works for the president. That is the chain of command, like it or not. Any U.S. president can insist on a national-security team that he is comfortable with, and if Trump is willing to take the heat from Congress and the media, he is entitled to hire an FBI Director that he is comfortable with.

As a Corporate Security Director for several financial institutions and one non-banking organization, I've seen the security function housed in a variety of ways. In my early years, when security was an afterthought in most organizations, security would typically be found in the Facilities or General Services area, since most of their responsibilities dealt with security equipment and branch construction. The only regulatory requirement affecting the security function was the Bank Protection Act. In 1999, the Gramm, Leach, Bliley Act mandated information security safeguards for financial institution customers, so many banks focused on information security. The term "convergence" came into vogue as many firms decided to combine information and physical security into one organizational unit. During those years, there was a tendency to house the security function under the Chief Information Officer because of the perceived synergies between physical and information security. Of course, the horrific events of September 11, 2001 had a dramatic impact on security's role in virtually every company, as potential terrorist attacks became a huge concern for the banking industry, especially the larger banks throughout the world. For a little over a year, there was a tendency to house the security function in the Human Resources Division because of its close ties to background investigations and training. Finally, the Sarbanes Oxley Act was passed in 2002, which was enacted as a reaction to a number of major corporate and accounting scandals, including Enron and WorldCom. The 11 sections of the bill cover responsibilities of a public corporation's board of directors, adds criminal penalties for certain misconduct, and required the Securities and Exchange Commission to create regulations to define how public corporations are to comply with the law. There were so many regulations related to security, many companies decided to house the security function in the Legal & Compliance area.

In my humble opinion (and I never thought I'd say this), the time has come for the corporate investigative function to be housed in the Audit Department, or some function that has a direct reporting relationship to the Board of Directors. If the Comey situation has taught us anything, it's that the investigative function should be completely separate from the influence of any individual within the organization.

WAR *Stories*

Booze Sting Nets Bandit

The capture of a bank bandit was credited to a police cadet who was working undercover in a sting operation to catch adults buying alcohol for minors. The cadet alerted other officers to suspicious activity across the street from where she was working. When the officers approached three men, they recognized Cedric Ray Vincent from surveillance photos taken during a bank robbery the day before. Vincent was recently released from prison and was on parole for robbery. He is a suspect in a second area robbery. As he makes his way back to prison, new charges have been added – suspicion of bank robbery, felony parole violation and receiving stolen property.

Suspect Was a Shoe-In

Women tend to be obsessed with shoes. On average, a woman owns 20 pairs of shoes at any given time. Cornetta Newton apparently had a favorite pair of shoes that she wore when she robbed four banks in Arizona earlier this year. Newton was arrested when she attempted a fifth heist at Amtrust Bank in Scottsdale. Dubbed the "SOS Bandit" by the FBI for her slip-on shoes, Newton has been charged with four bank robberies, in addition to one charge of attempted bank robbery. Hope she has shoes that coordinate with her new prison garb.

An Eclectic Disguise

In what may be the first-of-its-kind, or a sign of the times, a bank robber took advantage of an eclectic event to pull a heist, figuring she would just blend in with the crowd. While an annual LGBTQ parade was taking place in Northampton, MA, 37-year-old Jennifer Brumer – wearing a hooded sweatshirt with skulls on the front and a Mohawk graphic on the back and zipped up to cover her face – entered a TD Bank branch, handed the teller a demand note and left the bank with just $500. She was apprehended just 15 minutes later after purchasing liquor, beer and cigarettes. Brumer was charged with unarmed robbery and held without bail…or her pride.

QUESTIONS & *Answers*

Q. Television shows often refer to DNA testing as a conclusive way to convict a criminal. Is DNA evidence foolproof and will it alone convict a person of a crime?

A. Although 99.9% of human DNA sequences are the same in every person in the world, there is still enough of a difference in order to distinguish one person from another. Using a method called DNA testing, also known as DNA profiling, scientists analyze a long chain of DNA to identify specific "loci." These loci are very similar when you are comparing the loci of two closely related people, but among people unrelated, the differences are much greater. Thus, in criminal prosecutions, DNA evidence is often offered to link the accused with being at the scene of the crime, but it can also be used by the defendant to prove their actual innocence. Courts have accepted the overall accuracy and value of DNA testing. For example, courts have allowed prosecutors to search for suspects by interviewing people in the DNA database who have merely similar DNA to that found at the crime scene, indicating family members.

However, exact probabilities of a match remain disputed. The FBI estimates that the odds of a coincidental match are 1 in 108 trillion. Other estimates are 1 in 113 billion, 1 in 10 billion, or 1 in 8192.To explain the variance, more and more loci are being discovered. Another reason why there might be so much variance is that the DNA actually being analyzed is but a chemical replication of the original. Statistics may also take into account human error and the probability of obtaining an uncorrupted DNA sample.

Recently, the California Supreme Court addressed a "cold hit" murder case – where DNA at the crime scene was matched with a convict in the FBI database. The court allowed a "rarity statistic" to be told to the jury – that there was only a 1 in 930 sextillion chance of finding the same DNA profile in the general population. In short, DNA testing is an important tool that can be used to find the guilty party and rule out those who have not committed the crime. But it's not a magical solution to all law enforcement problems. It needs to be used carefully and responsibly to make sure that our criminal justice system is always fair.

Q. We've heard that banks are a part of the Federal Government's critical infrastructure, and as such we should be aware of the critical infrastructure plan. What exactly does that mean and should we be active in the critical infrastructure program?

A. There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The Financial Services Sector represents a vital component of our nation's critical infrastructure.

Large-scale power outages, recent natural disasters, and an increase in the number and sophistication of cyberattacks demonstrate the wide range of potential risks facing the sector. The Financial Services Sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. Financial institutions vary widely in size and presence, ranging from some of the world's largest global companies with thousands of employees and many billions of dollars in assets, to community banks and credit unions with a small number of employees serving individual communities. Whether an individual savings account, financial derivatives, credit extended to a large organization, or investments made to a foreign country, these products allow customers to:

1. Deposit funds and make payments to other parties
2. Provide credit and liquidity to customers
3. Invest funds for both long and short periods
4. Transfer financial risks between customers

The Financial Services Sector-Specific Plan details how the National Infrastructure Protection Plan risk management framework is implemented within the context of the unique characteristics and risk landscape of the sector. Each Sector-Specific Agency develops a sector-specific plan through a coordinated effort involving its public and private sector partners. The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector. All banks are urged to review the 2015 Financial Services Sector-Specific Plan (SSP) which provides an overview of the sector and the cybersecurity and physical risks it faces, establishes a strategic framework that serves as a guide for prioritizing the sector's day-to-day work, and describes the key mechanisms through which this strategic framework is implemented and assessed.

Q. My question is perhaps more personal than professional. Every once in a while I get a message on my computer that says my computer has been locked and I must pay money to have it unlocked. I'm embarrassed to ask anyone at work about this, but should I pay the money?

A. What you have experienced is a relatively low end "Ransomware attack" that was promulgated by a phishing attack. You probably didn't even notice it at the time, but some e-mail attachment or hyperlink deposited the ransomware on your computer. Despite the warning on the pop-up alert not to close the program or turn off the computer, that is exactly what you need to do. Open your task manager by pressing the control-alt-delete keys on your keyboard. Look through the list of processes until the name of the browser you are using appears (Edge, Chrome, Firefox, Internet Explorer, etc). Highlight the task associated with the browser and click "end task". This will close the browser and end the annoying message. Shutting down the PC will work as well, but putting the PC to sleep accomplishes nothing. One additional piece of advice is to run a virus scan first, and then change all of your passwords as soon as possible. Above all, do not pay the money as instructed on the alert. It's also a good idea to file a report with the FBI's Internet Crime Complaint Center (IC3).

WHAT DO *other* BANKERS *do?*

Help for Homebuyers

Low-income residents who are first time homebuyers in Massachusetts are getting a little help from their friends at Leominster Credit Union. The LCU is distributing a $110,000 grant to low-income homebuyers or displaced homemakers who are buying a home for the first time. The grant is part of the Equity Builder Program of the Federal Home Loan Bank of Boston, a wholesale bank cooperatively owned by more than 440 New England credit unions and other financial institutions. This is the fourth year the credit union has issued grants under the program, which has awarded more than $32 million in funds assisting 2,867 income-eligible households with home purchases throughout New England.

Money for Meals

The Meals on Wheels program operates in virtually every community in America to address senior hunger and isolation. Meals on Wheels of Ridgefield, CT has been providing meals for those needing assistance due to age, disability or illness since 1972. Each year, over 120 volunteers prepare and deliver more than 20,000 meals to local residents in need. The Fairfield County Bank presented the organization with a $5,000 donation to help fund the supplies needed by the organization to continue providing nourishing meals to low and moderate income residents.

Funding Community Support

Franklin Savings Bank (FSB) in NH established its FSB Fund for Community Advancement campaign to provide support for regional projects that enhance the lives of residents in the communities served by the bank. A wide range of local non-profits for various causes are supported by the Fund, including economic development, affordable housing, education, human services, and programs or services that address the needs of children, adolescents, and single parent families. In April, the bank awarded $20,500 in grants to four local organizations: Child & Family Services of NH, $7,500; Franklin Outing Club, $3,000; Grafton County Senior Citizens Council, $5,000; and Pemi Youth Center in Franklin, $5,000. Since its inception in 1997, the Fund has provided 188 awards totaling $898,000.

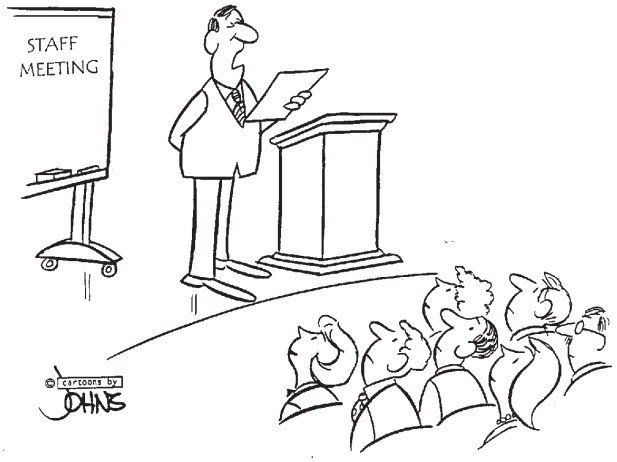
Helping Hand for Healthcare

In a generous show of support for Westfield Memorial Hospital and their mission to provide quality healthcare to local residents, Lake Shore Savings Bank presented a gift of $50,000 (to be distributed over three years) to the WMH Foundation for the hospital's RED (Renovate our Emergency Department) Campaign. To date, 50 percent of the RED Campaign's $650,000 goal has been raised and the upgrade is expected to begin this fall.

A Charitable Donation

The Eastern Bank Charitable Foundation provides grants and donations to regional charitable organizations. The Foundation donated $2,500 to the Greater Newburyport YWCA to further the development of ongoing initiatives supporting the community. The bank's donation will go toward programs at the local YMCA facility, such as activities for low-income children, reduced-fee child care for working families, and more.

AND IN *Conclusion*



"You must update your passwords regularly to contain letters, numbers, doodles, sign language, and a picture of your favorite pet."

BANKERS' Hotline

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.

BANKERS' Hotline
THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVII NUMBER 1

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.
This issue went to press on January 18, 2017

Presidential Priorities

Industry Wish List for 2017

by Teri Wesley

As we go to press with this issue, the United States will soon have a new Chief at its helm. Just as January signals the start to a fresh, new year — offering a clean slate for individuals and businesses to turn last year's negatives into this year's positives — January 20 is the dawn of a new era for America. No more than we can change the impact the Obama administration had on this country, there is no crystal ball to provide a glimpse into what's in store for this great nation – and the financial industry - under the regime of President Trump and the 115th Congress.

The industry's most prominent banking group has provided the House and Senate leaders its wish list of legislative priorities for the new administration. In a letter issued by Rob Nichols, president of the American Bankers Association (ABA), dated January 4, changes to mortgage rules, fintech oversight, cybersecurity, small-dollar credit, and money laundering were among the policy goals the ABA urged the new Administration to consider. In reference to the re-evaluation, and possible repeal, of the Dodd-Frank Act, Nichols called on the Administration, Congress and bank regulatory agencies to "work in a bipartisan manner to pursue legislative changes that will keep financial institutions strong and capable of fulfilling their mission." The letter points out that increased regulation and growing competition from unregulated fintech players has been instrumental in the failure of banks. Since 2006, more than 1,500 banks have failed, been acquired or merged, while only four new bank charters have been granted, Nichols said, adding that, "there are many factors beyond the Dodd-Frank Act that have caused the closure and consolidation of banks. Nichols added that "the sheer weight of more than 24,000 pages of proposed and final rules of this law has become a key consideration for many institutions in determining their future."

The legislative priorities outlined in the ABA's letter included:

- **Tailored regulation and arbitrary thresholds.** Tailor regulation to correspond to a bank's business model and risk, eliminate artificial and arbitrary regulatory asset thresholds, and pursue a more balanced supervisory process.
- **Mortgage rules**. Reform mortgage regulations that have raised costs and prevented banks from flexibly serving their customers without enhancing consumer protections or safety and soundness.
- **Housing finance reform**. Constrain the role of the federal government in housing finance with respect to loans made by private lenders and ensure equitable access to such programs by lenders of all sizes and from all communities.
- **Flood insurance**. Help homeowners protect themselves by providing more incentives to participate in the National Flood Insurance Program and encouraging development of a strong private flood insurance market.
- **Level playing fields**. Reduce economic distortions by providing more charter flexibility and capital options for thrift institutions, including mutual banks, and protecting S-Corp banks from arbitrary disadvantages due to the Basel III capital and other rules.
- **Small business growth**. Fuel lending to job-creating businesses through both increased funding for key SBA loan programs and eliminate regulations that artificially dictate business lending decisions.
- **Tax reform**. Reduce rates to drive growth while simplifying the complex tax code and eliminating poorly targeted subsidies to massive credit unions and Farm Credit lenders that no longer pursue their missions.

(continued on next page)

Presidential Priorities: Industry Wish List
(continued from front page)

- **Student debt**. Change the tax treatment of student debt repayments to help unburden those who have invested in their own potential.
- **Fintech and nonbank competitors**. Facilitate partnerships of banks and technology firms, ensure customers are protected through consistent and effective oversight of all providers and encourage innovations by providing a regulatory "greenhouse" for testing new products before roll-out.
- **Data breaches**. Ensure that all parties share accountability for protecting customer information and notifying the public after a breach, with the responsible party bearing the costs of their failure to protect customers.
- **Cybersecurity**. Expand collaborative public-private efforts to fight cyber threats through information-sharing and self-reporting of cyber risks without fear of regulatory sanctions or reputation risk.
- **Rural growth**. Pursue pro-growth policies to help farmers manage debt burdens and pricing challenges, fight deposit flight through encouraging access to longer-term stable funding sources, and address the shortage of qualified appraisers in rural areas that hinders real estate transactions.
- **Interchange**. Restore market pricing on debit interchange fees so that consumers can once again enjoy more flexibility in the products and services that banks offer.
- **AML/BSA**. Limit the burdens of Bank Secrecy Act compliance and reporting – especially new requirements that place undue burdens on customers – and eliminate potential sanctions for banking legal businesses.
- **Small-dollar credit**. Preserve banks' ability to serve customers with small-dollar loans and overdraft protection.
- **Sensible regulation**. Oversee finance in a way that promotes growth and innovation, while avoiding arbitrary and capricious penalties and providing robust exam review and appeal channels. Update rules to reflect changes in technology. Restore balance to the regulatory process, including Consumer Financial Protection Bureau reform and a focus on promoting both economic growth and safety and soundness.

As new leadership takes over in the Oval Office, we hope to see many of the items on this wish list fulfilled.

IN THE *News*

Risky The OCC on Risky Sales Practices

In the wake of the Wells Fargo scandal over improper sales practices in which Wells Fargo employees secretly created millions of unauthorized bank and credit card accounts for five years to hit sales targets and receive bonuses, the OCC's Semiannual Risk Perspective for Fall 2016 included an added focus on sales oversight. The report highlights the risks facing national banks and federal savings associations. In addition to strategic, credit, operational, and compliance risks, the OCC added sales practices to the key financial institution risks.

With banks facing challenges in growing revenue and competition from fintech providers, strategic risk remains high as banks adopt innovative products, services, and processes in response to the evolving demands for financial services. Operational risk continues to be another key risk area as banks face evolving cybersecurity threats, increased reliance on third-party relationships…and the need for sound governance over sales practices. Other key risks are in the areas of lending, meeting the integrated mortgage disclosure requirements and amended Military Lending Act regulatory requirements, and managing Bank Secrecy Act risks. You can find the OCC's release, dated January 5, 2017, and a link to the full risk report at www.occ.gov.

CFPB Cautions Banks About Sales Goals

As we enter the New Year and your institution sets its sales goals and incentives for 2017, make sure the bar isn't set so high that employees feel pressured to resort to deceptive tactics or illegal practices to reach what may be unrealistic goals.

While the future of the Consumer Financial Protection Bureau (CFPB) remains uncertain under the new Administration, the consumer watchdog agency continues its quest to protect American consumers from predatory practices. On November 28, the CFPB issued a bulletin warning supervised financial companies that creating incentives for employees and service providers to meet sales and other business goals can lead to consumer harm if not properly managed. Financial institutions that tie bonuses or employment status to unrealistic sales goals or to the terms of transactions may intentionally or unintentionally encourage illegal practices such as unauthorized account openings, unauthorized opt-ins to overdraft services, deceptive sales tactics, and steering consumers into less favorable products. On the flip side, practical incentives can benefit consumers and help financial services attract and retain valuable employees that contribute to the institution's overall success. CFPB Director Richard Cordray warned its supervised financial companies "to make sure that their incentives operate to reward quality customer service, not fraud and abuse." The CFPB bulletin outlines various steps that institutions can and should take to detect, prevent, and correct such production incentives to enhance customer service and prevent harm to consumers.

Train Today for Future Financial Stability

Today's young people will enter a financial marketplace that is much more complex than previous generations. Educating tomorrow's leaders today on how to spend wisely, manage credit, and save for the future helps them avoid common financial pitfalls and fosters economic stability. In 1997, a nationwide program was launched to organize bank volunteers to help young people develop early savings habits. The Teach Children to Save (TCTS) program, sponsored by the ABA Foundation, is celebrating 20 years this year. Banks of all sizes are encouraged to take part in this initiative by providing any savings-related lesson, presentation, or event, specifically those that focus on how to save, reasons to save and where to save. Examples include bank visits and events with other organizations that discuss saving, distributing savings-related materials, and in-school bank lessons that augment deposit collections.

Registration for the 2017 program is free (ABA membership not required). Banks that register have access to free presentation planning tools, lesson plans, a social media guide, and press materials to publicize the bank's efforts. They can also attend the Celebrate 20 Years of Teach Children to Save Webinar, on January 25, 2017 at 2:00 pm ET. The hour-long session is designed to familiarize bankers new to TCTS by breaking down the program and providing action steps, ideas and tips on putting together an effective TCTS lesson.

Statistics, *Facts &* Such

■ More than half (53%) of consumers surveyed prefer online or mobile banking for standard daily transactions.
CU Insight, *Fiserv Expectations & Experiences Survey,12/14/16*

■ Many (44%) consumers still prefer a traditional branch while 2% prefer fully automated branches.
Ibid.

■ More than 80% of consumers logged on to their primary financial organization's online banking site in the last month to check balances (79%), pay bills (47%) or transfer funds (41%).
Ibid.

■ Among those who have visited a branch in the last month (61%), the common reasons were to deposit checks (68%), withdraw cash (51%) or speak to representatives (22 %).
Ibid.

■ Only 16% of all consumers surveyed have used a mobile wallet – 20% of those were men and 12% were women.
Ibid.

■ Millennials are more likely to use mobile wallets – 36% of those are between the ages 18 to 24, and 33% are older millennials.
Ibid.

■ More SMEs (80%) will borrow funds in 2017 as they look to invest in their own companies,
Mercator Advisory Group 2016 Small Business Payments and Banking Survey, PYMNTS.com, *12/27/17*

■ Most SMEs (80%) have a business credit card.
Ibid.

■ Credit card delinquencies increased to 2.74 % in the 3Qtr2016.
CNBC, *1/10/17*

■ Auto loan delinquencies were up to 0.87% in the third quarter from 0.82% in the previous quarter.
Ibid.

■ Home-related delinquencies, including HELOCs and lines of credit, fell in the 3Qtr2016.
Ibid.

Tech *Update*

New Tailgate Alarm Technology

We've all been there before. An auditor visits one of your access controlled facilities, and piggy backs in a door behind a legitimate employee. The next thing you know, your boss is down your throat for failing an access control audit.
Piggy-backing has been a security nemesis for years, and finally, there may be a solution to this dilemma. At the 2016 ASIS Conference and the ISC – East Security Expo, Digital Security Inc. (DSI) exhibited their anti-piggy backing alarm technology that is compatible with most access control systems or available in a stand-alone application.

Designed to monitor door security and prevent forced intrusions, DSI door management products include alarms, pushbuttons, key switches, annunciators and accessories. A wide range of cost-effective, single-door security solutions are available and can be used as standalone devices or integrated into access control systems. Affordable, versatile, and easy to install, the Entry Sentry Tailgate Detection system uses 32 infrared sensors to detect tailgating through any door or hallway. The system includes a built-in door prop timer and a state-of-the-art sounder to set off an alarm when more than one person enters at a time. Entry Sentry can also be configured to trigger local or remote alarms. Its advanced sensor technology recognizes inanimate objects, while adjustable sensitivity helps eliminate false alerts. This smart and simple solution runs on 12 or 24 VDC. With diagnostics to help troubleshoot the access control system and a form "c" relay to control the lock, it integrates easily with other access control systems.

In environments with tighter security requirements, tailgating can pose unnecessary security risks. The DSI Entry Sentry is designed to deter such activity. Using unique algorithms, this solution can allow people with briefcases or pull bags to pass without causing alarms, making it one of the most accurate and cost-effective anti-tailgate devices in the industry. The units can be used to activate peripheral devices, such as, dialers, door locks, and cameras and can be keyed to match a building owner's master key system. The Entry Sentry series is available as both a standard unit (ES5200) and a unit with voice (ES5600).

All of Designed Security, Inc.'s door management products are compatible, complementary components to any access control system. They can enhance the level of security at any door and are visually as unobtrusive as a thermostat on the wall. Designed to eliminate forced-door intrusions or door prop/door held security risks, various alarm models are available to address unique security needs. DSI has the right tools you need to secure critical doors, such as emergency exits, file vaults and secure stairwells. For more information on the Entry Sentry, visit the DSI website at www.dsigo.com.

COMING *Up*

ASIS INTERNATIONAL

Assets Protection Course: Principles of Security (APC 1)
Boston, MA, March 6-9, 2017

ASIS 27th New York City Security Conf
New York, NY, June 7-8, 2017
Info: (703) 519-6200
www.asisonline.org

ASSOCIATION OF CERTIFIED

ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)

ACAMS 5th Annual AML Risk Management Conference
New York, NY, June 9, 2017
Info: www.acams.org

BOL CONFERENCES

BSA/AML TopGun Conference
Scottsdale, AZ, Mar 27-28, 2017
Info: (888) 229-8872 ext 87
www.bolconferences.com

JOHN REID SCHOOLS/SEMINARS

REID TECHNIQUE OF INTERVIEWING AND INTERROGATION
For Loss Prevention and Corp Security Personnel
* Oak Brook, IL, 2/6-2/8/17
* Sante Fe, NM, 2/14-2/16/17
* Kansas City, MO, 2/21-2/23/17
* Southgate, MI, 2/28-3/2/17
* Houston, TX, 3/14-3/16/17
* Little Rock AR, 3/28-3/30/17
* New Orleans, LA, 4/4/-4/6/17
* Philadelphia, PA, 4/10-4/12/17
* St Charles, MO, 4/18-4/20/17

Info: (800) 255-5747
www.reid.com

TRAINING **PAGE**

It's Income Tax Fraud Scam Season

by P. Kevin Smith, CPP

Recently, the Internal Revenue Service joined with representatives of the software industry, tax preparation firms, payroll and tax financial product processors and state tax administrators to combat identity theft refund fraud to protect the nation's taxpayers. These Security Summit partners have issued multiple alerts to taxpayers and tax preparers to be on guard against fake emails and various scams that have surfaced during this income tax preparation season. It would behoove bank security and operations personnel to be aware of these scams, so they may spot abnormal customer activity or respond to customer inquiries.

Tax Preparer Scams

As in the past, the Internal Revenue Service, state tax agencies and tax industry leaders warned tax professionals to be alert to an email scam from cybercriminals posing as clients soliciting their services. A new variation of this phishing scheme is targeting accounting and tax preparation firms nationwide. The scheme's objective is to collect sensitive information that will allow fraudsters to prepare fraudulent tax returns.

In some cases, the phishing emails may appear to come from a legitimate sender or organization (perhaps even a friend or colleague) because they also have been victimized. Fraudsters have taken over their accounts to send phishing emails. The tax professional may think they are downloading a potential client's tax information or accessing a site with the potential client's tax information. In reality, the cybercriminals are collecting the preparer's email address and password and possibly other information.

IRS-Impersonation Telephone Scams

An aggressive and sophisticated phone scam targeting taxpayers, including recent immigrants, has been making the rounds throughout the country. Callers claim to be employees of the IRS, but are not. These con artists can sound convincing when they call. They use fake names and bogus IRS identification badge numbers. They may know a lot about their targets, and they usually alter the caller ID to make it look like the IRS is calling.

Victims are told they owe money to the IRS and it must be paid promptly through a pre-loaded debit card or wire transfer. If the victim refuses to cooperate, they are then threatened with arrest, deportation or suspension of a business or driver's license. In many cases, the caller becomes hostile and insulting. Or, victims may be told they have a refund due to try to trick them into sharing private information. If the phone isn't answered, the scammers often leave an "urgent" callback request.

Surge in Email, Phishing and Malware Schemes

The IRS saw an approximate 400 percent surge in phishing and malware incidents in the 2016 tax season. Scam emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. These phishing schemes can ask taxpayers about a wide range of topics. Emails can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information. Variations of these scams can be seen via text messages, and the communications are being reported in every section of the country.

When people click on these email links, they are taken to sites designed to imitate an official-looking website, such as IRS.gov. The sites ask for Social Security numbers and other personal information, which could be used to help file false tax returns. The sites also may carry malware, which can infect people's computers and allow criminals to access your files or track your keystrokes to gain information.

Email Phishing Scam: "Update Your IRS e-file"

The IRS has also issued warnings about email phishing scams that appear to be from the IRS and include a link to a bogus web site intended to mirror the official IRS web site. These emails contain the direction "you are to update your IRS e-file immediately." The emails mention USAgov and IRSgov (without a dot between "IRS" and "gov"), though notably, not IRS.gov (with a dot). Don't get scammed. These emails are not from the IRS. Remember, the IRS does not initiate contact with taxpayers by email to request personal or financial information.

Tax Refund Scam Artists Posing as Taxpayer Advocacy Panel

According to the Taxpayer Advocacy Panel (TAP), taxpayers are receiving emails that appear to be from TAP about a tax refund. These emails are a phishing scam, where unsolicited emails which seem to come from legitimate organizations — but are really from scammers — try to trick unsuspecting victims into providing personal and financial information. Do not respond or click the links in them.

TAP is a volunteer board that advises the IRS on systemic issues affecting taxpayers. It never requests, and does not have access to, any taxpayer's personal and financial information such as Social Security and PIN numbers or passwords and similar information for credit cards, banks or other financial institutions.

Telephone Scams Are On the Rise

The IRS has seen an increase in "robo-calls" where scammers leave urgent callback requests through the phone telling taxpayers to call back to settle their "tax bill." These fake calls generally claim to be the last warning before legal action is taken. In the latest trend, IRS impersonators are demanding payments on iTunes and other gift cards. The IRS reminds taxpayers that any request to settle a tax bill by putting money on any form of gift card is a clear indication of a scam.

Additional telephone scams include criminals targeting students and parents during the back-to-school season and demanding payments for non-existent taxes, such as the "Federal Student Tax." If the person does not comply, the scammer becomes aggressive and threatens to report the student to the police to be arrested. As schools around the nation prepare to re-open, it is important for taxpayers to be particularly aware of this scheme going after students and parents.

The IRS has prepared numerous alerts and bulletins related to Income Tax season fraud. For additional details on the latest scams and security safeguards, visit their website at www.IRS.gov.

Regulator Reduces Regulatory Burden

As part of its review under the Economic Growth and Regulatory Paperwork Reduction Act of 1996 (EGRPRA), the OCC released its final rule to remove or amend outdated or unnecessary provisions of certain rules to reduce the regulatory burden on national banks and federal savings associations. The final rule, entered into the Federal Register on December 15, 2016 and effective January 1, 2017, affects only OCC regulations and institutions that are regulated by the OCC.

In addition to the EGRPRA final rule, the OCC took action on a final rule issued last year that removed outdated or unnecessary licensing requirements, as well as efforts to streamline Call Report requirements, and an interagency interim final rule that permits more qualifying community banks to be eligible for the 18-month examination cycle. The regulator also recommended legislative changes that would eliminate undue burden, such as a community bank exemption from the Volcker rule and a proposal to provide federal savings associations with greater flexibility to adapt to changing economic and business environments and meet the needs of their communities.

Student Loans in the Spotlight

The CFPB has released a report bringing student loan servicing problems in the spotlight. About 44 million consumers owe money on student loans, and 1 out of 4 student loan borrowers are past due or in default. In the last decade, the number of older student loan borrowers has quadrupled and the amount of debt per older borrower has roughly doubled. Some banks have already taken steps to protect older borrowers and co-signers on student loans. Ten of the nation's largest private student lenders have modified their co-signer rules to eliminate triggers for defaults in the event of a co-signers death or bankruptcy. In some cases, consumers can request that co-signers be released from their financial obligation on a student loan. Financial firms are encouraged to improve the terms of their student loan contract by implementing the changes to auto-defaults and renegotiating loans at a lower interest rate when borrowers are having trouble making payments.

Focus *on Fraud*

NYDFS Issues Cyber Proposal

Following a series of high-profile breaches and escalating cyber threats targeting the financial industry, the New York Department of Financial Services (NYDFS) became the first state in the U.S. to propose cybersecurity rules for its regulated banks and other financial services institutions. Originally proposed in September with an intended January 1 effective date, the state received resistance from industry players who complained that the rules may clash with future federal regulations, and that the rules failed to adequately distinguish between large and small firms. In light of the industry's concerns, the state's financial regulator issued a revised version of the cybersecurity proposal. Key revisions to rules were in the areas of reporting requirements for cybersecurity events, appointment of a chief information security officer and a greater emphasis on entity risk assessments. The rules will require banks, insurance companies, and other financial services institutions regulated by the NYDFS to establish and maintain a cybersecurity program designed to protect consumers and ensure the safety and soundness of the stat's financial services industry. The updated proposed regulation was published on December 28 and will be finalized following a 30-day notice and public comment period. While the rules will only apply to New York-based entities, the regulations are expected to establish best practices in other states, and could prompt the federal government to follow suit with similar proposals in the near future.

ATM Fraud: The Good, the Bad and the Ugly

In the 1966 Clint Eastwood film, The Good, The Bad, and The Ugly, three men searched for hidden loot during the Civil War. Today, a Cyber War is raging and the bad guys are devising new and innovative ways to pilfer loot from banks and bank customers. While New York may be the first state to issue a formal cyber proposal for its regulated banks, every financial entity needs take comprehensive measures to protect their networks and their customers' accounts.

The good news is that a recent annual fraud survey published by the ATM Industry Association (ATMIA) reported a decline in the number of ATM crimes, down from 51% in 2015 to 42% in 2016. ATM crime includes skimming, PIN compromise, cash trapping, dispenser jackpotting, ATM malware, and a wide range of attack vectors. The bad news is – that while the widespread adoption of EMV technology is expected to reduce skimming attacks – fraudsters are resorting to physical attacks and devising new attack methods to pilfer card data at the ATM. One newer method of attack that has emerged is ATM Shimming, which enables fraudsters to capture EMV or chip card transaction data using a shimmer device inserted into an ATM to intercept data exchanged between the EMV card and card reader. The stolen data is then used to create fraudulent magstripe cards. Cardless technology is also being deployed by banks to help mitigate fraud at the ATM. Acountholders can withdraw money using just their mobile phones, without the need to carry or insert a card. But, a recent case involving a Chase Bank customer who's EMV card was compromised revealed that technology that relies on a pin, phone and a password has its own inherent security flaws.

The ugly truth is that ATM crime remains a prevailing threat for banks and their customers. To mitigate these attacks, financial institutions need to have effective real-time solutions in place to prevent these persistent attacks, and stay informed on emerging threats to ensure that they have the right technologies and solutions in place to stop them. Educating consumers on security best practices will help keep your customers safe when conducting transactions at your ATMs.

Wartime Tech for Card Encryption

The very technology that has been deployed to protect cardholders has actually triggered a virtual crime wave. With EMV deployment becoming more widespread, criminals have beefed up their efforts to exploit old magnetic stripe cards while they can, stealing a record estimated $4 billion in 2016. An update to World War II technology that was used for deciphering foreign traffic is being patented by Barclays Bank to deploy new bank card encryption technology in the fight against card fraud. The new card encryption technology will replace the three-digit code on the back of cards that's been in use for the last 20 years. Users will simply enter their PIN on a keypad on their card to generate a one-time code that will be displayed next to the signature line, preventing theft from compromised cards and skimmers.

From the Editor

A Lesson from Hollywood

by P. Kevin Smith, CPP

I love going to the movies. It's one of my favorite things to do in life. I used to go primarily for the popcorn, especially since our theater offers self-serve butter, or I should say "butter like substance." On January 1st of each year, I purchase a large popcorn bucket (filled) for $19.95, and each time I return throughout the year, I get a popcorn bucket refill for $4.00. My wife waits around the corner for me to dump some of it into her little empty whip cream container, but there's still plenty for me to gorge on throughout the movie.

Maybe I'm getting too old, but lately I've been enjoying the movies just as much as the popcorn. The movies are not just entertainment for me. Some of them actually stimulate my mind when it comes to crime prevention or investigative techniques. Take a recent release for instance: Patriot's Day, which is the story about the Boston Marathon bombing. The film stars Mark Wahlberg, and it portrays the horrible tragedy from the perspectives of the victims, the first responders, and the investigators. Now you may be thinking, "What in the heck does this movie review have to do with bank security?" Well, once you see the film (and I highly recommend it) you will realize that the Boston Marathon bombing might not have been solved (and many more people would have died) were it not for the use of private sector video surveillance systems.

Once the injured parties were removed from the scene, the FBI took charge of the investigation, and relocated all of the evidence to a nearby warehouse, where they recreated the bomb scene and a six block surrounding area. They began looking at video evidence captured from cell phones and nearby stores, and they finally found an image of a suspect walking away from the area where one of the bombs exploded. With that image, they asked a police officer (Wahlberg) familiar with the area to identify other stores that might have video surveillance systems of value. Wahlberg stood in the center of the reconstructed bomb scene and began to rattle off additional stores that might have video coverage of the area leading to the bomb site. As he called out the names of the stores, agents accessed the various video systems and pieced together the suspect's movements prior to the bomb detonation. He was seen on video meeting a second suspect, who turned out to be the original suspect's brother. All of this video reconstruction led to the apprehension of the two brothers within 85 hours of the bombing as they were headed for New York City with additional bombs in their car.

Unfortunately, we in bank security have a tendency to focus on the inside of a branch, when it comes to video surveillance. It's true that many crimes have been solved through the use of exterior ATM video cameras, but let's face it, most of them are really transaction cameras that happen to capture an image in the background or a suspect eventually using an ATM (which also happened in the Boston Marathon bombing). But, for the most part, we typically employ cameras depicting shots of the branch interior (teller stations, back room, vault, etc.). Some banks still employ a single exit camera, which is somewhat useless, since they only capture a blurry image of a suspect running out the door. Those of us old enough to remember understand that exit cameras were once necessary because of the 35 mm hard film technology. The cameras were not active until a bill trap was pulled. Today's video technology runs constantly, so entrance cameras are the preferred design application.

My point is that video technology has become one of the most valuable assets to law enforcement in virtually every crime committed on the streets today. Many would say that it's more valuable than eye witness testimony. Patriots Day illustrates that police officers not only canvas an area for eye witnesses, they look for video evidence. It's nice to have interior branch surveillance video, but don't get caught with your pants down by not having exterior cameras. How would you feel (and what would the media say) if you failed to spend a few hundred dollars for parking lot or sidewalk coverage around your branch and a major crime happened in the area. By the way, I gave the movie 4 out of 4 stars.

WAR *Stories*

Quite a Character

Star Wars' most loved (and most feared) villain only made two appearances in the latest sequel of the movie, Rogue One. But Darth Vader was spotted recently in Denver, CO. The Dark Lord held up a UMB Bank branch in Littleton, CO. He fled with the loot after claiming he had a gun and demanding cash. A second bank was later robbed by a suspect disguised as the comic hero Black Panther. The FBI and Denver law enforcement agencies believe it's the same character in both cases and have dubbed him the "Comicon Bandit." They are searching for a 20 – 30 year old white male with short brown hair, approximately 5-foot-10 to 6-foot tall, with a thin build. May the Force be with them and may good triumph over evil.

The Name Game

While bank robberies are no joke – especially takeover-style ones – the FBI gives suspects catchy monikers based on their disguises or unique identifiable characteristics. When a ski mask-clad suspect walked into the Arizona Central Credit Union brandishing a silver handgun, ordered several people to the floor, and demanded money from the tellers, witnesses later recalled a notable trait to pass on to investigators. The bandit appeared to walk with his feet turning inward. Having a little fun with that, the FBI dubbed the suspect the "Packing Pigeon Bandit." In addition to his unusual gait, he was described as a middle-aged white male with an olive complexion, about 6 feet tall, weighing 200 pounds, with salt-and-pepper hair and a mustache, wearing a blue sweatshirt and black parachute pants. While not everyone who walks pigeon-toed is a thief, if your bank is in the Phoenix area and someone comes in matching the suspect's description – and walks funny – contact the FBI's Phoenix Field Office.

So what's in a name? Maybe more than you think. The Phoenix FBI office frequently uses these catchy monikers, which may be one reason that eight out of ten bank robbers (80%) in Phoenix are apprehended and end up in jail.

QUESTIONS & *Answers*

Q. Our security officer mentioned the other day that one of our customers was the subject of a 314(a) request. What exactly does that mean?

A. Well for starters, you should be extremely careful about discussing that information with anyone. A 314(a) request should be treated as highly confidential information that should only be shared with those within your company that have a need to know. Having said that, here's what the FinCEN website has to say about the 314(a) program and process.

FinCEN's regulations under Section 314(a) enable federal, state, local, and foreign (European Union) law enforcement agencies, through FinCEN, to reach out to more than 39,000 points of contact at more than 16,000 financial institutions to locate accounts and transactions of persons that may be involved in terrorism or money laundering. FinCEN receives requests from law enforcement and upon review, sends notifications to designated contacts within financial institutions across the country once every two weeks informing them new information has been made available via a secure website. The requests contain subject and business names, addresses, and as much identifying data as possible to assist the financial industry in searching their records. The financial institutions must query their records for data matches, including accounts maintained by the named subject during the preceding 12 months and transactions conducted within the last 6 months. Financial institutions have 2 weeks from the posting date of the request to respond with any positive matches. If the search does not uncover any matching of accounts or transactions, the financial institution is instructed not to reply to the 314(a) request.

Through an expedited communication system, FinCEN's 314(a) process enables an investigator to canvas the nation's financial institutions for potential lead information that might otherwise never be uncovered. This cooperative partnership between the financial community and law enforcement allows disparate bits of information to be identified, centralized and rapidly evaluated. It is important to note, however, that Section 314(a) provides lead information only and is not a substitute for a subpoena or other legal process. To obtain documents from a financial institution that has reported a positive 314(a) subject match, a law enforcement agency must meet the legal standards that apply to the particular investigative tool that it chooses to use to obtain the documents.

The 314(a) process has proven to be an effective tool in many law enforcement investigations. Results yield productive leads for both terrorist financing and money laundering cases and often lead to the identification of new accounts and transactions. These results enable law enforcement to efficiently direct its use of legal processes to promptly obtain critical evidence to help advance their investigations. Based on the total feedback we have received using the current revised feedback reporting form, 95% of 314(a) requests have contributed to arrests or indictments.

Q. I work for a small bank, and we often hear that our systems might be vulnerable to ransomware cybersecurity attacks. How does a ransomware attack occur and is it a problem unique to smaller banks?

A. While smaller banks might be perceived as more vulnerable, ransomware and other cyber attacks are a problem for all businesses, regardless of size. According to the FBI, who investigates large scale cyber attacks, hospitals, school districts, state and local governments, law enforcement agencies, small businesses, and large organizations are just some of the entities impacted by ransomware – an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them.

The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal and often irreplaceable items – including family photos, videos, and other data – can be devastating for individuals as well.

In a ransomware attack, victims – upon seeing an email addressed to them – will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the email might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins, because of the anonymity the virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam emails, but as email systems got better at filtering out spam, cyber criminals turned to spear phishing emails targeting specific individuals. And in newer instances of ransomware, some cyber criminals aren't using emails at all – they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

The FBI doesn't support paying criminals a ransom in response to a ransomware attack. Paying a ransom doesn't guarantee an organization that it will get its data back. There have been multiple cases where organizations never received the promised decryption key after having paid the ransom. Paying a ransom not only emboldens current cyber criminals to target more organizations, it also offers an incentive for other criminals to get involved in this type of illegal activity. And by paying a ransom, an organization might inadvertently be funding other illicit activity associated with criminals.

WHAT DO *other* BANKERS *do?*

Warm Hearts for Warm Relief

Homeless residents across the Northwest will be warmer this winter thanks to the generous donations from **Columbia Bank**, its customers and employees, and the community they serve. In 2015, the bank launched the Warm Hearts Winter Drive to support nonprofit organizations providing warmth to individuals, families and children in need. Surpassing their 2016 fundraising goal of $160,000 for Warm Hearts and exceeding funds raised in 2015 by more than 30%, $209,335.96 and 8,140 items were raised for 54 local homeless shelters during the second annual Warm Hearts Winter Drive. All of the clothing and funds collected during the campaign are donated to the shelters and relief organizations in the communities where the collections originated.

Funding Financial Empowerment

Summit Credit Union has launched a VISA Global Good Card campaign to help members throughout the world become more financially empowered. Developed in partnership with the World Council of Credit Unions (WOCCU) – which brings access to credit to low-income families and women in emerging countries – the credit union will donate up to $10 for every Global Good Card opened through January 31, 2017. Summit Global Good Card members will also have the option to donate $10 annually, while an additional 20 percent of interchange fees on all purchases made with the card will go to WOCCU.

Helping Heroes Save Lives

In the wake of recent active shooter incidents, **Resource One Credit Union** wanted to help their Heroes in Blue who serve and protect their community. The credit union donated 200 lifesaving tactical medical kits to Dallas County Sheriff's Department. The kits allow officers to be armed with supplies to treat serious injuries when warranted, and can be used to help officers save lives – even their own if needed. While the cost to supply the kits was minimal, if even one life is saved the value is priceless.

Tons of Toys for Tots

For the past five years, **Newtown Savings Bank** has participated in the Marine Corps Reserve's Toys for Toys fundraising campaign that distributes toys to children from low-income families at Christmas. This year, 15 of the bank's branches collected toys and presented the Ridgefield Marine Corps Reserve with a sizeable donation. The bank also held a raffle and used the $200 raised toward purchasing more toys.

A Helping Hand

Joining other local organizations, **Machias Savings Bank** in Portland donated $2,500 of a $8,000 donation that was presented to The Milestone Foundation, a nonprofit recovery center that helps people struggling with homelessness and substance abuse. The bank also donated $2,000 worth of medical scrubs and handwarmers. The scrubs will be used year-round in Milestone's recovery clinic.

AND IN *Conclusion*

"The bank warned us that thieves may disguise themselves as Uncle Sam."

BANKERS' *Hotline*

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.

BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVI NUMBER 12

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.

This issue went to press on December 15, 2016

Traditional Banking: Auld Lang Syne?

by Teri Wesley

As the seasonal song attests – It's the most wonderful time of the year! The time to reflect on the past – how banking has changed this year – and look forward to what lies ahead for the financial industry in the New Year. Some of the most common buzzwords in the industry in 2016 included fintech, blockchain, EMV, and biometrics. What do these trends have in common? They are not only driven by technology, but their primary goal is customer satisfaction. While successful and effective customer relationships have always been a factor in a bank's overall success, notable events and an increased emphasis on meeting the demands of today's tech-savvy consumers have reminded us that the people we serve are at the very core of what we do…and how we do it.

In the past year, we've seen the adoption of EMV technology as magnetic stripe cards were upgraded to EMV chip-enabled cards. In some cases, human tellers have been replaced by interactive tellers. Password authentication is being updated with more secure biometric technology using body parts in lieu of letters and numbers that can be easily guessed by criminals. As technology continues to evolve and become an integral part of everyday life, it continues to shape and transform the relationship banks have with their customers. Knowing how to effectively leverage the treasure troves of data banks have available, with the right systems in place, is the key to providing enhanced customer service and remaining competitive in today's financial marketplace.

Fintech is one of the hottest topics in the industry, and with regulators, as the end of 2016 draws nigh. The Federal Reserve recently published a research paper on fintech and provided some insight into how the nation's central bank plans to monitor financial innovations, such as blockchain. Noting that the distributed ledger technology that underpins bitcoin "is still in its infancy," the paper examined the potential impact of distributed ledger for payments, securities clearing and settlement. The Fed pointed out that a "number of challenges to development and adoption remain, including how issues around business cases, technological hurdles, legal considerations and risk management considerations are addressed."

Last year, technology giants Amazon, Apple, Google, Intuit and PayPal formed a coalition called Financial Innovation Now (FIN) to help foster greater innovation in financial services. Following the historical presidential election in November, the group issued a letter to the newly elected Trump-Pence team calling on the future administration to appoint pro-technology regulators and to develop policies to facilitate the development of, and broad access, to emerging fintech.

(continued on next page)

Final Rule Issued on Insured Deposit Access

by Teri Wesley

On November 15, the FDIC finalized the final rule related to Recordkeeping for Timely Deposit Insurance Determination that will require large banks — those with two million or more deposit accounts — to keep readily available records of their insured deposits. The 38 largest FDIC-insured institutions will have three years (instead of two years outlined in an earlier proposal) to implement the rule and establish recordkeeping requirements and IT systems that facilitate rapid payment (calculating the amount of insured money for most depositors within 24 hours) if the institutions were to fail. The rule goes into effect April 1, 2017.

Auld Lang Syne *(continued from front page)*

And, on December 2, the nation's primary banking regulator, the Office of the Comptroller of the Currency (OCC), announced a proposal to give fintech firms a special purpose charter. In a speech outlining the proposal, OCC Director Thomas Curry said "Technology-based products and services are the future of banking and the economy," and that charters will help fintech providers reach people who are underserved by traditional banking while maintaining consumer protections. If the proposed charters go forward, fintech applicants will be evaluated to ensure they have appropriate risk management controls in place, effective consumer protections, and strong capital and liquidity, and would face regular scrutiny to ensure they are meeting the standards put forth by the OCC. The regulator is accepting public comments on the charter process through January 15, 2017.

In its global predictions for 2017, Forrester Research noted that there is an emerging gap between financial firms that are embracing digital business transformation and those that continue doing business in traditional ways. That gap is expected to widen as leading financial firms experiment with the latest technology to win, serve and retain customers. With the increased focus on fintech, the research company predicts that leading financial providers will partner with fintech firms to build digital banking ecosystems, and that they will enable more open API (application programming interfaces) as they innovate to remain competitive with digital disruptors.

In its *World Retail Banking Report 2016,* global consulting firm Capgemini Group reported that 63.1 percent of consumers around the globe are currently using fintech products or services, with 81 percent of those polled citing that fintechs offer faster services, and 80 percent reporting that fintechs provide a positive experience. Those numbers have financial institutions stepping up their game, either in the development of their own digital offerings or to collaborate with fintechs. The report found that 65 percent of banks see fintechs as partners, only 28 percent view them as competitors, and a mere 7 percent think they are irrelevant.

With the future of banking being propelled by fintech, we could be saying Auld Lang Syne to traditional banking as the industry moves from digital disruption to digital transformation.

IN THE *News*

The FDIC IT Exam

Notably one of the biggest threats to the U.S. financial system, cybersecurity remains in the spotlight in the wake of high-profile hacks and increasing attacks targeting major banks, retailers and government entities. Regulators are stepping up scrutiny of the institutions they oversee.

In the past, FDIC-supervised bank IT exams relied primarily on bank management attestations regarding the extent to which IT risks are being managed and controlled. Today, examiners may give less weight to what bank management attests to concerning cyberattack preparedness, and focus more on how the bank is protecting data from external risks, detecting possible data breaches, and responding to and recovering from an actual breach.

When preparing for an FDIC bank IT exam, there are ten points bank directors should consider:

1. Does the bank have management qualified to oversee all aspects of the its IT operations, including compliance with applicable data security laws and regulations?
2. Is there a designated Vendor Management Coordinator in the bank with an appropriate level of due diligence and experience for the bank's IT services?
3. Do the directors understand what IT services are being outsourced and whether the Bank's Vendor Management Program meets the requirements and guidance of the FFIEC IT Examination Handbook, Outsourcing Technology Services?
4. Does the Bank's Business Continuity Planning/Disaster Recovery Plan adequately address the sudden loss of IT services?
5. When did senior management last review the organization's incident response portion of the BCP/DR Plan?
6. Has the incident response plan been strategically tested?
7. Has the incident response plan been operationally tested?
8. Does the bank have a plan for how it would communicate a breach to its customers, regulators and law enforcement?
9. Has the bank retained cyber insurance coverage? Does management understand what is, and what is not, covered under the policy?
10. Does the organization have external resources already identified, and under contract, to provide assistance in the event of a security incident?

Tools to Help SMBs Succeed

As the New Year approaches, many people take stock of what they have achieved so far and what their future goals are. With the volatile job market, and many positions being taken over by technology, a growing number of Americans are starting their own business. The FDIC and SBA (Small Business Administration) have enhanced their *Money Smart for Small Business* (MSSB) training curriculum for entrepreneurs. In addition to "Banking Services Available for Small Businesses," and other existing topics, three new modules were added to the curriculum on managing cash flow, planning for a healthy business, and helping aspiring entrepreneurs determine if owning a business is a good fit for them. The curriculum is available for download at no cost in both English and Spanish at https://www.fdic.gov/consumers/consumer/moneysmart/business.html

The agencies have also simplified the process for financial institutions and other organizations who want to join the Money Smart Alliance to educate their new, or currently operating, small business customers using the MSSB program.

Financial Resources for Servicemembers

Our active duty military members face unique challenges, such as deployments and frequent relocations, not to mention the requirement to be mission ready at all times. Their financial decisions can have long-term effects on their family life, security clearance, and even mission readiness. The FTC has launched a mobile-friendly financial readiness website to help military members and their families navigate personal financial matters. The site – www.Military.Consumer.gov – contains a toolkit for personal financial managers, counselors, and others in the military community with valuable tips they can share with their military customers, or distribute in newsletters or on social media. The "Tools for Personal Financial Managers" can be accessed directly at www.Military.Consumer.gov/toolkit.

Statistics, *Facts &* Such

■ .Of more than 2,000 U.S. Consumers surveyed, only 36% say their banks exceed expectations. When they report a problem to their bank, only 36% of customers say they receive a response from their bank with a resolution.
PR Newswire, *10/24/16*

■ The most common methods consumers use to report a complaint to their bank is by phone (63%), visiting a branch (40%) and via email (18%).
Ibid.

■ Self-service online and mobile channels are preferred by 68% of consumers. Those in the 21-29 (66%) and 30-39 (60%) age groups are more likely to use mobile apps, mobile web (33% and 32%) and online chat (15% and 11%), compared to customers over the age of 40.
Ibid.

■ Nine out of ten commercial banking professionals in the U.S., Europe and Canada are exploring the use of blockchain technology for payments.
Business Wire, *10/25/16*

■ Nearly a third (30%) of banks are in the advanced stages of adopting blockchain technology for payments, and 70% are still in the early stages of adopting the technology.
Ibid.

■ Regional and community banks ranked the highest in customer satisfaction scores in the retail banking industry, earning a score of 83 out of a 100.
ABA Banking Journal, *11/16/2016*

■ "Super-regional" banks earned a score of 79 points, while nationwide banks landed at 77, up from 72 points the previous year.
Ibid.

■ Of the survey's ten customer experience categories, regional and community banks led the way in all but two — number and location of branches and ATMs. They earned the highest scores for courtesy and helpfulness of tellers and staff (91 points), the speed of in-branch financial transactions (88 points) and website satisfaction (88 points).
Ibid.

Tech *Update*

FBI Unveils NIBRS

On December 12, 2016, the FBI released details on more than 5.6 million criminal offenses reported via the National Incident-Based Reporting System (NIBRS) in 2015. The Uniform Crime Reporting (UCR) Program's latest report, NIBRS, 2015, provides a diverse range of information about victims, known offenders, and relationships for 23 offense categories comprised of 49 offenses. It also presents arrest data for those offense categories plus 10 more offenses for which only arrest data are collected.

Because it offers a more complete picture of crime, NIBRS is slated to become the UCR data standard by January 1, 2021. In his recent memo to UCR state program managers, FBI Director James B. Comey elaborated on the FBI's desire for law enforcement agencies to transition from the Summary Reporting System (SRS) to NIBRS:

"This transition is supported by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB), the International Association of Chiefs of Police, Major Cities Chiefs Association, Major County Sheriffs' Association, and the National Sheriffs' Association, as well as the Executive Branch of our government....By transitioning to a NIBRS-only data collection over the next five years, the FBI will have faster access to more robust data that is necessary to show how safe our communities are and to help law enforcement officials and municipal leaders better allocate resources to prevent and combat crime in their jurisdictions." Director Comey went on to say, "NIBRS is a way in which we can all collect data in a way that we can identify patterns, trends, and help us prevent crime and have thoughtful informed conversations at the national level."

The 2015 NIBRS bank robbery table indicates some surprises in the arrests made by the FBI. Boston tops the list with 41, Miami-40, Chicago-32, Philadelphia-31, Dallas-30, Houston-30, Portland, 29, Charlotte-27, and Detroit-22. Las Vegas, San Francisco, Atlanta, and Minneapolis rounded out the top ten with 17 each.

Obviously, these numbers are significantly different from the Uniform Crime Report data because the NIBRS program is still in its infancy. Perhaps most impactful on the federal numbers is the fact that federal agencies often play a collaborative role with local and state agencies in crime investigations. Because the UCR Program has the "most local reporting" rule, which specifies that the agency involved that is the most local jurisdiction should report the incident to the UCR Program, investigations and arrests that federal authorities have worked on often are reported by a city, county, state, or tribal agency. It may not be the data analysis "Holy Grail", but it appears to be a good start. For details on the 2016 NIBRS Report and methodology, visit the FBI website at www.fbi.gov.

COMING *Up*

ASIS INTERNATIONAL

Assets Protection Course: Principles of Security (APC 1)
Boston, MA, March 6-9, 2017

ASIS 27th New York City Security Conf
New York, NY, June 7-8, 2017
Info: (703) 519-6200
www.asisonline.org

ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)

ACAMS 5th Annual AML Risk Management Conference
New York, NY, June 9, 2017
Info: www.acams.org

BOL CONFERENCES

BSA/AML TopGun Conference
Scottsdale, AZ, Mar 27-28, 2017
Info: (888) 229-8872 ext 87
www.bolconferences.com

JOHN REID SCHOOLS/SEMINARS

REID TECHNIQUE OF INTERVIEWING AND INTERROGATION
For Loss Prevention and Corp Security Personnel
* Dallas, TX, 1/9-1/11/17
* San Diego, CA 1/17-1/20/17
* Denver, CO, 1/24-1/26/17
* Oak Brook, IL, 2/6-2/8/17
* Sante Fe, NM, 2/14-2/16/17
* Kansas City, MO, 2/21-2/23/17
* Southgate, MI, 2/28-3/2/17

Info: (800) 255-5747
www.reid.com

TRAINING
PAGE

Bank Security Case Law Review

by P. Kevin Smith, CPP

Case Details

According to a press release from the U.S. Postal Inspector, the former manager of a Wells Fargo Bank branch in Glendale, CA was recently arrested and arraigned on federal charges that allege he was part of a scheme to launder the proceeds of a mass mailing scam targeting holders of U.S. trademarks. Two other Los Angeles-area men had previously been charged for perpetrating the scam and committing bank fraud in furtherance of the crime.

Albert Yagubyan, 36, of Burbank, pleaded not guilty to charges contained in a second superseding indictment filed on July 14, 2016. The indictment charges Yagubyan with one count of conspiracy to commit money laundering, four counts of concealment money laundering, one count of false bank entries and one count of witness tampering. A trial in the case was scheduled for September 13.

Artashes Darbinyan, 36, of Glendale; and Orbel Hakobyan, 41, also of Glendale, were previously charged in this case. Darbinyan and Hakobyan are charged in the second superseding indictment with conspiracy to commit money laundering. Hakobyan is also charged with three counts of concealment money laundering. Darbinyan is charged with four counts of mail fraud, three counts of aggravated identity theft, five counts of concealment money laundering and one count of bank fraud.

"The new defendant added in this case allegedly used his position of trust at a large financial institution to further a scheme that bilked trademark holders," said United States Attorney Eileen M. Decker. "In addition, the co-schemers used stolen identities to further mask this scheme. Activities such as this scheme threaten the stability of financial transactions upon which businesses depend."

According to the second superseding indictment, Yagubyan was the manager of a Wells Fargo branch in Glendale until October 2015. The indictment alleges that from 2013 to 2015, Yagubyan allowed Darbinyan and Hakobyan to open bogus bank accounts at the Wells Fargo branch through which proceeds of the trademark scam could be laundered in exchange for a share of the proceeds. Darbinyan and Hakobyan deposited checks from the victims of the mass mailing scam into bogus accounts at Wells Fargo, then Yagubyan allegedly instructed Wells Fargo employees to approve withdrawals by Darbinyan and Hakobyan from those accounts, even though the two men were not the signatories on the accounts, according to the second superseding indictment.

Yagubyan is also charged with making false bank entries for allegedly instructing a Wells Fargo employee to open an account for Darbinyan under the identity of another person. The second superseding indictment also charges Yagubyan with witness tampering for instructing a Wells Fargo employee to withhold the truth from federal investigators.

Darbinyan was originally charged in October 2015 with 12 counts of mail fraud and four counts of aggravated identity theft. A first superseding indictment filed in January 2016 charged Darbinyan and Hakobyan each with conspiracy to commit bank fraud and one count of bank fraud. Darbinyan was additionally charged with mail fraud, aggravated identity and money laundering counts.

The indictment unsealed in November 2016 alleges that with Yagubyan's assistance, Darbinyan and Hakobyan were able to launder $1.29 million into gold and cash through Wells Fargo. For a $385 fee, the companies promised to monitor for possible infringement and send reports to the client, court records show. Instead, Darbinyan opened bogus accounts, in which he and Hakobyan deposited or cashed checks sent by the trademark holders, prosecutors allege. "Let this indictment serve as a warning to all professionals, including bank managers, who open bogus bank accounts and launder the proceeds of a fraudulent scheme – you will be held accountable for your actions," said Aimee E. Schabilion, Acting Special Agent in Charge of the IRS-Criminal Investigation's Los Angeles Field Office. "This joint investigation continues to demonstrate our efforts to ensure that our financial institutions will not be abused by those serving their own selfish greed at the expense of others."

Lessons Learned

While we may not know all of the details of the incident, the above case illustrates three very important operational lessons for banks. First it highlights the value of a solid "back office" new account verification program. Using pedigree information (name, address, telephone number, social security number, etc.), a back office software program could do a logical comparison to see if the date of birth is consistent with the social security number, the telephone is consistent with the address, or if the address is logical for the branch location. It might also be used to bounce the information against credit bureau data in search of red flags, or it might be compared to known criminal lists, prohibited lists such as those published by OFAC. The key is that new account verification should always be done by a back office operation. Banks should never rely solely on the discretion of the new account officer (or anyone in that chain of command) to verify the new account information. New account verification should be performed by a fraud prevention team.

The case also illustrates the value of an account monitoring system. When properly tuned, an account monitoring system will signal an alert to money laundering or "out of pattern" behavior. Companies or businesses that make numerous consistent "same amount" deposits should be flagged and investigated immediately. Granted, there are legitimate companies that receive multiple identical deposits, but that activity warrants a follow-up investigation. Here again, you should never rely on the account officer to conduct that follow-up investigation.

Finally, the case illustrates the need for employee education and a whistle blower program. If the employees who were instructed by the branch manager to violate company policies and procedures would have reported the activity to their security or audit departments, this activity might not have continued over a two year period. The Sarbanes Oxley Act requires financial institutions to provide a means for employees to report inappropriate behavior on the part of another employee. While many organizations comply with the letter of the law, some fail to adequately train their employees on their duty and obligation to report employee transgressions.

The Future of the CFPB

The CFPB recently issued its semiannual update of its rulemaking agenda. But, if the banking industry has its way, the consumer watchdog agency may have other things to worry about in the New Year. A coalition of bank industry trade groups – the Consumer Bankers Association, Credit Union National Association, Independent Community Bankers of America, and the National Association of Federal Credit Unions – issued a joint letter to the Senate Banking Committee, calling on Congress to legally change the structure of the CFPB, and to roll back a number of the CFPB's recent and pending regulations on banks and lenders.

The financial industry feels that the Bureau's structure of having a single Director, rather than a multi-member commission, running the agency is unconstitutional and puts too much authority into the hands of one person. The letter follows legal briefs that were filed in support of the CFPB by both lawmakers and consumer advocates, who argued that the Bureau's structure is intended to shield the agency from industry bullying and political whims.

Wanted: Feedback on Cybersecurity Standards

As malicious attacks targeting the financial industry continue to escalate and evolve, regulatory agencies are working hard to ensure the entities they oversee implement up-to-date cybersecurity controls. In October, the three federal banking regulatory agencies – the OCC, the FDIC, and the Federal Reserve – issued an Advance Notice of Proposed Rulemaking (ANPR). The ANPR is seeking feedback and comments from industry players aimed at developing and improving the initial draft proposal, or recommendations against issuing any standards.

Comments can be submitted by January 17, 2017 via email to regs.comments@federalreserve.gov or fax to 202-452-3819. Include Docket number R-1550 and RIN 7100-AE-61 in the subject line.

Start the New Year off by helping to shape the future of proposed cybersecurity standards for banks.

Focus *on Fraud*

Cyber Grinches Stole Millions in 2016

In the holiday classic by Dr. Seuss' "*How the Grinch Stole Christmas,*" the Grinch slithers into the little town of Whoville during the night disguised as Santa Claus, with his dog dressed as a reindeer, and steals presents, trees, and food while the Whos of Whoville are snug in their beds. Like the menacing cave-dwelling green monster, cyber Grinches invaded banks, organizations and social media sites in 2016, and pilfered millions of dollars and terabytes of data as unwitting IT administrators were caught unaware. Over two billion records were stolen in 2016 alone. Highlights from a few of the newsworthy incidents this year included:

- In February, one of the world's largest cyber heists was orchestrated when hackers stole $81 million from Bangladesh Bank using the global financial messaging system, SWIFT. The investigation into the hack recently revealed that some of the bank's officials were involved in the crime.
- In May 2015, the IRS reported that 100,000 American taxpayers had their personal information compromised when the agency's "Get Transcript" system was hacked. In February 2016, the agency disclosed that those numbers had increased to over 700,000.
- In June, $10 million was stolen from a bank in the Ukraine by hackers.
- In August, the personal data – names, emails, telephone numbers, DOBs, passwords – associated with at least 500 million Yahoo user accounts that had been compromised in a breach 2 years ago were up for sale on the dark web.
- And most recently, in November, 20,000 Tesco Bank customers in the UK woke up on a Monday to find their account balances unexpectedly low. The bank confirmed that tens of thousands of its customers' accounts were compromised in just a 24 hour period over the weekend,

Wrap Your Network in Malware Protection

When some of the children of Whoville awoke to find the Grinch in their home, they were lulled back to sleep by a false sense of security when they saw the intruder dressed as Old St Nick. It's during this most busiest time of the year that cyber Grinches prey on unsuspecting victims to distribute their malicious gifts under the guise of legitimate emails and special offers. There are myriad types of malware – but they all have one purpose**:** to infect a computer or network with the malicious intent to steal data or funds. Knowing how hackers operate and the tactics they deploy to gain entry to a device or network are key factors in keeping the nefarious criminals out of your network. In its December edition of FedFocus, Federal Reserve Financial Services provides some key steps your institution can take to keep malware from dampening your holiday spirits. Get the details at www.frbservices.org/fedfocus/

Global Crime Network Dismantled

In the spirit of the "Go Big or Go Home" philosophy, an international law enforcement cyber operation brought home a big win when they dismantled a global crime network that had been operating since 2010. Known as Avalanche, the complex and sophisticated network of computer servers hosted more than two dozen of the world's most malevolent types of malicious software as well as several money laundering campaigns.

Targeting not just the individuals involved, but the entire infrastructure behind the operation, a multinational law enforcement coalition, with the cooperation of 40 countries, took down the crime network in an operation that was unprecedented in its scope, scale, and reach. The operation also successfully redirected traffic from infected victim computers intended for the criminals' servers to servers controlled by law enforcement. They found more than 800,000 malicious domains associated with the network that the criminals used to funnel information, such as sensitive banking credentials, from the victims' malware-infected computers through the layers of Avalanche servers and ultimately to the cybercriminals.

The Avalanche network was estimated to serve clients operating as many as 500,000 infected computers worldwide on a daily basis. The monetary losses associated with malware attacks conducted over the Avalanche network are estimated to be in the hundreds of millions of dollars worldwide. More exact calculations are difficult due to the high volume of malware families found on the network.

From the Editor

Don't Forget Mom & Pop

by P. Kevin Smith, CPP

In this tech-savvy world, those of us in the security field have a tendency to focus on phishing attempts, data breaches, and internet fraud, and it seems as if good old fashioned "mail fraud" is nothing but a faded memory. After all, why would criminals waste the cost of postage when they can reach thousands of people with the click of a mouse?

Even the postal inspector's staffing levels indicate mail fraud is a forgotten crime. In fiscal year 2014, the USPIS had 2,376 field employees, a decline of 44.7% from fiscal year 1995 (this figure excludes headquarters staff). In 2008, the U.S. Postal Inspection Service had 2,288 full-time personnel with the authority to make arrests and carry firearms on duty. This represented a 23.1% drop over the previous five years. Unfortunately, while the investigative resources have declined, mail fraud continues to be a significant problem. According to a recent USPS publication, Postal Inspectors reported over 5,500 arrests and about 5,000 convictions related to postal crimes, primarily those involving mail theft, fraud and prohibited mailing in 2015. 35,000 counterfeit postal money orders with a face value of nearly $34 million and another 4,200 counterfeit financial instruments (such as checks), with a face value of about $6.4 million, were identified and seized by Inspectors last year alone. Not surprisingly, the vast majority of those victims were over the age of 65. You see, not all senior citizens have fully grasped the internet lifestyle. Sure, they may do Skype with the grand kids or read an occasional post on Facebook to keep track of their relatives, but many of them still rely on newspaper ads and the plethora of sales circulars that keep the US Postal Service afloat, for their shopping tips and bargain alerts. With all of those seductive marketing brochures being delivered to the door of a lonely soul who looks forward to reading the mail, it's no wonder mail fraud has continued to flourish.

An elderly neighbor of mine (Joe) recently received a postcard from the Notification Warehouse Center, with no return address. It was the "last effort," officially notifying the 80-year old Florida resident that a "package containing jewelry worth approximately $297 was on hold for him in a secured warehouse." Joe had 10 days to call a toll-free number and claim it. There was a $12.95 cost for shipping and handling, payable by credit card. Curious, Joe made the call, but he said it all "sounded suspicious," so he hung up. Knowing that I was a former "security guy," he gave me the postcard and asked me to check it out. When I called, I was told that I had reached a call center in Portland, Maine. The jewelry item was a pearl pendant necklace that was an appreciation gift from a company with whom I had done business. When I offered to pay by check instead of a credit card, the call center operator refused and hung up. Without the ability to vet the company or process, at best this appears to be a possible deceptive marketing effort for a monthly jewelry club, or at worst, it could be mail fraud.

Postal Inspectors arrest more than 1,000 suspects each year for fraud conducted via the mail, and the Postal Inspection Service is just one of many federal agencies that target this type of criminal activity. Although people 60 and older account for 26 percent of all telemarketing fraud victims, 60 percent of people in that age group are victims of prize or sweepstakes fraud. That number may sound high, but the actual figure is probably even higher. Victims of prize or sweepstakes fraud often never report it to authorities. It can be embarrassing, even humiliating, to admit you've been had.

While it may not be a legal requirement, security representatives and branch employees have a moral obligation to protect their elderly customers from these unscrupulous criminals, who prey on the gullibility of senior citizens. Help your elderly customers understand the risks they face as they grow older. Don't give up on statement stuffers, "take-one" pamphlets in the branch, or even brown bag sessions, where you invite local law enforcement officers to present elderly crime prevention tips. A quarterly tea and cookie session goes a long way toward improving customer relations. Preventing financial crime is not all about virus detection software and passwords. That may be the case in 10-15 years, but for now, don't forget Mom & Pop.

WAR *Stories*

No Way to Get Away

Who robs a bank without lining up a getaway vehicle ***before*** the heist? Elias Chapanoff apparently. Chapanoff, 53, entered a Wells Fargo Bank branch in Pasco County, FL, stated that he had a gun in his shirt, and demanded cash. When he tried to flee the scene of the crime, he asked a woman sitting in her car to "get him out of here." When she refused and put her window up, he tried to illicit the help of another driver by threatening him with his non-existent gun. Police arrived before he could get in the car and arrested him after a brief chase.

Quit When You're Ahead

Joshue Flores hit an M&T Bank in Peekskill, NY, took an undisclosed amount of cash, and got away. Instead of stopping while he was ahead, Flores decided to try his luck a second time at a local supermarket later that same day, where he threatened the cashier with a firearm and demanded all the money in the register. He fled the store without any cash. Investigators identified Flores after circulating his photo in the media and throughout local businesses. They found him later than evening hiding in a brook near the supermarket. Flores was charged with robbery in the first degree, one count of third-degree attempted robbery, and grand larceny in the fourth degree.

Returned to the Scene of the Crime

An (unidentified) man in a black sweatshirt entered a Key Bank branch in Everett, demanded money and took off with his loot. But a dye pack the teller had placed in the stash exploded as the thief was making his escape. The explosion ignited a small fire in the bag that spread to his jacket, so he threw the smoking bag into some bushes. Witnesses called police to report that he was back less than two hours later, trying to retrieve the bag. With smudges on his hands and smelling like fire, he denied any involvement in the robbery when he was arrested. He went to jail anyway where he was held on suspicion of first-degree robbery…and second-degree stupidity.

QUESTIONS & *Answers*

Q. It seems like every day we hear about another cyber security incident against a government agency or a private company. Who actually investigates these incidents and is there a coordinated effort to do so?

A. While most incidents are reported at the local level (mainly because most businesses don't know where or how to report a cybercrime), the FBI has taken a lead role in cybercrime investigations through its iGuardian program. With cyber threats continuing to emerge at the forefront of the FBI's criminal and national security challenges, engaging public-private partners in information exchange alongside law enforcement and intelligence communities is critical. To bring trusted industry partners into the intelligence fold, the FBI has adapted its Guardian threat tracking and management system to include iGuardian – a secure information portal allowing industry-based, individual partners to report cyber intrusion incidents in real time.

The iGuardian portal is an evolution of eGuardian, the platform through which the FBI's law enforcement partners provide potential terrorism-related threats and suspicious activity reports. While eGuardian enlists law enforcement users, iGuardian was developed specifically for partners within critical telecommunications, defense, banking and finance, and energy infrastructure sectors and is available over the sensitive but unclassified InfraGard network.

Comprised of thousands of vetted, industry-aligned members nationally, InfraGard is the FBI's public-private infrastructure protection coalition. The organization maintains its own secure network to distribute FBI alerts and bulletins and allow sharing of key threat information across its membership. Using the iGuardian system, members are encouraged to submit intrusion specifics directly to the FBI, including detail regarding malware infections, website defacements, and denial of service attacks. The iGuardian program likewise affords InfraGard partners access to information and intelligence derived from related incidents.

Each iGuardian incident report is expedited through Guardian to CyWatch, the FBI's 24/7 cyber operations center, where agents and analysts triage and de-conflict the input, notify previously unknown intrusion victims, and assign leads to appropriate field offices for further investigation. This centralized management of criminal and national security cyber incidents positions the FBI to work more effectively with our partners to leverage known intelligence and forward pending investigations and operations.

Q. One of our customers said that since the election, she has been inundated with offers for cut-rate supplemental health insurance. Is this a new trend in the fraud schemes we've seen on the internet?

A. Health care scams are not really new, but the fear of Obamacare being repealed has expanded the pool of victims. The US Postal service offers the following on their website. Senior citizens, perhaps more so than any other group of people in America, are aware of the high cost of medical care. While Medicare does cover many bills, it does not pay for everything. Seniors, who generally live on fixed incomes generated by Social Security, interest, and small pensions, sometimes buy supplemental insurance to pay for medical expenses not covered by Medicare.

There are sources for legitimate supplemental medical insurance. However, some policies offered to seniors through mailed advertisements and in other ways are offered by unscrupulous companies and salesmen who will try to sell anything they can, whether there is a need for it or not. Such policies will provide inadequate or inappropriate coverage. One 93-year-old woman thought she was purchasing a valuable health insurance policy, only to learn that she had bought maternity insurance.

Help your senior customers reduce their chances of falling victim to health insurance fraud by reminding them to read sales promotions they receive in the mail, including the "fine print" in the policy. And to be suspicious if a company requests that they pay their premiums in cash, pay a year's premium in advance, or pressures them to buy immediately because "it's your last chance," or wants them to sign a blank insurance form.

Inform them to be cautious about companies that offer policies that will protect them and their loved ones for "only pennies a day." Such low premiums will be effective only for a short time (usually 30 days); thereafter, the premium will increase dramatically. They may also find they have purchased a policy which does not include the kind of coverage they need. They should be careful if a company uses a name which suggests it is connected with the federal government, the Medicare program, or a well-known company. Unscrupulous companies will choose titles, business addresses, and stationary styles purposely to mislead them into thinking they are purchasing something of value from the government or a respected private company.

If they have any doubts about a health insurance policy that someone is trying to sell them, encourage them to discuss the offer with a knowledgeable friend or relative or with an accountant, attorney, or other trusted advisor. They should also notify their local postmaster or the nearest Postal Inspector about deceptive health insurance promotions received through the mail so action can be taken to prevent other people from getting taken. These are excellent recommendations for branch personnel to convey to anyone that expresses a concern about health care fraud, especially for older customers.

Q. I've heard the terms BEC and EAC used when discussing the act of hacking emails. Could you please explain the difference between these two types of crimes and what are the chances of making a recovery in these scams?

A. BEC stands for Business Email Compromise and it targets a financial institution's commercial customers. EAC stands for Email Account Compromise, and it targets a victim's personal accounts. BEC and EAC schemes are the methods used by criminals to compromise the email accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds. Since 2013, there have been approximately 22,000 reported cases of BEC and EAC fraud involving $3.1 billion. While the recovery of BEC stolen funds is not assured, the chances of recovery are enhanced when victims or financial institutions report unauthorized wire transfers to law enforcement (FinCEN) within 24 hours. For more details on this activity, visit FinCEN's website and check out FinCEN advisory #FIN-2016-A003, dated September 6, 2016.

WHAT DO *other* BANKERS *do?*

A Festive Way to Fight Cancer

Customers and employees at **Paducah Bank** have a festive way to support those in their community who have or are battling a devastating disease. The bank partnered with Baptist Health Foundation Paducah for its third year this holiday season to help fund the Foundation's provision of services and support to cancer patients. For a minimum donation of $5.00, bank customers and employees can customize a tree ornament in honor or memory of a loved one to be hung in any of the bank's five branches. The bank has donated more than $3,000 from ornament sales to date. The Baptist Health Foundation Paducah was established seven years ago and to date has raised more than $3.3 million to support cancer patients and their families.

Toys for Sick Tots

A California credit union's internal fundraising efforts, and its collection of toys from customers throughout its 11 branches, will brighten the spirits of pediatric patients at Rady Children's Hospital. The **Pacific Marine Credit Union** (PMCU), an annual sponsor and supporter of AJ's Kids Crane – a local event that directly benefits the children at the hospital – presented a $22,500 check to a local radio station to purchase toys for the children at Rady Children's Hospital. The amount of the donation was not only a new record for PMCU, but was also the largest monetary donation even presented to AJ's Kids Crane. Now in its eighth year sponsoring this event, PMCU has raised over $90,000 to provide toys for sick tots.

Wreaths to Remember

Wreaths Across America is a national movement to honor our fallen military heroes during the holiday season with wreaths placed at veteran cemeteries throughout the country. This year, thanks to a generous donation from **First Arkansas Bank & Trust**, every headstone at the Arkansas State Veterans Cemetery in North Little Rock, AR will be covered with a wreath. The bank's $16,000 donation to Arkansas Run for the Fallen went toward the purchase of 5,100 wreaths that will be placed at the cemetery and its columbarium during this year's ceremony on December 17.

Good Deeds for Those in Need

Some friends in need in Springfield, IL will have a brighter Christmas this year thanks to the Friend-in-Deed campaign that provides Christmas meals to area families. **Marine Bank** and **Illinois National Bank (INB)** joined with local businesses that donated to the campaign this year. Marine Bank raised $532 during one of their monthly casual day fundraisers, and INB contributed $624 to the charity through its Touchdowns for the Table initiative and employee donations. The families who benefit from the campaign receive a food basket just before Christmas that contains all the ingredients for a holiday meal.

Since its inception in 1960, Friend-in-Deed has raised more than $8.35 million and helped more than 75,000 families in the Springfield area and surrounding communities.

AND IN *Conclusion*

2017 Federal Reserve Bank Holidays

Date	Day of Week	Holiday
January 2	Monday	New Year's Day
January 16	Monday	Martin Luther King, Jr Day
February 20	Monday	Presidents' Day
May 29	Monday	Memorial Day
July 4	Tuesday	Independence Day
September 4	Monday	Labor Day
October 9	Monday	Columbus Day
November 11*	Saturday	Veterans Day
November 23	Thursday	Thanksgiving Day
December 25	Monday	Christmas

** Holidays falling on Saturday, Federal Reserve Banks and Branches will be open the preceding Friday. However, the Board of Governors will be closed. Holidays falling on Sunday, all Federal Reserve Banks and Branches will be closed the following Monday.*

BANKERS' Hotline

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.

BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVI NUMBER 9

WHAT'S INSIDE

BANKERS' Hotline (ISSN 1046-1728) is published 12 times a year by Bankers' Hotline, PO Box 1632, Doylestown, PA 18901. $249/year.

This issue went to press on September 27, 2016

Change is in the Air

by Teri Wesley

Summer has ended, kids are back in school, campers are closed up for the season, and temperatures are cooling off in many regions. In our nation's capital, however, things are heating up as the presidential election draws near. Not only are the democratic and republican parties battling it out for that coveted seat in the Oval Office, but the left and right wings are at odds over legislation that could revamp the federal government's approach to regulating banks. On September 13, a House committee approved legislation for a bill written by Chairman Rep. Jeb Hensarling (R., TX) that would essentially replace the Dodd Frank Act. The proposed bill, known as the Financial Choice Act, contains dozens of initiatives to eliminate core elements of the Dodd-Frank law, including limiting the CFPB's power to penalize institutions for "abusive practices." It would also replace the Bureau's sole director with a five-member bipartisan commission and a budget subject to congressional appropriations. In his opening statement at the hearing, Hensarling said the bill offers "true consumer protections so that our consumer agency will enforce the law and not actually make it up." Small community banks and credit unions would gain some relief from regulatory oversight, said Hensarling, specifically reporting requirements. Under the new bill, the NCUA would take on new obligations to assist in managing and reporting credit union performance.

The House's vote to pass this controversial bill came on the heels of one of the nation's biggest banks getting hit with $185 million in civil money penalties (CMP) for illegal sales practices that included bank employees opening as many as two million deposit and credit-card accounts without customers' knowledge. Wells Fargo Bank encouraged sales of new accounts and services in a program that established sales goals and bonus incentives, which led to a widespread employee practice that boosted sales figures by opening deposit and credit card accounts without customer authorization.

(continued on next page)

FTC Seeks Input on Safeguards Rule

by Teri Wesley

The Standards for Safeguarding Customer Information regulation (16 CFR Part 314, the "Safeguards Rule"), which took effect in 2003, requires financial institutions to develop, implement and maintain a comprehensive information security program for handling customer information. For purposes of this Rule, a financial institution is "any institution the business of which is engaging in financial activities as described in section 4(k) of the Bank Holding Company Act of 1956." Any institution that is significantly engaged in "financial activities" qualifies as a financial institution; however, the term "financial activities" is currently limited to those activities that are truly financial in nature, and excludes activities that are incidental or complementary to financial activities. The Federal Trade Commission is seeking input on the scope of the Rule; particularly the definition of "financial institution" and whether to amend the Rule to include "incidental" activities or activities that were determined to be financial in nature after the GLBA was enacted. The agency has published a list of five specific issues on which they request comment. Comments may be submitted online by November 7, 2016 at https://ftcpublic.commentworks.com/ftc/safeguardsrulenprm

Change is in the Air
(continued from front page)

In addition to the CMPs, the bank will issue about $2.5 million in restitution payments for failing to monitor and control its cross-selling incentive program. Neither admitting or denying the allegations, the bank has agreed to the fine and a consent order settling civil claims brought by the Office of the Comptroller of the Currency (OCC), the Consumer Financial Protection Bureau (CFPB) and a Los Angeles attorney. About 5,300 employees involved in the scheme have been fired over the last few years, according to the bank.

The Wells Fargo case was a recurring theme throughout the committee's session. Democratic lawmakers argue that the bank is a prime example of why the CFPB was given the authority to go after abusive practices and that doing away with the Dodd-Frank Act to replace it with this bill would make it easier for banks to abuse consumers. Hensarling was criticized by the democratic members for failing to call a hearing to examine Wells Fargo's sales tactics. Mr. Hensarling responded in a written statement that his bill "holds Wall Street accountable with the toughest, strongest, strictest penalties ever – far greater than those in Dodd-Frank. And as recent headlines attest, obviously stronger penalties are needed." Following the hearing, he further indicated that the panel would be looking into the bank's practices.

The CFPB wasted no time in posting a blog to let consumers who were harmed by any unauthorized Wells Fargo accounts know where they could go to complain...er, we mean, get help if they were one of the unfortunate ones who incurred fees as a result of an unauthorized Wells Fargo account. The CFPB cautioned the bank's customers to always closely monitor their accounts to check for any unauthorized products or account activity, and to contact their financial institution immediately if they suspect that they had an unauthorized account opened. If the consumer continues to have an issue, they are directed to submit a complaint to the CFPB.

Industry associations that represent small institutions, i.e., the American Bankers Association and the Independent Community Bankers of America, have endorsed the bill, welcoming efforts to remove regulations that are particularly costly to smaller banks.

IN THE *News*

Tracking Bandits – There's an App for That!

If the infamous Bonnie and Clydes, John Dillingers and Willie Suttons were pulling off their prolific crimes in today's digital age, their careers might have been short-lived and far less profitable. Most-wanted posters that used to hang in local post offices were upgraded in 2012 with the FBI's Bank Robbers website featuring a gallery of unknown bank robbery suspects wanted by the Bureau. Now, when financial institutions and law enforcement agencies want to view photos and information about bank robberies and the most wanted in their region, there's an app for that. Bank robberies can be sorted by the date they occurred, the state they took place in, the category they fall under (i.e., armed serial bank robber), or the FBI field office working the case. Users can even view a map that shows the bank robberies that took place in their geographic area. Surveillance photos, physical description information, robbery details, and the FBI's wanted poster for each suspect can also be accessed via the app. Available for Apple and Android devices, the app is free at Apple's app store or Google Play.

The Fed on Facebook

Jumping on the social media bandwagon, the Federal Reserve Board launched a Facebook page in August. The intended goal is to increase "the accessibility and availability of Federal Reserve Board news and educational content," and to better inform Americans about who they are and what they do. While the Board's website remains its primary channel of communication and selected announcements will be available on the website before posting to Facebook, they will share press releases, speeches, reports, educational materials, frequently asked questions, and more with their followers. The Fed reported that in its first week, the page reached more than 100,000 people and increased traffic to their website. Not all the feedback was positive, however. Critics of the Board were quick to post unfavorable comments about the organization. The Fed says they are reading the comments and will respond to selected posts with additional information to address common questions.

In the Aftermath of a Disaster

The arrival of fall is welcomed after a summer with unrelenting heat and massive floods that killed hundreds of people and caused more than $50 billion in losses around the globe. The insurance industry reported that from June to August, there were at least 10 different weather disasters that each caused more than $1 billion in losses. Regulators encourage financial institutions to work with affected borrowers and other customers in the wake of a major disaster. These efforts may include waiving ATM fees, waiving account overdraft and late fees, easing restrictions on availability of check cashing, offering extended payment due dates, etc. When Hurricane Hermine hit the East Coast, the OCC issued a bulletin on "Supervisory Guidance on Natural Disasters and Other Emergency Conditions" to provide guidance for banks with customers in areas affected by the storm. When residents of Louisiana were hit hard by catastrophic flooding, the FDIC issued guidance to provide regulatory relief to financial institutions and to facilitate recovery in those areas greatly impacted by the flooding. In addition, HUD accelerated federal disaster assistance to the state to provide support to homeowners and low-income renters forced from their homes. Americans who have lost homes and belongings or are otherwise impacted by floods and other natural disasters are particularly vulnerable to scammers who exploit these tragedies. Charity scams that appeal to the generosity of others who want to help are particularly common. The FTC provides tips and links to resources assist victims dealing with the aftermath of a flood and avoiding flood-related scams. Make sure your customers know how you can help them during the recovery process and other resources that are available to them at www.consumer.ftc.gov

Consumer Tips on Account Management

Providing your customers with financial management resources can enhance loyalty, increase revenue, and prevent losses incurred as a result of unpaid overdrafts and fraud. The FDIC's Summer 2016 edition of the FDIC Consumer News provides tips for consumers on choosing and managing the right deposit account as well as avoiding credit and debit card fraud. You can drive more customers toward your digital offerings with articles on remote deposit capture. There are also suggestions for consumers on how to prepare financially for natural disasters. Get the latest issue at:www.fdic.gov/

Statistics, *Facts & Such*

■ Visa reports that chip cards outnumber U.S. residents at 326 million vs. 324 million, respectively;
ATM Marketplace, *7/26/16*

■ One in four dollars spent in stores with Visa was spent with a chip card used at a chip terminal
Ibid.

■ Counterfeit card fraud fell 35% in March (compared to March, 2015) at chip card-ready merchants.
Ibid.

■ CEOs (81%) in the automotive, banking, technology and retail sectors report that their companies had been compromised by cyber-attacks in the past 24 months – ranging from malware and botnets to other attack vectors.
Help Net Security, *7/27/16*

■ Retail cyber executives (89%) reported the most breaches in the past 24 months, followed by automotive (85%), banking and technology (76%.)
Ibid.

■ Only 49% of executives have invested in IT security in the past year. Banks topped the list (66%), technology was next (62%), retail at 45% and automotive at just 32%.
Ibid.

■ Reputation (53%), financial loss (50%) and job security (49%) were the top concerns of ramifications cited by security executives associated with falling victim to cyber-attacks
Ibid.

■ There has been a 172% increase in ransomware and $3 billion in losses due to business email compromise (BEC) scams so far in 2016, compared to 2015.
Help Net Security *8/25/16*

■ The FBI listed more than 22,000 BEC victims in 2016 to date.
Ibid.

■ There were 79 new ransomware families identified in the first six months of the year, which surpasses the total number found in all of 2015. Both new and old variants caused a total of US $209 million in monetary losses to enterprises.
Ibid.

Tech *Update*

Same Day ACH is Here

On September 23, NACHA implemented Phase 1 of the Same Day ACH processing, which includes credits only with funds availability at end of the Receiving Depository Financial Institution (RDFI) processing day. Same Day ACH processing is automatically available to all network participants and does not require any form of registration or sign up. Banks, especially those with multiple systems, and vendors will need to adjust processes and systems to meet new windows if they have not already done so. On September 16, the Federal Reserve Bank Services issued frequently asked questions on Same Day ACH. Just a sampling of some of the questions that are addressed in the FRB's FAQs include:

Same Day ACH Transaction Transmission and Settlement

- Will Same Day ACH transactions be included with non-Same Day ACH transactions in the outgoing file transmissions?
- Will the same file identification modifiers be used for outgoing files, as is currently done? (updated as of September 16, 2016)
- Can a customer expect its output files to be delivered with sequential file ID modifiers (e.g., A, B, C, D)? (new as of September 12, 2016)
- Will the Fed include an identifier to distinguish in which settlement window the transactions will settle?
- Will there be any new outgoing files distributed as a result of Same Day ACH? (updated as of August 29, 2016)
- Will an ODFI be allowed to request an extension on the Same Day ACH deadlines?
- Will the return deadlines be changed to sync with Same Day ACH deadlines?

Overall Edits and Reject Process

- What will the operator process look like for editing and rejecting batches/files?
- The ACH Rules specify that an optional indicator (company descriptive date field of the batch header record) can be used by the originator to inform the ODFI of its desire to settle the batch same day. Will the operators edit this field?
- The ACH rules specify that a return entry must not settle prior to the settlement of the corresponding forward entry. Do the operators ensure that this does not occur?

Value-Added Services

- How does the FedACH Risk® Origination Monitoring (FROM) Service function with Same Day ACH for transaction monitoring and risk mitigation?
- How does the FedPayments Reporter service complement Same Day ACH for reporting and reconciliation?
- How does the FedACH Risk RDFI Alert Service complement Same Day ACH for transaction monitoring and risk mitigation?

The complete list of questions and more information is available at:
https://www.frbservices.org/help/same_day_ach.html

COMING *Up*

Bankers Hotline 22nd Annual Security Officers Workshop
Philadelphia, PA, October 5-6, 2016
(optional pre-workshop October 4, 2016)
Attend In-Person at the Philadelphia Airport Marriott or via Remote Streaming
Registration remains open up to the day of the conference!!
www.bolconferences.com/sow/

BOL CONFERENCES

Lending Compliance Triage Conference
Scottsdale, AZ, Dec 6-7, 2016

BSA/AML TopGun Conference
Scottsdale, AZ, Mar 27-28, 2017

Info: (888) 229-8872 ext 87
www.bolconferences.com

JOHN REID SCHOOLS/SEMINARS

REID TECHNIQUE OF INTERVIEWING AND INTERROGATION
For Loss Prevention and Corp Security Personnel
* Baltimore, MD, 10/24-10/26/16
* Reno, NV, 11/1-11/3//16

Info: (800) 255-5747
www.reid.com

TRAINING
PAGE

Laptop Theft Prevention

by P. Kevin Smith, CPP

According to the Gartner research firm, a laptop is stolen every 53 seconds. Recent police statistics suggest a vast majority of these are stolen from bars or public transportation venues. "The reality is that there is a burgeoning market for stolen laptops," says Raj Samani, European CTO for Intel Security. "The goods go to pawn shops or unsuspecting people purchasing electronics from the internet in the majority of cases. It's much less common for a thief to be specifically interested in your data." While lap-top theft is indeed a traumatic personal experience, it has become a significant risk for corporations as well.

A comprehensive and converged physical, procedural, and information security program is essential for every organization, regardless of size, industry, or ownership. And part of that program must address laptop security and the related loss of potentially sensitive data. Implementing the appropriate security measures requires money, time, and effort. Companies must be committed to supplying all three, and management must realize that a lack of funding is a serious impediment to a comprehensive protection program. Many companies have implemented successful strategies, but research shows that those who have failed to do so lack a formal security program that is embraced by all employees, including laptop users, management, and security professionals from both physical and electronic disciplines.

Seven Steps to Laptop Theft Prevention

Two distinct yet overlapping issues require attention from security professionals. First, the laptop itself must be protected. And second, the information on the laptop must be secured. These two goals can be achieved and implemented by adopting the following seven steps:

Step 1: Conduct an audit to determine where laptops are used within the organization. This audit determines specific information about a company's laptops, such as where they are being used in the organization, how many are in the inventory, who is using them, for what purpose, and what type of data is residing on each one.

Step 2: Determine whether specific employees need a laptop to do their jobs. If a laptop is not required, it should be replaced with a desktop unit. If the laptop is an essential part of the employee's work, the next steps should be pursued.

Step 3: Classify data on the laptop according to organizational guidelines. The classification scheme should be specific to the organization and its culture. A number of classification models are available. The one selected should be clearly understood, implemented, and followed by all employees.

Step 4: Determine if data residing on each laptop is necessary for employees to complete their jobs. If not, the data should be removed. If the data is necessary, the next step should be pursued.

Step 5: Conduct a risk assessment to determine possible theft scenarios for the data stored, processed, or transmitted by laptop. Devise appropriate security measures to protect both the data and the laptop. The assessment puts the required physical, procedural, and electronic security measures into perspective, as well as the necessary security awareness training. Obviously, the higher the classification of the data, the more security measures should be in place. A number of risk assessment methodologies are available. For example, the American Society for Industrial Security International (ASIS) has published a General Security Risk Assessment Guideline, available to download for free at www.asisonline.org. Similarly, the American Bankers Association (ABA) has a risk assessment tool available for a nominal charge.

Step 6: Implement the required protection strategies. Protective strategies start with security awareness programs; employees must understand their obligation to use the security measures required to protect laptops and data. Educate them on basic theft prevention tips such as carrying a laptop in something other than a laptop bag. This may seem unusual, but using a laptop bag makes it very obvious to thieves. Use something more inconspicuous, such as a backpack or messenger bag. Or, remind them to never leave a laptop in plain sight in a locked car. Lock it in the trunk and make sure no one sees you put it there. Employees should be required to indicate, in writing, that they understand the established laptop and data protection guidelines. Department managers and senior managers should show their support for the policy by signing similar forms. Both facility and IT security personnel have special responsibilities for implementing the policy, and should indicate their willingness to assist on the appropriate forms.

Step 7: Create a loss response team to monitor laptops and data. Should a loss occur, the affected employees should be required to report the loss in writing. The team then responds to the report by investigating the losses and determining the scope of the data breach. In addition, the team should be regularly educating users, conducting audits to ensure compliance, annually assessing data needs, and destroying or removing data when it is no longer required. This process is cyclical, since new laptops and data enter and leave the organization on a regular basis.

Clean the Hard Drive

Perhaps the most important part of any laptop protection policy is educating the user about what should be kept on the hard drive. They should be encouraged to strip their hard drive back to the bare essentials, storing most of their vital documents and files elsewhere. Have them look at everything on their machine and ask, "Does this top-secret government file have to go with me everywhere?" If not, leave it on your home or office computer, or store it on a small encrypted drive or USB memory stick (just don't keep this in the same bag as your laptop).

According to a 2007 survey by McAfee and Datamonitor, a data breach involving personal customer information could cost a company, on average, $268,000 in reporting expenses—even if the data is never used. You can take several key steps to protect both your laptops and your data. By adopting these measures, you'll greatly reduce the risk of losing key hardware and data in your organization.

FinCEN Guidance on Email Fraud

Email fraud schemes in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers are increasing at an alarming rate. Earlier this summer, the FBI issued a warning that "Business Email Compromise" ("BEC") scams were evolving and targeting businesses of all sizes. Since 2013, these scams have hit more than 22,000 victims for a combined dollar loss of greater than $3 billion. These and other email fraud scams are highly effective because they mimic legitimate requests.

On September 6, the Financial Crimes Enforcement Network (FinCEN) issued an advisory to help financial institutions guard against these burgeoning threats. The guidance (FIN-2016-A003) provides detailed analysis of how these scams are deployed and examples of different scenarios. The advisory also provides red flags that financial institutions can use to identify and prevent these types of schemes. The full advisory is available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003

Updated IT Security Guidance

The Federal Financial Institutions Examination Council (FFIEC) has issued updated guidance in its "Information Security" booklet, which is part of the FFIEC IT Handbook. The revisions are designed to help financial institutions manage security risks and to explain how examiners will review their information security programs. The guidance directs financial institutions to focus on specific factors that the FFIEC believes are necessary to assess the level of security risks to a financial institution's information systems. The booklet contains updated examination procedures and outlines four broad assessments that examiners will consider with regard to a financial institution's information security program.

The IT Handbook is available at http://ithandbook.ffiec.gov/.

Focus *on Fraud*

Proposed AML Rules for Exempted Banks

Under Section 352 of the USA Patriot Act, most banks are subject to an AML program. Banks that lack a federal functional regulator, while required to comply with BSA recordkeeping, reporting, and (for some) CIP requirements, have been exempt from the AML program requirement. FinCEN has published a proposal to amend portions of the AML rules by adding AML program requirements for banks that lack a federal functional regulator, and extending CIP and beneficial ownership requirements to those banks not already subject to those requirements. In the proposed rule published in the Federal Register on August 25, the agency noted that "the statutory mandate that all financial institutions establish anti-money laundering programs is a key element in the national effort to prevent and detect money laundering and the financing of terrorism. Banks without a Federal functional regulator may be as vulnerable to the risks of AML and terrorist financing as banks with one. This proposed rule would eliminate the present regulatory gap in AML coverage between banks with and without a federal functional regulator." FinCEN is accepting written comments on the proposed rule on or before October 24, 2016.

Check Fraud Ring Taken Down

Under the "if it sounds too good to be true" category falls most of the online work-at-home and "mystery shopper" scams that target unwitting individuals eager to make a quick buck. Even savvy consumers have been known to fall prey to scams that lure victims with the promise of making extra income doing something they enjoy. The Better Business Bureau reports that thousands of Americans have lost millions of dollars to mystery shopper scams. Federal authorities are cracking down on these scams. Six U.S. citizens and a Nigerian national were recently sentenced to federal prison for their roles in an online counterfeit check fraud ring that distributed more than $40 million in counterfeit checks. The defendants were members of a large-scale international financial fraud conspiracy that included romance scams through online dating sites, check fraud, mystery shopper, and work-from-home schemes. The checks paid to the "hired hands" would bounce after victims sent the proceeds to various locations in the U.S. that ended up in Nigeria. Victims owed their banks for the full amount of the counterfeit checks, and often hundreds of dollars in bank fees. The fraud ring was taken down by the U.S. Immigration and Customs Enforcement's (ICE) Homeland Security Investigations.

Menacing ATM Malware Threat

When malware was recently found on one of its bank ATMs, the central bank of Thailand shut down about half of its ATMs. An Eastern European gang is believed to be responsible for planting malware on the ATMs that siphoned $12 million baht ($346,816) from 21 of the bank's ATMs manufactured by NCR, which had been showing problems with missing money. An investigation revealed that some of the machines were spitting out up to 1 million baht at a time, and that 960,000 baht had gone missing from five of the ATMS in just one week from August 1 to August 8. Security firm FireEye has identified the malicious ATM malware dubbed "Ripper" that deploys unique techniques never before seen. The malware sample was found to have been uploaded to VirusTotal from an IP address in Thailand a couple of minutes before the Bangkok Post reported their 12 million baht ATM heist. The malware leverages technology to access physical devices and can compromise multiple vendor platforms. Banks will want to be on the lookout for this menacing ATM malware threat.

CFPB on Elder Financial Abuse

Financial scams targeting individuals and businesses are on the rise. One sector that is particularly vulnerable to financial losses is aging Americans. Seniors are more susceptible to fraud and financial exploitation, often falling victim to abuse by family members or caregivers. Annual financial losses by victims of elder abuse are estimated at $36 billion. To address this growing problem, the Consumer Financial Protection Bureau (CFPB) has issued "Report and Recommendations: Fighting Elder Financial Exploitation through Community Networks" outlining recommendations to protect older Americans against financial exploitation and a resource guide providing best practices on elder financial abuse. Get the report and resource guide at www.consumerfinance.gov.

From the Editor

Security Orientation is a Must

by P. Kevin Smith, CPP

Protecting your company assets begins with ensuring your employees are prepared to assist in maintaining a safe and secure workplace. The best security technology in the world can't help you unless employees understand their roles and responsibilities in safeguarding sensitive data and protecting company resources. This will involve putting practices and policies in place that promote security and training employees to be able to identify and avoid risks. We tend to think our employees know the basics of security, but the reality is that most new employees don't have a clue about their role in your security program.

Many years ago, before information security was the buzz of the industry and security training was en vogue, a golfing buddy of mine asked if I would speak to his son's high school class about "ethics in the workplace." I owed him quite a bit from poor golf bets, so I agreed to speak to the senior class of Blake High School in Silver Springs, Maryland. When the day came, it was snowing rather hard in the Silver Springs area, and I found myself anxiously listening to the radio. Like most of the Blake High School students, I was hoping that school would be canceled for the day, but just like those times when my homework was incomplete and I rooted for snow, the radio confirmed my fears… school was in session. I drove to school that morning on relatively clear streets (damn those snow plows) and arrived to a full parking lot and the principal waiting for me in the school vestibule. I was surprised to learn that my lecture was not just for a small group in a single classroom, but a full assembly with nearly 500 students in the audience. I sat in the front row listening to another guest speaker, while spit balls and paper airplanes filled the air, thinking to myself, "What have you gotten into now?"

I had my training manager assist me in putting together a very basic slide presentation that opened with the security practitioner's mantra – the "10-80-10 rule." In every group of individuals, you will find 10% who are perfect angels and would never steal anything that didn't belong to them. In that same group you will find 10% who are outright thieves and would steal anything they can get their hands on. The remaining 80% of the group would take something that didn't belong to them if they had the perfect opportunity to do so. Now during my explanation of the 10-80-10 rule, there were snickers, fingers being pointed between students, and outright laughter, but when I shifted gears to a sobering picture of the twin towers, you could hear a pin drop. I explained to the students how the world had changed on September 11, 2001 in more ways than they could possibly know. Specifically, I told them how background checks would be heavily scrutinized, and those stupid mistakes like petty larceny and behavioral improprieties in the workplace might preclude them from finding a meaningful job.

By the end of my presentation, I had that crowd, which by definition consisted of 50+ juvenile delinquents, in the palm of my hands. They were completely engaged and hanging on my every word. As I left the stage to significant applause, it occurred to me that some of these 17 & 18 year old students were next year's employees. My training manager, who was also in the audience said, "why aren't we giving that same presentation to all of our new employees?" From that day forward, the "Workplace Ethics" program became a staple of our new employee orientation program, and it was expanded to include information security, physical security, and the employee's role in the corporate security program.

Training employees is a critical element of security. They need to understand the value of protecting customer and colleague information and their role in keeping it safe. They also need a basic grounding in other risks and how to make good judgments throughout their daily routines. Most importantly, they need to know the policies and practices you expect them to follow in the workplace regarding both physical and electronic security. If your security department doesn't play a role in the new employee orientation program, you are missing the boat. Security is not just locks, cameras, and alarms… it's a state of mind, and it all starts when that new employee walks through the door for the first day.

WAR *Stories*

Dressed for the Heist

When Eric Reaves arrived at the AmeriChoice Federal Credit Union in York Township, PA dressed as "Erica," he never made it past the front door. The credit union had received a call from Donald Hopple, a regional detective who warned them they were about to be robbed. Bank employees were able to lock the inner doors before Reaves arrived. Hopple and another officer had been tailing the cross- dressing suspect after he robbed an M&T Bank last month wearing an orange wig, a dress and carrying a purse. The officers took Reaves into custody when they arrived right behind him at the bank. They found the demand note in his purse. Reaves has history of committing bank robberies disguised as a female.

Went for Round Two, Twice

When Willie Weathersby robbed a Fifth Third Bank in Chicago, he needed to get out of town fast…and should have. Less than two hours after the heist, he drove off a used car lot with his newly purchased 1998 Nissan Maxima (the down payment obviously not part of a dye pack). Police were tipped off to Weathersby's identity by a former co-worker who Weathersby told he had $4,000 and had asked for a ride to Wisconsin. Before they caught up to him, he robbed a Royal Savings Bank branch and hit the same Fifth Third branch again. He was arrested after a fourth failed robbery attempt, again at the Royal Savings Bank.

Marital Escape Plan

Most couples have marital problems at some point. But not many would choose prison over marriage. Lawrence John Ripple, 70, is the exception. Following a spat with his wife, Ripple told her that "he'd rather be in jail than at home" – a threat he followed through on. Ripple walked into the Brotherhood Bank and Trust in Kansas City, handed the teller a note saying that he had a gun and wanted money. After the teller handed him nearly $3,000 in cash, Ripple took a seat in the lobby and waited there until police came and took him to the local jail. Sure hope he gets along well with his cell mate.

QUESTIONS & *Answers*

Q. Our bank is considering expanding our background checks for new employees to include fingerprint checks through the FBI. Is that the same system used by gun dealers to check on the criminal history of a prospective gun buyer?

A. The short answer is no. Federal Firearms Licensees (FFLs) operate under procedures established by the Brady Handgun Violence Prevention Act (Brady Act) of 1993, Public Law 103-159. Under the Brady Bill the National Instant Criminal Background Check System (NICS) was established for FFLs to contact by telephone, or other electronic means, for information to be supplied immediately on whether the transfer of a firearm would be in violation of Section 922 (g) or (n) of Title 18, United States Code, or state law. The NICS is a national system that checks available records on persons who may be disqualified from receiving firearms. The FBI developed the system through a cooperative effort with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and local and state law enforcement agencies. The NICS is a computerized background check system designed to respond instantly on most background check inquiries so the FFLs receive an almost immediate response.

Banks have access to the FBI criminal records under the authorities granted by the Federal Deposit Insurance Act (12 U.S.C. 1829). Section 19 of the act imposes a duty upon the insured institution to make a reasonable inquiry regarding an applicant's history, which consists of taking steps appropriate under the circumstances, consistent with applicable law, to avoid hiring or permitting participation in its affairs by a person who has a conviction or program entry for a covered offense. The FDIC believes that at a minimum, each insured institution should establish a screening process that provides the insured institution with information concerning any convictions or program entry pertaining to a job applicant. This would include, for example, the completion of a written employment application that requires a listing of all convictions and program entries. Due to this federal mandate, federally insured banks may obtain permission from the FBI to submit fingerprints for identity verification and criminal background checks. So, the two processes differ in that one is a telephone check based on pedigree information (name, address, DOB, SS#, etc.), while the other is based on the submission of fingerprints.

Q. The term ransomware seems to be dominating the information security world these days. What exactly is ransomware, and how does it work?

A. Ransomware is an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them. The inability to access the important data these kinds of organizations keep can be catastrophic in terms of the loss of sensitive or proprietary information, the disruption to regular operations, financial losses incurred to restore systems and files, and the potential harm to an organization's reputation. Home computers are just as susceptible to ransomware and the loss of access to personal and often irreplaceable items – including family photos, videos, and other data – can be devastating for individuals as well.

In a ransomware attack, victims – upon seeing an email addressed to them—will open it and may click on an attachment that appears legitimate, like an invoice or an electronic fax, but which actually contains the malicious ransomware code. Or the email might contain a legitimate-looking URL, but when a victim clicks on it, they are directed to a website that infects their computer with malicious software.

Once the infection is present, the malware begins encrypting files and folders on local drives, any attached drives, backup drives, and potentially other computers on the same network that the victim computer is attached to. Users and organizations are generally not aware they have been infected until they can no longer access their data or until they begin to see computer messages advising them of the attack and demands for a ransom payment in exchange for a decryption key. These messages include instructions on how to pay the ransom, usually with bitcoins because of the anonymity this virtual currency provides.

Ransomware attacks are not only proliferating, they're becoming more sophisticated. Several years ago, ransomware was normally delivered through spam emails, but because email systems got better at filtering out spam, cyber criminals turned to spear phishing emails targeting specific individuals. And in newer instances of ransomware, some cyber criminals aren't using emails at all—they can bypass the need for an individual to click on a link by seeding legitimate websites with malicious code, taking advantage of unpatched software on end-user computers.

Q. I know there are several regulations around Vendor Risk Management, but where do we start with assessing the risk our vendors present?

A. You are correct that vendor risk management is a hot button with the regulators right now. The OCC guidelines state in part, "Banks must maintain adequate risk management processes throughout each phase of a third party relationship's life cycle…a bank should adopt a risk management process commensurate with the level of risk and complexity of its third party relationships." In other words, one size does not fit all.

The company who services the machines in your data center, for example, poses a greater risk that the company that delivers your office supplies. One basic step is to ensure that the vendor is indeed who they claim to be. Ask for their unique DUNS number, which ties the vendor to Dunn &Bradstreet's database, allowing for verification of basic organization contact information and satisfying basic Know Your Vendor (KYV) requirements. A second resource is the better business bureau and other key financial risk indicators. There are several independent resources that predict financial stress of a vendor. Ask your commercial lending folks for advice in this area. Finally, you should run the company name and any of its principals against all known watch lists, global sanction lists, etc.

The American Bankers Association has an excellent white paper on VRM that discusses which vendor relationships should be included in an institution's vendor oversight program and to what level they should be reviewed.

WHAT DO *other* BANKERS *do?*

Disaster Relief Donations

In the wake of historic flooding in Louisiana, tornadoes in the Midwest, wildfires on the West Coast and other natural disasters, U.S. Bank made it possible for their customers to reach out and help those affected by these crises. Accountholders were able to make monetary donations to the American Red Cross at the bank's ATMs through September 16. All funds were distributed directly to Red Cross Disaster Relief. The bank commits $250,000 annually to the Red Cross for vital disaster services. Throughout the year, the bank employees can also donate blood and volunteer time to the charity.

A Hit for Homeowners

When members of the Milwaukee Brewers pro baseball team were up to bat at the Brewers home games this season, every hit scored a $150 donation tallied on an Associated Bank Check Deck screen for Housing Resources, Inc. (HRI). The Hits for Homes program raised $100,000 during the 2016 season. Associated Bank and Brewers Community Foundation wrapped-up the Hits for presented a check to HRI at a Brewers game in early September. The donation to HRI will be used to provide emergency and essential home repair grants in low-to-moderate-income neighborhoods in the Milwaukee community. In addition to the financial contribution, Associated Bank and Brewers Community Foundation conducted a tool drive and collected 160 new or gently used tools to support HRI's Tool Loan Center, to help area homeowners restore and maintain their homes.

Building Stronger Communities

To help strengthen the communities it serves and ensure that children and families of all backgrounds are provided equal opportunities, TowneBank in Richmond, VA donated $500,000 to the YMCA of Greater Richmond. The donation will fund efforts to revitalize urban YMCA facilities in North and South Richmond and the city of Petersburg. The center provides not just physical exercise but leadership and education programs as well for those who may not otherwise be eligible for such programs. Last year, the bank donated $250,000 to the capital campaign of Goodwill of Central and Coastal Virginia.

CU Gives $1M 4Kids

The Children's Miracle Network receives generous support from credit unions across the nation - their 3rd largest sponsor. Celebrating 30 years of partnership, Firstmark Credit Union has given more than $1 million to the CMN's Credit Unions for Kids (CUFK) fundraising program. Employees and members raised money through donations, bowling events, hosting giveaways, and many other community initiatives.

All monetary contributions collected through these efforts are used to fund various needs of The Children's Hospital of San Antonio Foundation, including life-saving research, cutting edge and innovative technology, and essential charity care required to treat children every year. Firstmark's goal in 2016 is to raise $50,000 to support the efforts of CUFK and The Children's Hospital of San Antonio. Since 2006, CU4Kids has raised $150 million for Children's Miracle Network Hospitals.

AND IN *Conclusion*

"This is how he chooses which security training topics to cover?"

BANKERS' Hotline

P U R P O S E :

To keep front line, security, and operations personnel up-to-date on industry trends, regulatory and compliance issues and industry related techniques. To assist administrators in maintaining high morale. To provide a timely, reliable information source for the banker who does not have access to all pertinent banking publications, nor the time to read and evaluate them. To supply a sounding board for the purpose of sharing information and creating communication between all parts of the financial industry. To assemble all of the above in a readable, understandable, usable format that can be photocopied and distributed in-house by each subscriber.

PUBLISHER
George B. Milner, Jr.
Bankers Information Network

EDITOR
P. Kevin Smith
Bankers' Hotline

Subscription Rates: To order or renew Bankers' Hotline, call (800) 660-0080 or notify by mail at PO Box 1632, Doylestown, PA 18901, for a one year subscription at $249. Letters to the Editor may be sent to the same address or emailed to bh@BankersOnline.com.