BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXVII NUMBER 5

WHAT'S INSIDE

2 In The News
- Fintech, Regtech, and an Upset
- CFPB Delays Prepaid Account Rule
- Reduce Risk and Build Relationships

3 Statistics, Facts & Such

3 Tech Update

3 Coming Up

4 Training Page:
The (in)Security of (im)Perfect Passwords
by P. Kevin Smith, CPP

5 Banks Responding to Consumer Complaints

5 'Tis the Season for Same Day ACH Testing

5 Focus on Fraud
- New Cyber Executive Orderer
- ID Theft is a Booming Business
- Good Guys-1, Bad Guy-27
- Billion Dollar BEC Scams

6 From the Editor:
Security's Place
by P. Kevin Smith, CPP

6 War Stories
- Booze Sting Nets Bandit
- Suspect Was a Shoe-In
- An Eclectic Disguise

7 Questions & Answers

8 What Do Other Bankers Do?
- Help for Homebuyers
- Money for Meals
- Funding Community Support
- Helping Hand for Healthcare
- A Charitable Donation

8 And In Conclusion

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.

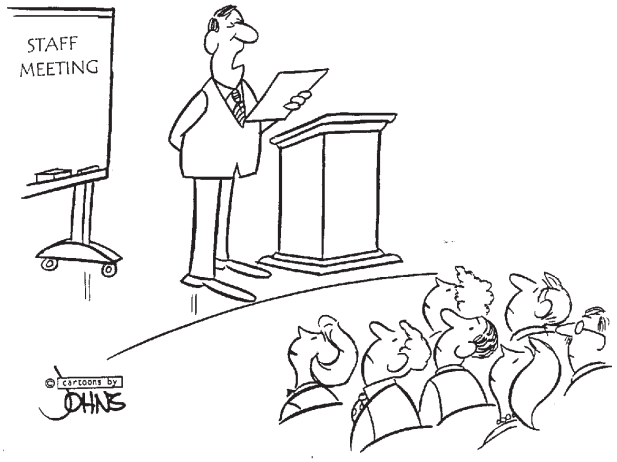
Helping Hand for Healthcare

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.