BANKERS' Hotline

THE MONTHLY RESOURCE FOR BRANCHES & OPERATIONS

VOLUME XXV 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 22, 2015

The OCC's Perspective on Risk

by Teri Wesley

The Office of the Comptroller of the Currency (OCC) recently released its "Semi-annual Risk Perspective for Spring 2015," which highlights key risk areas the agency has identified that pose a potential threat to the safety and soundness of banks. Based on bank financial data recorded at the end of 2014, the report is directed at banks supervised by the OCC and establishes the regulator's supervisory priorities for the next twelve months. However, state-chartered institutions should also take heed to the risks facing banks that are outlined in the report.

Following are some of the key points the OCC has highlighted in its spring report:

Cybersecurity

Banks and their employees, customers, and third-party service providers are vulnerable to evolving cyber threats that can compromise data or systems and allow criminals to illegally obtain personally identifiable data. OCC examiners will review a bank's program for assessing and mitigating such threats and vulnerabilities. OCC reviews will include assessments of data and network protection practices, business continuity practices, risks from vendors, and compliance with any new guidance.

Third-Party Vendors

To lower overhead expenses, banks are outsourcing critical functions to third-party providers without establishing the risk management processes necessary for appropriate oversight and controls to monitor associated risks. An assessment of a bank's operational risk by OCC examiners will include a focus on third-party risk management.

(continued on next page)

Consumer Protection for Faster Payments

by Teri Wesley

The primary function of the Consumer Financial Protection Bureau (CFPB) is to advocate for consumers' rights and protections with regard to their finances. The bureau has supported the development of faster and more secure payments in both new and existing payment systems. As these faster payment systems are developed, the CFPB wants to ensure that consumer protections are built into new payment systems from the start. On July 9th, the CFPB issued its guidelines for the development of faster payment systems in its Consumer Protection Principles, which relate to privacy, transparency, costs, security and consumer control of faster payments. The bureau also wants to ensure that new faster payments systems are equipped to deal with fraud and error resolution. "While American consumers benefit from and make use of these payment systems, there remain opportunities to improve efficiency, reduce transaction costs for consumers and reduce credit and fraud risks," said the CFPB. The bureau further pointed out that faster payments provide consumers with real time information about their account balances, thus helping them avoid potential overdrafts.

The CFPB's payments guidelines can be accessed at **www.consumerfinance.gov**

The OCC's Perspective on Risk
(continued from front page)

Compliance

As banks work to comply with new mortgage lending requirements and manage Bank Secrecy Act/Anti-Money Laundering risks, compliance risk remains high in these areas:

1) Bank Secrecy Act/Anti-Money Laundering (BSA/AML) risks. The OCC has noted that "BSA programs at some banks have failed to develop or incorporate appropriate controls as products and services have evolved, and insufficient resources and expertise have been devoted to BSA/AML in some banks."
2) Risk of unfair or deceptive practices arising from the use of third parties to conduct all or a portion of consumer credit-related product development, implementation and fulfillment. Some banks are failing to exercise adequate risk management and controls when developing and offering add-on products to customers.
3) Fair lending risk arises when banks engage a third party to conduct all or a portion of the application or underwriting process or make decisions regarding terms or pricing.
4) Risk created by the need for banks to implement significant changes to policies and procedures to comply with the new RESPA (Real Estate Settlement Procedures Act) mortgage disclosure requirements that become effective later this year.

Going forward, OCC examiners will review a bank's BSA/AML program and controls, as well as management's measures to maintain an effective program. For large banks, OCC examiners will coordinate with the CFPB to determine compliance with consumer laws, regulations, and guidance. For both large and smaller banks, OCC examiners will assess a bank's effectiveness in identifying and responding to risks created by new products, services, or terms and, with regard to fair lending, assess a bank's efforts to meet the needs of creditworthy borrowers, and monitor the bank's compliance with the Community Reinvestment Act, fair lending laws, and other consumer protection laws.

The report also notes declining revenues and profitability overall in OCC-supervised institutions. Get the full risk report at www.occ.gov. Feedback on the report can be submitted by email to NRCReport@occ.treas.gov.

IN THE *News*

Banks Get Their Own Domain

A new domain name for banks was launched last month to provide enhanced security for financial websites and prevent online banking users from being redirected to fake bank websites. Financial institutions are quickly adopting the new .bank domain name. Open to a select group of institutions during a "sunrise" phase in May, there were 782 registered banks already on board when it opened up for general availability in late June. More than 3,000 banks registered for the domain within 24 hours of its release. Only verified members of the global banking community that meet enhanced security requirements can register for a .bank domain name. The basic registration costs are $1,000 to $2,000, which includes the cost of ongoing verification and monitoring. The new, more secure domain is operated by fTLD Registry Services, LLC, an international coalition of banks, insurance companies, and financial services trade groups, that is overseen by the ABA and the Financial Services Roundtable. For more information or to register for the .bank domain name, go to: https://www.register.bank/

A Secure BYOD Solution

Many financial services employers prohibit the use of mobile devices in the workplace for the privacy and protection of corporate and customer data. Vermont-based Union Bank has found a solution that is a win-win for both its employees and data security. The bank is deploying the ZixOne mobile email app to enable employees to access corporate data on their personal mobile devices. ZixOne streams corporate email to smartphones and tablets without allowing the data to reside on the devices. Therefore, if the device is lost or stolen, corporate data is not at risk – an important consideration in the financial services industry. The mobile app is downloaded and installed without any training required.

Free Consumer Protection Resources

Auto insurer Geico's popular advertising mantra "15 minutes can save you 15 percent" relays the message that significant savings can be quick and simply obtained. The Federal Trade Commission is offering to save consumers a heap of trouble in even less time than that. The agency has released several videos that are less than two minutes long covering three topics that affect millions of consumers every day – renting housing property, car title loans and recovering from ID theft. These videos are available at www.consumer.gov for a deal that can't be beat – free! Additional videos and printed resources are available at no cost (in English and Spanish) that banks can post on their website or share on social media to help customers manage their money, protect their credit, and protect themselves from scams and identity theft.

Digital Disruption Leads to Branch Trimming

As more consumers navigate toward digital and mobile banking channels, traditional bank branches are swaying in the growing tide of change. Cincinnati-based Fifth Third Bank, which reports $140 billion in assets, will be trimming 100 of its branches in response to the digital disruption. "Technology continues to impact our service delivery and revenue generation tactics and strategies," said the bank's vice chairman and CEO Kevin T. Kabat. Currently with 1,303 banking centers across 12 states (including grocery store branches), the cuts will trim Fifth Third's branch network by approximately eight percent and reduce ongoing operating expenses by $60 million.

Banks Paying Billions in Fines

Compliance is costly. Non-compliance is even more so. According to global business and technology consulting firm Capco, banks have paid over $300 billion in fines since 2010. That number is staggering. In the pursuit of compliance and the use of technology to streamline and make more effective use of data, IT spending in the retail banking industry is predicted to increase 20 percent over the next four years and to reach $150 billion in 2018. The ability to gather, analyze and interpret data in real-time can help banks meet the increasing regulatory demands and decrease the amount of non-compliance penalties.

Statistics, *Facts & Such*

■ Security incidents target financial services 300% more frequently than any other industry. 33% of all lure stage attacks target financial services.
Marketwatch, *6/23/15*

■ Fraudulent debit card transactions occurring outside the U.K. on U.K. debit cards were up 25% in 2014.
ATM Marketplace, *6/26/15*

■ Fraudulent cross-border transactions accounted for 31% of all fraudulent transactions in 2014, up from 23% in 2013.
Ibid.

■ The U.S. accounted for 47% of all fraudulent cross-border transactions on U.K. debit cards in 2014.
Ibid.

■ While 24% of debit card transactions occurred at cash machines, just 12% of fraudulent transactions came from cash machines. Still, cash machines topped the list of merchant categories for fraudulent debit card use, followed by financial institutions at 12%.
Ibid.

■ Midsize businesses view a data breach among their top risks and a majority consider IT security very important when selecting a supplier. That's because 43% had experienced a data breach in the prior three years, and 13% have had a supplier's data breach impact their business.
Help Net Security, *6/29/15*

■ General purpose reloadable (GPR) cards are seeing increased use by unbanked and banked consumers, especially among unbanked cardholders who tend to use GPR cards like checking accounts.
Pymnts.com, *Banking on Prepaid report, 7/2/15*

■ GPR prepaid cards are regularly used by 23 million adults nationwide.
Ibid.

■ Of the unbanked GPR users, more than 8 out of 10 cardholders have annual household incomes lower than $50,000 and roughly one-third of that number have incomes below $15,000.
Ibid.

Tech *Update*

OPM Data Breach Offers Valuable Lesson

How much information to release about a data breach is a question that is debated almost daily in corporate situation rooms around the country? The recent U.S. Office of Personnel Management (OPM) data breach exposed an estimated 21.5 million records, including the highly invasive questionnaires used for background checks. The questionnaires collected sensitive, personal information about mental and emotional health, illegal drug use, alcohol abuse, personal finances, police records, involvement in non-criminal court actions, divorces and association with organizations advocating violence. The records include not only information about actual and prospective government employees, but also contractors, consultants, and others, which make up approximately 7% of the total US population. At first the public was told that the hackers had gotten a limited amount of basic personal information on some US government employees, then the extent of the information that was accessed was broadened until it was admitted that a vast trove of highly personal information from security clearance applications were accessed. The seriousness of the data breach has been indicated by the fact that Office of Personnel Management (OPM) director Katherine Archuleta has been forced to resign.

The OPM is offering credit monitoring services and identity theft insurance through a company that specializes in identity theft protection and fraud resolution. This comprehensive, 18-month membership includes credit report access, credit monitoring, identity theft insurance, and recovery services, and is available immediately at no cost to affected individuals identified by the OPM. Affected employees are also being provided an option to sign up for credit monitoring and other identity monitoring services for an extended period beyond the 18-month program.

Recently, two unions representing federal employees – the National Treasury Employees Union (NTEU) and the American Federation of Government Employees (AFGE) – have filed suit against OPM for failing to protect employee information. NTEU alleges that OPM's collection violates a constitutional right of privacy and seeks to enjoin OPM from collecting further employee information until appropriate safeguards are implemented. The AFGE filed a class action lawsuit on behalf of all breach victims asserting OPM's failure to comply with federal security requirements.

The lesson learned from the OPM debacle is that companies must be open and honest in disclosing the extent of a security breach. Melanie Dougherty Thomas, who advises companies on computer breaches, said deciding how much to disclose about a breach, and when to say it, is vital. "The general public understands there are breaches all the time," she said. "If you wait too long, you give the perception you're trying to hide the facts, and that to people is unforgivable."

COMING *Up*

Get all the details and register now!

Bankers' Hotline 21st Annual Security Officers Workshop
Philadelphia, PA, Oct 7-8, 2015 (pre-workshop sessions October 6)
via Live or Remote streaming
Discounted registrations fees for Bankers' Hotline subscribers!
Register online at: www.bankersonline.com/sow
Info: (800) 660-0080

ASIS INTERNATIONAL

61st Annual ASIS Seminar and Exhibits
Anaheim, CA, Sept 28-Oct 1, 2015

ASIS 26th New York City Security Conference and Expo
New York, NY, April 27-28, 2016
Info: (703) 519-6200
www.asisonline.org

ASSOCIATION OF CERTIFIED ANTI-MONEY LAUNDERING SPECIALISTS (ACAMS)

14th Annual AML & Financial Crime
Las Vegas, NV, Sep 28-30, 2015
Info: (866) 459-2267
www.acams.org

BOL CONFERENCES

BSA/AML Top Gun Conference
Scottsdale, AZ, Mar 22-23, 2016
via Live or Remote streaming
Info: (888) 229-8872 ext 87
www.bolconferences.com

INDEPENDENT COMMUNITY BAiNKERS OF AMERICA

BSA/AML Institute
Indianapolis, IN, Aug 3-5, 2015

Community Bank IT Institute
Minneapolis, MN, Aug 10-14, 2015
Info: (800) 422-7285
www.icba.org

TRAINING
PAGE

Tips for Identifying the Enemy Within

by P. Kevin Smith, CPP

A subscriber recently asked if we could offer any advice on how to address a recent rise that he is seeing in the area of bank employees exploiting elderly customers. He shared the following news stories as evidence of his concern.

From Alpena, Michigan

A Mt. Pleasant woman working as a bank manager in Alpena, Michigan admitted she created bank accounts with fake names and transferred money to them from elderly and deceased customers. The suspect pleaded guilty to stealing more than $300,000 in 2010 and 2011. As a branch manager and personal banker in Alpena, the suspect opened accounts in fictitious names and then transferred funds to them from certificates of deposit held by elderly and deceased customers. The suspect later transferred the funds from the accounts in the fictitious names to an account at another financial institution controlled by the suspect. According to court records, the suspect embezzled approximately $86,489 in 2010 and $222,983 in 201. In her position as a branch manager, the suspect managed other bank employees, opened new accounts, renewed certificates of deposit and generated sales.

From Media, PA

A former bank employee in Delaware County is facing multiple charges for stealing more than $430,000 over a ten-year period from elderly bank customers and from the estates of the deceased. Delaware County District Attorney Jack Whelan charged the suspect with theft by unlawful taking or disposition, receiving stolen property, forgery-unauthorized act in writing, theft by deception, criminal use of communication facility, identity theft, and other theft related charges. The theft was discovered in September 2014, when the bank was contacted by an attorney regarding unusual activity involving the estate of a deceased client. A transaction occurred on the deceased victim's account in August of 2014, after she had passed away in July. An investigation lead to the discovery that the suspect stole from eight different accounts by changing the account addresses to a P.O. Box owned by the suspect bank employee.

From Quakertown, PA

More than $354,000 was stolen in the past five years by a bank manager who took the money from six elderly consumers' accounts. A former branch manager living in Quakertown, PA, was charged with identity theft, forgery, access device fraud, theft by unlawful taking, theft by deception, theft by failure to make required disposition of funds and receiving stolen property.

In mid-November, the bank's security director reported the bank became aware of the thefts after an 83-year old woman noticed her balance was less than it should be and withdrawals that the woman had not made or authorized were discovered, police said in the affidavit of probable cause. An investigation revealed that the suspect, who was a branch teller at the time, had victimized six other elderly customers, ranging in age from 80 to 95 years old. A review of the video evidence showed the suspect conducting transactions with no one present at his teller window. The thefts, which took place between January 12, 2009, and November, 2014, involved at least 59 transactions and totaled more than $354,000, investigators said. "In each instance, the suspect was the teller of record, and the accounts involved Certificates of Deposit which belonged to elderly customers," according to the affidavit.

In each of the cases noted above, the activity might have been prevented through data analytics, which is the wave of the future in terms of loss prevention. If you are not using data analytics for both internal and external fraud prevention, then you are definitely in the minority. There are a number of software programs available today for both large and small financial institutions, but the basic concepts are the same in most if not all the systems available. The key is to identify normal activity associated with a position or function, and look for anomalies or out of pattern activities. For example, if a call center operator normally accesses 50 accounts in a full day of taking calls, rules may be written in a fraud detection system to alert on any call taker who looks at more than 75 accounts in a day. Programs of this nature are excellent tools for identifying employees who data mine for high dollar accounts. Similarly, rules may be written to identify a teller who processes more than a "normal" number of transactions for elderly clients, or someone who processes an abnormal number of CDs in a given period.

The more sophisticated programs actually learn behavioral patterns and look for variances to that activity, similar to the processes used to identify money laundering activity. If a customer typically deposits $3,500 every two weeks, a deposit of $25,000 should set off an alert. Applying that concept to employee activity will help identify abnormal transactions in a timely manner. For example, excessive sales activity may be an indication that customer service representatives may be creating fictitious accounts to make goal in an incentive based compensation program.

Another popular form of data analytics is to compare employee data with new account information on a daily basis. Home addresses, cell phone numbers, and emergency contact information may be a potential red flag for employee misconduct. We know of one case where an employee address was used to open several accounts in different names, similar to the Media, PA case noted above.

Of course the main ingredient to any fraud prevention initiative is a solid Code of Business Conduct. Educating new employees about the Code of Business Conduct and reminding them of their responsibilities to report any violations is a great way to establish a security culture for your organization. Make them aware of the systems used to identify policy violations and criminal behavior, and ensure they understand the consequences of making a bad choice. Employees must understand that theft will be prosecuted regardless of the amount of money involved. The company's position on employee misconduct should be clearly stated in the employee handbook, and everyone should be reminded of those expectations at least annually.

Cyber Assessment Readiness Tool is Ready

In an effort to increase awareness of cybersecurity risks and help financial institutions identify and mitigate their risk, the Federal Financial Institutions Examination Council (FFIEC) has launched its Cybersecurity Assessment Tool. By using the tool and its accompanying resources to assess their cyber readiness, institutions can be better prepared to mitigate evolving threats. Beginning in late 2015, the Office of the Comptroller of Currency (OCC) will incorporate the assessment tool in their examinations of national banks, federal savings associations, and federal branches and agencies of all sizes to evalute the institution's inherent risk and cybersecurity preparedness.

Other resources available from the FFIEC include an executive overview, a user's guide, an online presentation explaining the Assessment, and appendixes mapping the Assessment's baseline items to the FFIEC Information Technology (IT) Examination Handbook and to the NIST Cybersecurity Framework.

Risk-Based Guidance for Virtual Currency

Once thought to be a passing fad, virtual currency is shaking up the traditional landscape of banking, trade, and business. Of growing concern to regulators is the money laundering and terrorist financial risks presented by virtual currency payment products and services (VCPPS). On June 29, the Financial Action Task Force (FATF) issued guidance urging the industry to take a risk-based approach to virtual currencies and services, particularly with regard to convertible virtual currency exchangers. Convertible virtual currency, such as Bitcoin, is that which has an equivalent value of, or acts as a substitute for, real currency. It is digitally traded between users and can be purchased for or exchanged into U.S. dollars or Euros. The FATF's "Guidance for a Risk-Based Approach to Virtual Currencies" recommends that virtual currency exchanges should be registered and licensed, and subject to the same scrutiny as other financial institutions and money transfer businesses. Likewise, VCPPS should do the same due diligence as their traditional counterparts, and those accepting wire transfers from foreign countries should maintain adequate records of senders and beneficiaries.

Focus *on Fraud*

Making Sure Bank Employees Don't Get Hooked

Criminals are increasingly using data mined from social media sites to craft legitimate-looking and effective phishing scams, many of which are used to target financial institution employees as well as customers. According to Verizon's 2015 Data Breach Investigations Report, their tactics are working, with 23 percent of recipients opening phishing emails and 11 percent clicking on infected attachments. As more banks and bank employees regularly use social media outlets, employee education – particularly with an emphasis on social media awareness – is a key component of mitigating phishing attacks. Employees need to be aware that personal information, such as their interests and hobbies and where they work, can be used by attackers to expose the employee and the bank to risks. Once an employee has been compromised through phishing, criminals can use this access to penetrate the network and conduct advanced, persistent attacks, enabling them to extract large amounts of customer and business data, often times undetected over a long period of time. Having a comprehensive social media awareness and assessment plan and providing effective employee education can help prevent your staff from getting hooked and putting themselves – and your institution – at risk.

Preparation Prevents Panic

In 1997 Bankers Video Library, in conjunction with Bankers' Hotline, produced its very first training video, titled Preparation Prevents Panic. The video covered takedown bank robberies and provided robbery response training required under the Bank Protection Act. That video has since been updated to a more "modern" version. While these physical threats still exist today, robbing banks and stealing funds (and data) is more commonly perpetrated by more sophisticated and modern modus operandi in the form of cyber attacks.

Earlier in July, three technical "glitches" within hours apart grounded the flights of one of the largest U.S. airlines, temporarily crippled a major news site, and halted stock trading for hours. While Homeland Security Secretary Jeh Johnson went on record to assure Americans that the malfunctions "were not the result of any nefarious actor," the outages sparked fears of cyber attacks and highlighted the growing dependency on fragile technology.

According to a recent report released by IT security firm Centri, over 200 significant security incidents occur on a daily basis, with nearly six actual breaches each day. Just as many banks think that violent bank robberies will "never happen there," every financial institution – from the smallest to the largest – should be prepared to defend and respond to a cyber intrusion. It can happen anywhere! Preparation now prevents panic in the event such an attack occurs.

AML/KYC Compliance Worth the Cost

In the "good ole days" most bankers either knew their customers personally or through the referral of another client. With the explosive growth in banking and the Internet, the Know Your Customer (KYC) process has become much more arduous, time-consuming, and costly. Failing to properly implement KYC policies exposes an institution not only to myriad types of potential fraud, but to legal, compliance, and reputational risk as well. Today, hundreds of millions of dollars are spent on anti-money laundering (AML) and KYC compliance. Financial institutions are increasingly outsourcing parts or all of their AML/KYC monitoring processes. Given that, a growing number of KYC registries have cropped up to streamline the data verification process. Last year, the SWIFT registry reported that its community of more than 7,000 correspondent banks make more than 1.3 million exchanges of KYC data each year. Earlier this year, Thomson Reuters Accelus ID reported its total records managed have exceeded 12,000.

From 2004 to 2010, 110 financial institutions were fined for AML failures. In a recent enforcement action taken against a small bank, FinCEN imposed $4.5 million in fines against West Virginia-based Mingo Bank for its "severe and systemic failures" in nearly every aspect of its AML program, including monitoring anomalous activity. Whether you outsource your AML/KYC processes or manage them in-house, the costs of doing so far outweigh the substantial monetary penalties of failing to have an effective AML compliance program in place, as well as the potential civil and criminal liability for BSA violations.

From the Editor

Patience – The Lost Virtue

by P. Kevin Smith, CPP

A young Reggie Jackson, rookie outfielder for the Baltimore Orioles, was waiting anxiously on first base for the steal sign from the third base coach, after receiving a walk with one out in the seventh inning of a tied ball game. Reggie was one of the fastest players in the league, and he knew he could steal second with no trouble at all. When the coach failed to give him a green light, Jackson decided to steal on his own. On the second pitch, he got a great jump and took off for second base. The throw was late, and Jackson made it easily into scoring position. Unfortunately, Jackson never scored because two batters later that inning ended on a 6-4-3 double play. As Jackson made his way to the dugout, Baltimore's Manager Earl Weaver summoned Jackson to the back corner of the dugout, where he chastised his young star for taking matters into his own hands. "Look kid," Weaver said, "your stupid move took the bat out of our most productive hitter's hands. They intentionally walked him, so they could set up a double play and pitch to a guy who is in a 0 for 12 slump. Now we have the bottom of our batting order coming up next inning, and I'll have to pinch hit for a pitcher that is doing very well on the mound. I didn't want you to steal because I see the big picture. You are only thinking about the short term rewards and showing off your skills. There are times when you must be patient and trust what your manager has in store."

So it is with life in corporate America. We must be patient and trust in the long term vision of management and the company we work for. In the world of security, patience is a virtue that is worth cultivating among the investigative team, especially those young sleuths from Generation X. Unfortunately, patience is becoming a lost virtue. Think about it…we no longer prepare a meal, set the timer and wait for the oven to cook dinner while we relax in a chair with a pre-dinner cocktail or glass of wine. Today, we pace back in forth in front of a microwave for our food to be done. And, heaven forbid that we do some research in the comfort of a library or home office. Most of us have a "Google reflex" while driving, just to find out the age of an artist we heard on the radio.

Bank investigations are all about patience; gathering data, conducting interviews, and evaluating the results. A rush to find out what went wrong and how we can prevent it from happening again often leads to over-reaction and snap judgements. The recent Amtrak catastrophe in Philadelphia illustrates this point. Initial data showed that the train was traveling in excess of 100 MPH, which prompted Philadelphia Mayor Michael Nutter to say, "Clearly it was reckless in terms of the driving by the engineer. There's no way in the world he should have been going that fast into the curve." Now, the Mayor might be right, but a representative from the National Transportation Safety Board responded to the mayor's comment by saying, "We want to get the facts before we start making judgements." Faulty brakes, he noted, could have been involved.

No matter what the stakes are in any investigation, and no matter how visibly the gun is smoking, it's critical not to rush to a conclusion. Instead, you need to have all of the facts before any conclusions are drawn. As Meric Bloch, author of the book "The First Information Is Almost Always Wrong," once wrote, "spreading hysteria is always more entertaining than dealing with facts."

Too often, management exhorts pressure on the investigative team to find the guilty party or correct a control weakness. It's the investigator's job to balance those management inquiries and needs with the main objective, which is to conduct a thorough investigation by gathering all of the facts, taking the time to evaluate the results without preconceived notions, and render a decision that is best for the company. Ultimately, management will decide on a course of action, but it's the investigator who must weigh the evidence and conclude whether there is a preponderance of evidence that a crime has been committed or a policy has been violated. Remember, patience is the key to making a well informed decision.

WAR *Stories*

Third Time Wasn't a Charm

Employees at the Hoffman Estates community bank took the popular Stephen King quote "Fool me once, shame on you. Fool me twice, shame on me. Fool me three times, shame on both of us" to heart. A teller recognized 52-year-old Shelton Brooks last month when he came back a third time to rob the bank. Brooks made his first appearance in December, and returned in January to hold up the bank again. Both times he got away with a significant amount of cash. This time, however, the teller yelled "Robber! Robber!" as soon as she saw Brooks. He was detained by the bank security guard until police arrived.

Not the First Time

Police in Yuba City didn't need witness accounts or surveillance footage to identify the man who held up a Yuba City bank. When the thief handed the teller at Umpqua Bank a note that read "Give me $10,000 dollars or I will kill you," he had graciously signed it "John Chapman." You might think that was an understandable mistake for a first-time bandit. However, Chapman was previously convicted in 2012 after he presented a similar note in a heist he pulled at Bank of America in Marysville. Where, incidentally, Chapman was arrested just hours after the Yuba City robbery while waiting for a Greyhound bus bound for New York.

An "Unusual" Weapon

When Aaron Stein entered a PNC Bank branch in Crafton, PA with what appeared to be an explosive device tucked inside his shirt, tellers quickly handed the 35-year-old man the cash he demanded to avoid setting him off – or the gadget with wires and a green light on top they believed was a trigger button. Stein was pulled over by the local police as he was getting on the interstate. A search of his vehicle revealed the stolen loot in a garbage bag and the device he used to threaten the bank's staff. Stein was arrested on nine felony counts, including aggravated assault, robbery, threatening to use a weapon of mass destruction and the unusual charge of possessing a facsimile weapon of mass destruction – which turned out to be a vibrator.

QUESTIONS & *Answers*

Q. We recently had a female customer notify us of an attempted scam related to online dating. How is a bank involved with an online dating scam?

A. The Federal Trade Commission has reported several instances of online dating scams related to the banking industry. Here's what their website has to say about online dating fraud.

Not everyone using online dating sites is looking for love. Scammers create fake online profiles using photos of other people – even stolen pictures of real military personnel. They profess their love quickly. And they tug at the victim's heartstrings with made-up stories about how they need money – for emergencies, hospital bills, or travel. Why all of the tricks? They're looking to steal their money.

As if all that isn't bad enough, romance scammers are now involving their victims in online bank fraud. Here's how it works: The scammers set up dating profiles to meet potential victims. After they form a "relationship," they come up with reasons to ask their love interest to set up a new bank account. The scammers transfer stolen money into the new account, and then tell their victims to wire the money out of the country. Victims think they're just helping out their soulmate, never realizing they're aiding and abetting a crime.

Q. There are so many scams these days, you can't pick up the paper without reading about some stupid person who fell victim to another overseas con artist. Is there anything being done to capture these criminals and bring them to justice?

A. Funny you should ask. The Department of Justice recently announced the extradition of six Nigerian nationals from South Africa to Mississippi to face a nine-count federal indictment for various Internet frauds. These six people join 15 others who were previously charged with, among other things, conspiracy to commit mail fraud, wire fraud, bank fraud, identity theft, and money laundering. The charges stem from the defendants alleged participation in numerous Internet-based complex financial fraud schemes, including romance scams, re-shipping scams, fraudulent check scams and work-at-home scams, as well as bank, financial and credit card account takeovers.

According to the allegations in the indictment, from as early as 2001, the defendants identified and solicited potential victims through online dating websites and work-at-home opportunities. In some instances, the defendants allegedly carried on fictitious online romantic relationships with victims for the purpose of using the victims to further certain objectives of the conspiracy. For example, the indictment alleges that the defendants convinced victims to ship and receive merchandise purchased with stolen personal identifying information (PII) and compromised credit card and banking information, to deposit counterfeit checks, and to transfer proceeds of the conspiracy via wire, U.S. mail or express delivery services.

A total of 20 individuals were charged in this case, which is being prosecuted by the U.S. Attorney's office in the southern district of Mississippi. So, while it may be difficult to extradite and prosecute these online con artists, it is possible when the dollar value is sufficient and there is sufficient evidence to support the charges.

Q. We have a customer who is challenging charges to his credit card account, and he says we must resolve the issue for him under the Fair Credit Billing Act. We're not aware of any responsibilities for the bank under the FCBA. Can you offer a recommendation on how we should respond to the customer?

A. The Fair Credit Billing Act (FCBA) referred to by your customer applies to "open end" credit accounts, like credit cards, and revolving charge accounts, like department store accounts. It doesn't cover installment contracts — loans or extensions of credit you repay on a fixed schedule. People often buy cars, furniture, and major appliances on an installment basis, and repay personal loans in installments, as well. The FCBA settlement procedures apply only to disputes about "billing errors." For example:

- unauthorized charges. Federal law limits a consumer's responsibility for unauthorized charges to $50;
- charges that list the wrong date or amount;
- charges for goods and services a consumer didn't accept or that weren't delivered as agreed;
- math errors;
- failure to post payments and other credits, like returns;
- failure to send bills to a consumer's current address — assuming the creditor has the consumer's change of address, in writing, at least 20 days before the billing period ends; and
- charges for which the consumer asks for an explanation or written proof of purchase, along with a claimed error or request for clarification.

To take advantage of the law's protections, a consumer must:

- write to the creditor at the address given for "billing inquiries," not the address for sending payments, and include the consumer's name, address, account number, and a description of the billing error.
- send the letter so that it reaches the creditor within 60 days after the first bill with the error was mailed to the consumer. It's a good idea to send the letter by certified mail; ask for a return receipt to prove when the creditor received it. Include copies (not originals) of sales slips or other documents that support the claim. Keep a copy of the dispute letter.

The creditor must acknowledge a consumer's complaint, in writing, within 30 days after receiving it, unless the problem has been resolved. The creditor must resolve the dispute within two billing cycles (but not more than 90 days) after getting a consumer's letter. If it turns out that the consumer's bill has a mistake, the creditor must explain it to the consumer – in writing – the corrections that will be made to the account. In addition to crediting the account, the creditor must remove all finance charges, late fees, or other charges related to the error. If the creditor's investigation determines the bill is correct, the consumer must be told promptly and in writing how much they owe and why. More often than not, the consumer's dispute is with the creditor who posted the charge, but it would be advisable for banks to understand and be able to explain the process.

WHAT DO *other* BANKERS *do?*

Texas CU Gives Back Big

They say everything is bigger in Texas. That certainly rings true with the generous support University Federal Credit Union (UFCU) shows its members and communities. Last year the credit union gave 10% of its net earnings back to the community with charitable contributions that totaled $1.3 million toward higher education and healthcare. A big chunk of last year's donations was a $1.5 contribution toward the construction of a new medical center. In addition to a $1 million annual monetary donation to the UFCU Disch-Falk Field (home of the Texas Longhorns), the credit union contributes $125,000 annually to Texas State University for scholarship and academic program funding. So far this year, the credit union has donated $50,000 to the UT-Dell Medical School, a $30,000 scholarship donation to the University of Texas, a $25,000 donation to St. Edwards University to support international students' travel, and $10,000 in scholarship funding to Texas A&M University.

Contributing to Cancer Care

Franklin Savings Bank in New Hampshire has pledged $15,000 to Concord Hospital Trust toward the purchase of next generation radiation technology for the Payson Center for Cancer Care. The donation is part of a campaign to raise $2 million for a new linear accelerator (or LINAC), valued at $4 million, that will improve cancer treatment by precisely targeting radiation to destroy cancer cells. The new LINAC will enable the Payson Center to continue treating the growing number of individuals seeking cancer care, and help the cancer center provide advanced care for current patients and future patients.

Charitable Grants for Community Causes

Thomaston Savings Bank Foundation in CT has awarded charitable grants to three local organizations. The foundation awarded a grant to The Bristol Hospital's Parent & Child Center for its Caring Closet program, which provides basic items to low-income families. TheWolcott Fire Training School received a grant to fund the purchase of a cargo trailer to travel to local fire companies and provide training in hazardous materials and confined space rescue. A grant was also awarded to the Waterbury Youth Services' Project Safe Place to fund the purchase and distribution of marketing materials for Project Safe Place, which provides youth in crisis a safe place to go. In 2014, the Thomaston Savings Bank Foundation awarded $560,000 in charitable grants.

Summer of Sharing

Summer is heating up in Plymouth, MI as local nonprofit organizations have a chance to receive $1,000 a day for 60 days. Community Financial Credit Union has kicked off its fifth annual Summer of Sharing campaign. Members can nominate their favorite nonprofit group at **www.SummerOfSharing.org** and tell how the organization benefits the community and why they deserve financial support. In addition to the recipient of the $1,000 a day for 60 days, all of the stories remain live on the site to bring awareness to the organizations. Since the Summer of Sharing program started in 2011, the credit union has donated over $180,000.

AND IN *Conclusion*

"I'd like you to give a presentation on business ethics. If you don't have time to prepare something, just steal it off the Internet."

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.