Ohio | Department of Commerce
Division of Financial Institutions
John R. Kasich, Governor Jacqueline T. Williams, Director

Kevin R. Allard, Superintendent
Phone: 614-728-8400
Fax: 614-644-1631
Email: Web.dfi@com.ohio.gov

The Regulatory Focus

A Message from Superintendent Kevin Allard

Welcome to October! The year seems to have gone by quickly and before we know it, the new year will be upon us. While the seasons will change, one thing that won't change is the division's continued emphasis on outreach and education to our regulated industries, and to consumers from a financial literacy perspective.

This month, our annual regional roundtables will be held in five locations around the state. These meetings provide you with the opportunity to personally interact with us, your regulator, and maybe catch up on a current hot topic. More information, including dates and locations, are included in this newsletter.

October also is recognized as National Cybersecurity Awareness Month (NCSAM). Since its inception in 2004, NCSAM is a collaborative effort between the U.S. Department of Homeland Security and the National Cyber Security Alliance. This month highlights the critical importance of cybersecurity and the need for vigilance and protection for all financial services providers and consumers.

As you know, cybersecurity continues to be a critical concern for banks, their customers and the financial system. The 2018 Global Risks Report by the World Economic Forum noted that cyberattacks are the most likely man-made risk facing the global economy. Not only does this issue touch businesses, it touches every person who uses technology.

Throughout October, we will email cybersecurity tips and informational articles on this very important topic to you. In addition, we will provide access to other cybersecurity resources, including information from the Department of Homeland Security, the Conference of State Bank Supervisors and the federal banking agencies. This information is designed to help you think about how your organization addresses this very important issue.

As always, if you have any questions on these or any other topics, please feel free to contact me directly at Kevin.Allard@com.ohio.gov or 614-728-2631.

In This Issue:

Social Engineering

By Jennifer Oldiges, IT Examiner

Did you know that people – and human error – are the weakest links in an organization's security chain?

Social engineering, or the practice of impersonating someone else to gain access to passwords, personal information and security codes, continues to be used by criminals to access customers' banking information and accounts. Most people know how to spot an attack via email or a phone call, but as criminals become more sophisticated, so do their techniques. Financial institutions and their employees must be aware of all forms of social engineering to protect the organization from attacks.

Here's how the bad guys do it:

Phishing
The criminal attempts to acquire private information such as usernames, passwords and account details via email. Typically, the phisher masquerades as a trustworthy entity using bulk email to evade spam filters. Emails claiming to be from popular websites, IT administrators or management are commonly used.

Vishing
Also known as "voice phishing," the criminal uses the telephone to access private personal and financial information.

Spear Phishing
Similar to phishing, the criminal specifically targets individuals who have access to the information they're after.

Water-holing
This technique takes advantage of websites people regularly visit and trust. The attacker will gather information about a targeted group to find out what those websites are, then test the websites for vulnerabilities. The criminal leverages that vulnerability and uses the site to access the target organization's system. This is effective because people don't hesitate to follow a link on a website they often visit and trust.

Baiting
This technique places physical media in sight of the victim. For example, malware-infected CD-ROMs or USB flash drives are left in locations where people will find them (parking lots, sidewalks, elevators, etc.), give the device a curiosity-piquing label and wait for the victim to insert the media into a company-owned computer.

Quid pro quo
Latin for "something for something," the criminal offers a benefit to the victim in exchange for information. For example, a hacker pretends to be IT support and calls with a quick fix to a common problem. The hacker will have the user type in commands that give the attacker access to or launch malware on the computer.

Tailgating
The criminal gains access to a building or other protected area by waiting for an authorized user to open and pass through a secure entry and then following right behind.

The Attackers
Reports claim cyberattacks cost financial services organizations more to address than any other industry. The rate of breaches continues to rise and the average cost of cybercrime to financial services organizations continues to increase. Why do the bad guys do it? Simply put, it's lucrative and relatively low risk. And when some criminal groups break up or are caught, newer groups with more sophisticated attack techniques take their place.

SOCIAL ENGINEERING *cont'd.*

A 2018 report from Positive Technologies, a leading global provider of enterprise security solutions, completed a study of cybercrime and cybersecurity in the banking industry. Over a three-year period, the study found:

All banks tested had vulnerabilities in web applications, insufficient network security and/or server configuration flaws

- 58 percent had deficiencies in user account and password management
- At 22 percent, experts successfully breached the bank's network
- 75 percent were vulnerable to social engineering attacks
- At 100 percent, experts obtained full control over the infrastructure
- At 58 percent, experts obtained access to banking systems
- At 25 percent, experts were able to compromise the workstations used for ATM management

The study cited specific weaknesses that made it possible for more than half of the banks tested to have their banking systems accessed.

> *"The main vulnerabilities and flaws in security mechanisms common on the bank network perimeter can be divided into four categories: vulnerabilities in web applications, insufficient network security, server configuration flaws, and deficiencies in user account and password management software. On average, an attacker who has penetrated the bank's internal network needs to only exploit those four flaws to gain access to the banks' electronic crown jewels."*

The report concludes with four points:

1. If an attack is detected and stopped in time, intruders can be thwarted. Preventing losses is possible at any stage if appropriate measures are taken.
2. Email attachments should be checked in an isolated environment instead of relying solely on antivirus solutions on users' computers.
3. Antivirus and other protection systems should be configured to send immediate notification when there's a suspected issue, and those notifications should be addressed immediately.
4. Security must be monitored continuously by a dedicated team using documented procedures and solutions.

Read the full report by Positive Technologies here.

Fighting the Threat of Social Engineering

There are multiple ways to fight social engineering, and using them in a layered approach is most effective. Here are a few tips:

Education
Ensure employees and customers are educated on social engineering and how to spot a scam.
Training: Ensure employees receive timely training. Train new employees as soon as possible after starting. Require regular, ongoing training for all employees.

SOCIAL ENGINEERING *cont'd.*

Testing
Establish a testing program to ensure employees can recognize a potential attack.

Password policies
Develop password policies and procedures that require strong passwords, require changing passwords on a regular basis and prohibit reusing passwords.

Multi-factor authentication
Implement multi-factor authentication to make it more difficult for hackers to access devices.

Patch management
Develop strong policies and procedures to ensure manufacturer updates and patches are deployed in a timely manner.

As cyber activity continues to evolve, financial institutions must continue to ensure up-to-date procedures are in place to prevent attacks.

Ohio Pooled Collateral System – One Year Later

By Sheila Schroer, Chief Bank Examiner

On July 1, 2017, the pooling method by which financial institutions collateralize public deposits changed significantly when the Ohio Pooled Collateral System (OPCS) became effective. The new program requires pooled securities be pledged to the state treasurer for all state and local public deposits. The burden for managing pledged collateral rests with the treasurer's office, which administers and monitors the program. Fifty-five institutions are using the OPSC and, of these, 27 are Ohio state-chartered banks.

Ohio Revised Code Section 135.18 provides two options for financial institutions to use to secure all public deposits. They can either use a specific pledge at 105 percent or the OPCS (O.R.C. § 135.182) at 102 percent ,or a lower rate when certain conditions are met; however, they must choose one of these options. All security interests in public deposits must be perfected.

If a financial institution uses a letter of credit from the Federal Home Loan Bank (FHLB) to collateralize the deposits of more than one public entity, it must participate in the OPCS. If the letter of credit is only pledged to one entity, then it does not have to participate.

Only deposits of public entities may be collateralized. If an institution is uncertain as to whether an entity's deposits are public funds, the burden of proof is on the public entity. It may not be evident from the entity's name (e.g., a volunteer fire department, local ambulance unit). The local government in question should contact its legal counsel, generally the prosecutor and have him/her contact the attorney general's office. Generally, the legal counsel for the entity needs to be the one to ask for this opinion.

For more information, questions or concerns, contact Lizz Lewis, director of Legislative, Policy, and Constituent Affairs, Ohio Treasurer of State, at 614-995-3773 or **constituentaffairs@tos.ohio.gov**.

Senate Bill 2155 § 213: Making Online Banking Initiation Legal and Easy

By Cathleen Hensel, Case Manager

On May 24, 2018, Senate Bill 2155 – the Economic Growth, Regulatory Relief, and Consumer Protection Act – was signed into law. Among other items addressed in the bill, it creates a national standard for financial institutions to accept scanned driver's licenses or identification cards for complying with the Customer Identification Program (CIP) when the customer's request for products or services is initiated through an online request.

Section 213 of the bill affects the retention of copies or electronic images of a customer's driver's license or personal identification card. Under the new law, these images must be deleted once the copy or image is used for the lawful purpose as prescribed by the Bank Secrecy Act (BSA), enabling a financial institution to form a reasonable belief that it knows the true identity of the customer

SENATE BILL 2155 § 213 *cont'd.*

obtaining a financial product or service. What is key is that Section 213 explicitly refers to products or services that are initiated through an online service defined as a website or mobile application. Images or copies of driver's licenses or personal identification cards for financial products or services applied for in-person are not required to be deleted under the bill. CIP rules under the BSA require financial institutions to obtain the following identifying information from each customer prior to opening an account:

Name

Date of birth

Address

Identification number

Verification of this information must be through documentary and/or non-documentary methods. The documentary method of verifying the information involves reviewing a non-expired government-issued identification document evidencing nationality or residence and bearing a photograph or similar safeguard. CIP record keeping requirements include describing the type of document(s) used, including the identification number, date of issuance and expiration date of the document. The CIP rules under BSA do not require a financial institution to make or retain a copy or image of the identifying document.

Many financial institutions currently retain photocopies or electronic images of their customers' government-issued identification cards as part of their CIP. These images also serve the dual purpose of identifying a customer when conducting in-person transactions within a branch. Financial institutions that currently are retaining copies or images of a customer's driver's license, identification card or other form of identification should consider the impact of S.B. 2155 and their online account opening practices. The institution's compliance staff should continue to monitor the new law for updated and additional guidance.

Medical Marijuana in Ohio

by Ingid White

House Bill 523 legalized medical marijuana in Ohio in September 2016. As the program continues to ramp up, financial institutions have been considering their appetite and preparedness to bank marijuana-related businesses (MRB).

An informal telephone survey shows Ohio's banks are at different points in their decision-making process. Some are still considering whether to participate in the industry while others indicated that they have a policy in place. Wherever banks are in the process, there are a few things to keep in mind.

First, if they haven't already, banks should have discussions about participation in the industry at the board level and consider developing and adopting policies for deposits and/or loans for MRB clients. Topics that can be discussed in these policies include account opening and closing procedures, account fees, internal controls for high cash volumes, source of funds tracking, board reporting frequency and, for lending relationships, concentration limits and ALLL methodology.

Second, banks should review their Customer Information Program (CIP) and Customer Due Diligence/Enhanced Due Diligence (CDD/EDD) procedures to ensure they include steps to ascertain whether the customer is an MRB. This will allow the institution to identify when to apply its MRB policies. One thing to note is that, if an MRB customer is intent on seeking an account relationship, they may try to hide their true identity and purpose for the account by using a misleading name, inaccurately describing business operations, structuring cash deposits or through other means. Additionally, businesses that act as ancillary businesses to MRBs may not be captured. Since both MRBs and ancillary companies may require some form of BSA reporting, a bank that relies on its existing CIP and CDD may inadvertently open and manage an MRB account or ancillary account that is not compliant with BSA reporting requirements.

Third, whether an institution opts to work with MRBs, it should be prepared for MRB-related questions during the examination process.

MEDICAL MARIJUANA *cont'd.*

Division examiners for both banks and credit unions are now asking questions about MRB risk assessment, BSA management and, if applicable, board policies and procedures for the provision of account services to MRBs.

If the institution has decided to open MRB accounts, examiners will ask whether the board has approved policies relative to MRBs. Examiners will also ask whether the institution has a written risk assessment for the MRB relationships or business line, and whether the institution has confirmation from third party providers that they will service the program (e.g., armored car company, ATM servicer, correspondent financial institutions, etc.).

Institutions that intend to open MRB accounts should also ensure their EDD form captures all appropriate information for the MRB and related individual(s), and they should revise their BSA policies to incorporate the increased reporting requirements for the MRB relationship. The BSA officer and staff must be properly trained, internal controls for red flag monitoring should be ensured and procedures for the filing of Limited/Priority/Terminated SARs should be adopted.

Also, examiners will inquire whether a legal opinion has been obtained to ensure the board and management have a full understanding of federal and state laws that may be applicable, including the seizure of property, forfeiture/subordination of collateral and uninsured losses. Financial institutions with MRB accounts should also have a contingency plan that details the closure of the account relationship should there be changes in federal or state law.

Banks that would like more information on how to comply with the FinCEN guidance for the Limited/Priority/Terminated SAR filing procedures can contact FinCEN at 800-767-2825 or FRC@fincen.gov.

Regional Roundtables

The Division of Financial Institutions is continuing its long-standing tradition of holding Regional Roundtable meetings this fall. These roundtable discussions allow for a unique opportunity for bankers and the senior staff of the division to meet, exchange ideas, and discuss topics affecting the banking industry both in Ohio and nationwide. This interaction provides the division with valuable feedback about your communities, competitive challenges, regulatory burden, concerns with the examination function, etc. In the past, we have used information gathered during these meetings to provide feedback to the Conference of State Bank Supervisors, adjust examination practices, formulate industry outreach opportunities, devise training opportunities for DFI examiners, and provide written guidance to our financial institutions.

This is your chance to meet with the Superintendent, Deputy Superintendent, Chief Examiner, Regional Supervisors and Case Managers of the division. It also provides an opportunity to meet with other bankers, many of which face the same challenges you do. Please join us at one of these five roundtable events. We want to hear your ideas, concerns and feedback.

Wednesday, October 10
Ohio University Inn
331 Richland Avenue
Athens, Ohio 45701

Thursday, October 11
Courtyard by Marriott
4375 Metro Circle NW
Canton, Ohio 44723

Tuesday, October 23
Quality Hotel Cincinnati Blue Ash
5901 Pfeiffer Road
Blue Ash, Ohio 45242

Thursday, October 25
Findlay Inn
200 E Main Cross Street
Findlay, Ohio 45840

Wednesday, October 31
Ohio Department of Agriculture
8995 E. Main Street
Reynoldsburg, Ohio 43068

Registration Website: http://www.cvent.com/events/odfi-fall-roundtables/event-summary-f80427c8ef17489e826843750f888bba.aspx

Ohio Banking Commission

Ingrid White, Chair, Division of Financial Institutions
John Brown, President/CEO, Security National Bank, Springfield
Fred DeBiasi, President/CEO, American Savings Bank, Middletown
Robert Lameier, President/CEO, Miami Savings Bank, Miamitown
William Martin, President/CEO, Mercer Savings Bank, Celina
Scott McComb, President/CEO, Heartland Bank, Whitehall
Jordan Miller, President, Fifth Third Bank, Columbus
James Smail, Former Chairman, The Monitor Bank, Big Prairie
Eddie Steiner, President/CEO, CSB Bancorp, Millersburg

How To Contact Us

77 South High Street
21st Floor
Columbus, Ohio 43215-6120

Tel: 614-728-8400

Fax: 614-644-1631

TTY/TDD: 800-750-0750

www.com.ohio.gov/fiin

Email: Web.dfi@com.ohio.gov

Kevin Allard,
Superintendent
Kevin.Allard@com.ohio.gov
614-728-2631

Ingrid White,
Deputy Superintendent for Banks
Ingrid.White@com.ohio.gov
614-644-7501

Ohio | Department of Commerce

Division of Financial Institutions

John R. Kasich, Governor
Jacqueline T. Williams, Director