Focus On...

Helping you bring your organization into focus.™

November 2020 • Volume 10, Issue 11

CYBER

Cybersecurity Threats in the Banking Sector

Over the last half a decade, cyberattacks have been considered one of the biggest threats to financial institutions. Cybercriminals' skill and techniques have evolved with technology; they have become more organized, forming groups like Lazurus, making it difficult for financial services to have the upper hand in the war on cybercrime. The loss from cybercrime is substantial in the banking sector, ranging from litigations, to cost of preventing another breach and a dent to the reputation of the institution.

Financial service providers such as the banking sector are more likely to be targeted compared to any other financial service sector.

Cybersecurity measures of financial institutions which adopt mobile and web delivery services tend to have a weak security system, making them ripe targets for cybercriminals. In addition, cybercriminals are sometimes able to hijack customer and employee information, using it to penetrate the bank's security system.

Let's look at the various cybersecurity threats facing the banking sector:

Identity theft

Every year it is estimated that the banking sector suffers a loss of over $10 million through identity theft. According to the research by Javelin Strategy and Research, over 15 million customers in the United States have fallen victim to this kind of fraud.

Identity theft occurs when someone uses another person's personal identifying information, like their name, identifying number, or credit card number, without their permission, to commit fraud or other crimes.

Threat from employees

Human error and disgruntled employees contribute to a large percentage of the risk.

Many employees use their personal devices to access the bank's services or use the bank's devices to check their personal email. This creates an opportunity for malware and phishing attacks sent to them disguised as a genuine request or offer.

Inside This Issue

Cyber: **Cybersecurity Threats in the Banking Sector**

Compliance: **CFPB Issues New RESPA Section 8 FAQS**

Awareness: **ALERT: Netflix Phishing Scam**

Focus Audits will be closed on Wednesday, November 11, 2020 in observance of Veterans Day.

FOCUS AUDITS™

CYBER

Additionally, disgruntled bank employees may steal sensitive bank information which they can decide to sell to cybercriminals.

Supply chain attack
Some networks have security vulnerabilities which can easily be accessed by a backdoor malware attack such as DNS lookup. This type of attack can allow a hacker to get remote access to the network and bypass the detection system without the user being aware.

Ransomware
The financial sector remains one of the biggest causalities of this attack.

Ransomware is a type of malware from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid.

Employees are prone to this attack when they open a link in a suspicious email which activates the malicious software into the system.

ATM malware and ATM jackpotting
ATM jackpotting is the exploitation of physical and software vulnerabilities in automated banking machines that result in the machines dispensing cash. ATM jackpotting cases have been rampant in Europe and the United States. With physical access to a machine, ATM jackpotting enables the theft of the machine's cash reserves, which are not tied to the balance of any one bank account. Thieves who are successful and remain undetected can walk away with all of the machine's cash.

The culprits use a portable computer to physically connect to the ATM along and use malware to target the machine's cash dispenser. In this bold public approach, an attacker will often use deception and weaker targets to limit risk, like dressing as service personnel to avoid scrutiny. Stand-alone ATMs in retail and service outlets are more likely targets, away from a bank's tighter monitoring and security. Older machines, which may not be fully up to date, are also common targets. ATM owners are encouraged to apply all available updates.

Synthetic identity theft
Synthetic identity theft is a type of fraud in which a criminal combines real and fake information to create a new identity. The real information used in this fraud is usually stolen. This information is used to open fraudulent accounts and make fraudulent purchases.

Synthetic identity theft allows the criminal to steal money from creditors including credit card companies who extend credit based on the fake identity.

Fraudsters who commit synthetic identity theft steal information from unsuspecting individuals to create a synthetic identity. They steal Social Security numbers (SSNs), and couple that with false information like names, addresses, and even dates of birth. Because there is no clearly identifiable victim in this kind of fraud, it often goes unnoticed.

People who commit synthetic identity fraud can use multiple identities simultaneously, and may even keep accounts open and active for months—even years—before the fraud is even detected.

Source: ***Oliviah Nelson, CyberExperts***

Wikipedia—Identity Theft

Wikipedia—Ransomware

Margaret Rouse, WhatIs.com

Investopedia

Focus On...

COMPLIANCE

CFPB Issues New RESPA Section 8 FAQS

The Consumer Financial Protection Bureau (CFPB) on Oct. 7, 2020, announced that it has rescinded Compliance Bulletin No. 2015-15 (Bulletin) regarding the Real Estate Settlement Procedures Act (RESPA). The CFPB replaced the Bulletin – RESPA Compliance and Marketing Services Agreements (MSAs) – with RESPA Frequently Asked Questions (FAQs) designed to provide "clearer rules of the road for [MSAs]." In deciding to rescind the Bulletin, the CFPB stated that the Bulletin "does not provide the regulatory clarity needed on how to comply with RESPA and Regulation X."

The new FAQs specifically include FAQs that discuss RESPA § 8 (a) as it applies to MSAs (MSA FAQs). They also include FAQs on RESPA § 8 in general, RESPA § 8(a), and RESPA § 8(a) as it applies to gifts and promotional activities, which are not addressed in this alert. This section will be confined to the MSA FAQs.

The MSA FAQs distinguish lawful MSAs from unlawful "agreement[s] for referrals," and indicate that the determination as to whether an MSA is a lawful MSA or an unlawful "agreement for referrals" "depends on the facts and circumstances, including the details of the MSA and how it is both structured and implemented."

The MSA FAQs also explain that a "referral" is an oral or written action directed to a person which has the effect of affirmatively influencing the selection of a particular Provider, such as handing clients a Provider's contact information; whereas a "marketing service" is not directed to a person, but is generally targeted at a wider audience, such as placing an ad in a trade publication. The MSA FAQs further explain that arrangements that purport to be MSAs but where the compensation being paid to the Source is based on the number of referrals are prohibited, whereas those involving marketing services that are actually provided and for which only reasonable market-value compensation is paid are not prohibited.

And, importantly, the MSA FAQs make it clear that "RESPA Section 8 does not prohibit payments under MSAs if the purported marketing services are actually provided, and if the payments are reasonably related to the market value of the provided services only," although a cautionary note is added that "under Regulation X, the value of the referral, i.e., any additional business that might be provided by the referral, cannot be taken into consideration when determining whether the payment has a reasonable relationship to the value of the services provided."

The MSA FAQs also make it clear that an MSA is or can become unlawful if the facts and circumstances show that the MSA as structured, or the parties' implementation of the MSA — in form or substance, and including as a matter of course of conduct — involves, for example:

- An agreement to pay for referrals.
- An agreement to pay for marketing services, but the payment is in excess of the reasonable market value for the services performed.
- An agreement to pay for marketing services, but either as structured or when implemented, the services are not actually performed, the services are nominal, or the payments are duplicative.
- An agreement designed or implemented in a way to disguise the payment for kickbacks or split charges.

Conclusion and Takeaways

While further guidance regarding specific structuring and implementing issues that might cause an MSA to cross over the line from compliant to prohibited would be helpful, the CFPB's decision to rescind the Bulletin and issue the FAQs appears to be a step in the right direction.

Source: Lexology.com

AWARENESS

ALERT: Netflix Phishing Scam

If you've checked your email any time recently, you've probably seen a plethora of junk messages relating to COVID-19, your bank and bills in need of attention. If you haven't already guessed, most of these are spam and scams, but why are so many of these obvious traps slipping through our filters so easily?

The answer is complicated, but it has to do with the fact that more people are online than ever these days. Between coronavirus lockdowns and the shuttering of mass gatherings and entertainment, the online population is far larger and riper for exploitation by hackers. Tap or click here to see why there are so many phishing scams nowadays.

To make matters worse, a new scam is circulating that poses a unique danger to your bank accounts. This phishing email looks like a real message from Netflix describing a billing error with your account. But if you make the mistake of filling out the form it links you to, your entire bank account can be drained.

Netflix is urging subscribers to avoid opening a phishing email that claims to come directly from the company. If it appears in your inbox, interacting with the message can give the hackers behind it access to your bank account — and potentially other personal data as well.

Here's how it works:

The email arrives with an urgent alert that there has been an error processing your monthly Netflix payment. In the text, you're prompted to click a link to update your payment and account information.

Clicking the link takes you to what appears to be Netflix's website, but filling in your payment details and account information results in your card information, email and password being harvested by scammers.

But that's not the only danger surrounding this scam. Many incarnations of the email include what appears to be a text file as an attachment. Downloading this attachment can potentially result in ransomware or other malware being installed on your computer on top of the phishing issue. It's a double-whammy of scam in one message!

The threat of ransomware is everywhere these days. That's why it's important to back up all of your essential files with a company you can trust.

But as bad as this scam is, it's actually quite easy to detect and avoid — even if you've accidentally ventured deeply into the scam site.

As with nearly every phishing email claiming to come from an official source, the easiest telltale sign to look for is the sender field of the email itself.

If you get a suspicious email or text, Netflix has a help page. Click here for instructions.

You can also manually log into your account on a separate browser, not clicking on the links in the emails, and checking the status there.

Boston 25 News, Natalie Dreier, Cox Media Group National Content Desk
Updated: September 4, 2020 - 12:21 PM

Komando.com, James Gelinas, July 29, 2020

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com