FRAUD PREVENTION FRIDAY

Friday, July 12, 2024

Top News

Fraudsters' Growing Use of Call Forwarding

- Fraudsters are increasingly resorting to call forwarding to receive one-time passcodes (OTP) as part of their persistent endeavors to gain online access to and take over bank and other financial accounts.
- Call forwarding allows the fraudster to redirect incoming calls from the victim's phone to a phone number in the fraudster's possession.
- Unlike SIM swapping, where the fraudster gains full control of the victim's cellular service, malicious use of call forwarding only temporarily pauses incoming calls to the victim's phone but otherwise the service is not interrupted.
- The simultaneous ring function offers similar opportunities to fraudsters without impacting the victim's ability to receive calls. In this technique, multiple phones can be reached by dialing the victim's phone number1.
- The use of call forwarding to receive OTP codes appears to be attracting interest from fraudsters when attempting to access compromised online bank accounts.
- Chatter surrounding compromised online bank accounts advertised with call forwarding access increased by 226% in 2024 vs. 2023.
- Telegram chatter reveals several strategies for activating call forwarding on a victim's phone, including the use of insiders at phone companies, obtaining the victim's wireless account credentials, and social engineering.

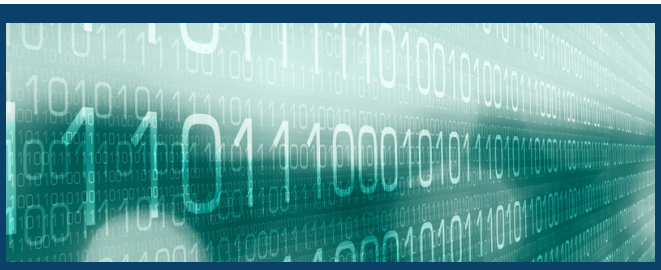
Patelco Credit Union Cyber Attack

Patelco Credit Union has assets of $9 billion, 750 employees, and over 450,000 members nationwide.It is the 22nd largest credit union in the country, operating 37 branches throughout Northern California.

On June 29, 2024, Patelco Credit Union experienced a ransomware attack. As of July 11, 2024, almost two weeks after the cyber incident, they are still recovering systems, and many services are still unavailable for their members. In response to the incident, the credit union proactively shut down some of its day-to-day banking systems to contain and remediate the issue, including online banking, their mobile App, and call center. While electronic transactions such as transfers (including Zelle), direct deposit, balance inquiries, and payments are still unavailable, members can access cash from ATMs in limited amounts. Debit and credit card transactions are functioning but in a limited capacity. They are experiencing longer than normal wait times in their offices and on calls.

Since the initial event on June 29, 2024, Patelco Credit Union has been the target of two class-action lawsuits because of the data breach and possible exposure of personal information.

(Continue reading below.)



Key Takeaways from a Wiperware Cyberattack Simulation

Wiperware can literally wipe out all your institution's systems, including backups — are you resilient enough to withstand such a cyberattack? Wiper malware is malicious software that is designed to delete files or destroy data on any device it attacks.

To test the industry's resilience, NACHA and the Global Resilience Federation (GRF) — a nonprofit that offers multi-sector cyber and physical security information and education — conducted two exercises in March and April of this year. These exercises were based on the Operational Resilience Framework, developed in conjunction with industry stakeholders and financial regulators.

The goal was to test the operational resilience of financial institutions and help them assess how to reach minimum viable service levels after a wiperware attack that included an outage of ACH payment systems. That way, even if they couldn't be completely up and running, they could at least deliver direct deposits, online bill payments, and other key services.

We invited Bill Nelson, Chairman of the GRF, to be a guest writer for this article and share information about the tabletop exercises and the insights gained through them.

Patelco Credit Union Cyber Attack - Continued

The lawsuits were filed on July 1 and July 3 on behalf of two Patelco customers and others "similarly situated." They both allege the Dublin-based credit union has not safeguarded customers' personal information, such as account numbers, Social Security numbers, and addresses, from the data breach. One lawsuit was filed by a California resident named Shawn Kent in Alameda County Superior Court, claiming that Patelco "intentionally, willfully, recklessly, and/or negligently" failed to protect its clients' private information.

"This is especially true given that (Patelco) is a large, sophisticated operation with the resources to put adequate data security protocols in place," the suit filed by attorneys Scott Edward Cole and Laura Grace Van Note said. They are seeking class-action status.

The Oakland-based attorneys also wrote that Patelco caused a "substantially increased risk of fraud, identity theft, and misuse" of its clients' private information. Kent wants to ensure his private information "is protected and safeguarded from future breaches," the suit says.

On July 9, 2024, the president and CEO of Patelco, Erin Mendez, announced its network is "stabilized," and transactions are now being processed as the devastating cyber-attack that crippled its systems remains unsolved.

"Once this is complete and we achieve full banking functionality, our members will be able to access their account balance and accounts as they typically would under normal circumstances," she wrote. "I can't share an exact date when we will be back to business as usual, but we can see the light at the end of the tunnel."

Their website information shares their infrastructure is stable and secure, and they are making positive momentum daily toward their final goal: getting back to business. They hope to have systems and information updated by the end of this week. Once that happens, they have shared they will be able to confirm the date when members will be able to access their accounts.

Once they are fully online and back in business, there will undoubtedly be many antidotal assessments of what happened, how it happened, why it happened, and more. The state of their business may well look very different as everyone moves forward with more internal security. It is also likely many of their members will look to place their financial assets and trust elsewhere.

This is a stark reminder for all community bankers of how critical processes, procedures, training, and trusted partners are to the success of our industry. We have consulted with several CBM IT partners and want to share the following reminders and recommendations as a result of these conversations:

- Do you have a business continuity plan that has recently been reviewed, including robust and frequent tabletop exercises?
- Do you have an incident response plan in place with the same testing?
- Who do you partner with regarding your cyber insurance?
- Do your banking processes follow what you have shared in your insurance application to ensure what you said you are doing is being done in daily practice?
- Most cyber breaches have occurred because of employee error. Are you training employees regularly using a variety of methods and tactics?
- Are employees using caution and verifying information from every source, vendor, law, CPA firm, and associations – including the CBM?

IT and cyber security remain a top priority for all community banks. Don't take your eyes off this critically important area of the business, as the consequences can be devastating.

DID YOU KNOW

32 Community Banks joined yesterday's Q6 Cyber Check Fraud - A National Pandemic Webinar. Contact KateAngles@cbofm.org if you missed the webinar and are interested in watching the recording.