July 2024

Member Insights

MERCK EMPLOYEES
FEDERAL CREDIT UNION

Member Spotlight: Stolen Check Leads to Sophisticated Fraud

Happy summer to all our wonderful members. On behalf of everyone at the credit union, we wish you a safe and fun summer season. Here at the credit union there are a lot of exciting things happening. Please check out our Summer Specials on page 2. I also want to thank everyone for their patience during our recent systems conversion. The conversion ensures the credit union maintains its safety and soundness and is offering our members a safe and effective banking experience. Speaking of change, there is one further change to note. The credit union's main member service number has changed. The new member service number is 732-484-4811. This month we are pleased to present a one-on-one dialogue with one of our members, Anthony Sabatelli. Mr. Sabatelli graciously agreed to be part of a Q&A based on a recent fraud attack he experienced that stemmed from a stolen check.



Gentile: Thank you Mr. Sabatelli for being willing to share your story. First, please tell us about yourself.

Sabatelli: I am a long-time credit union member. I appreciate the safety of the credit union and the great service. I am a former Merck Intellectual Property attorney and still appreciate the tie to the credit union and those great days. I worked at the Merck Rahway site for many years, and I now reside in Connecticut and work at a law firm.

Gentile: So how did you discover the fraud?

Sabatelli: This all started when I mailed a check and it never made it to the recipient. After a number of weeks, I grew concerned and put a stop-payment on it to protect myself. I know mailing checks is not ideal as there is a lot of theft, so I started to get worried. I do want to point out that I thought I was protecting my mailed check by mailing the check at a U.S. Postal Service office and sending it to a P.O. Box, but clearly that was not sufficient.

Gentile: Yes there is now a lot of mail theft and that is why we advise all of our members to avoid mailing checks. They are stolen right out of the mail, washed and deposited fraudulently. But your fraud was deeper than that. What happened next?

Sabatelli: The fraudster obtained my account information from the stolen check, but they also created a fake ID. The picture didn't match me, but they did somehow get my correct Driver's License number. The number was correct but the expiration date wasn't. In any event, they created a pretty good fake license. They went to Shared Branching locations in California and withdrew approximately $2,800 in cash.

Gentile: This is deeper than we usually see. Rather than just washing the stolen check, they went a step further and created a fake ID. Your account information though was obtained by the check. I know that most members know this but it is worth nothing again that at the bottom of your check is the credit union's routing number as well as the member's account number. That's a lot of information for fraudsters to work with. Many checks also have the member's address so now you are talking about a lot of data. Other than the anxiety and concern about the fraud what else did you learn about the fraud process that might help other members?

Sabatelli: I recommend that people check in on their accounts regularly. That's how you know if something hasn't cleared or there's an incorrect charge. You also have to go through all the channels. I contacted the credit union immediately and they guided me through the recovery process, but you will also be speaking with the police and filing a police report. All these things have to be done when you're a victim of fraud like I was. In this case I also learned about Shared Branching.

Gentile: Shared Branching is a credit union system feature that allows our members to go to other credit union branches through the country to do transactions. We do believe most things can be done remotely and that is why we have seen Shared Branching transactions decline to only about 1,000

IMPORTANT

The credit union's main member service number is now 732-484-4811.

(Continued on back)

(Continued from "Member Spotlight...")

transactions a month. Members should know the Shared Branch locations have ID requirements and are held to a high standard but in this case the fake ID allowed the fraudster to withdraw cash. Fortunately we have cash withdrawal limits in place to reduce the amount of cash that can be taken from a Shared Branch. There's also a process in place to recover the funds. Mr. Sabatelli, in the case of your credit union fraud, we were able to recover the funds and re-issue your accounts to further protect you, but are you worried about more fraud happening given that someone created a fake ID in your name?

Sabatelli: I certainly am and that's why I took more action. I put a freeze on my credit. I have set credit alerts set up on all my accounts and am notified if any credit attempts are made. I am just paying very close attention now to any activity. I also am using identity theft protection. It's unsettling, but I do feel like I've taken the right steps. As for mailing checks…I certainly won't do that any more!

Gentile: Thank you for sharing your story and we wish you well and we will continue to be here to assist you and all of our members who deal with fraud. The two big takeaways from this case are please try to avoid mailing paper checks at all costs and also check in on your accounts regularly. The sooner we are made aware of fraud, the smoother the recovery process will be.

Fraud Tip: Digital Wallets Can Help Protect Against Latest "Skimming" Fraud

New Jersey has seen a rash of card "skimming" attacks recently where fraudsters place devices on ATMs, credit and debit card readers and "skim" your credit or debit card information to defraud you.

Recently, the Aldi supermarket chain announced skimming devices were found at check-out terminals in its stores in Roselle and Union, NJ. The skimming devices have been in place for many months, but they were just recently discovered by Aldi, meaning customer card data was exposed for a very long time. Wawa also recently announced similar "skimming" breaches at many of its locations.

These skimming devices are just one more potential fraud that consumers must protect against as criminals get bolder and bolder trying to steal your data.

Fortunately, there is one powerful tool that credit union members can use to protect themselves against the "skimming" fraud. Your Merck Employees Credit Union Visa Credit and Debit cards can be added to ApplePay, SamsungPay or GooglePay, which utilize tokenization to protect your data at checkout. Unlike debit and credit cards, which use the 16-digit number on the card for every transaction, digital wallets use a different randomly assigned number for each transaction. This allows you to skip the card reader where a skimming device could be lurking and use your mobile device for convenient and safe payments.

Digital wallet payments have become more universally accepted, making the Digital Wallet a powerful tool to combat fraud. As an example, both Aldi and Wawa accept Digital Wallet payments.

More and more credit union members are utilizing Digital Wallet capabilities from the credit union. If you need more information, please call 732-484-4811 Opt. 4.



MERCK EMPLOYEES FEDERAL CREDIT UNION
Your Prescription to Financial Health.

Member Services: 732-484-4811 Opt. 2
Loan Department: 732-484-4811 Opt. 1
Debit Card Lost/Stolen: 800-554-8969
Credit Card Lost/Stolen: 800-237-6211

Established in 1936, Merck EFCU is federally-chartered and federally insured by the National Credit Union Administration.

EQUAL HOUSING OPPORTUNITY

NCUA

Featured Loan & Deposit Rates

Auto Loans as low as 5.35% APR*	E-Checking 0.125% APR*	Credit Cards as low as 13.50% APR*
Share Cert. 6 months 3.85% APY*	Share Cert. 12 months 4.50% APY*	IRA Cert. 6 months 3.85% APY*
IRA Cert. 12 months 4.50% APY*		
Savings 1.25% APR*	IRAs 1.80% APR*	Home Equity as low as 8.50% APR*

**Annual percentage rate. Visit www.merckcu.com or visit a branch for more information.*