### (Approx. 979 words)

### Credit Card Fraud (A Personal Experience)

By Tom Burt, Vice President
Sun City Summerlin Computer Club
<https://www.scscc.club>

tomburt89134 (at) cox.net

Mrs. Burt and I recently experienced an unusual form of credit card fraud. There were various ramifications, and it took us about four weeks to completely resolve the issue with the credit card company. First, I’ll share the story and then discuss some of the implications and steps you can take to help prevent having a similar experience.

## Strange ATM Withdrawals

Mrs. Burt regularly checks our various credit card accounts online to watch for fraudulent transactions. On one of our cards, she noticed some ATM cash advance transactions in a small town in Iowa. In all, there were three that had occurred within a day of each other.

We called the credit card company immediately to report the transactions as fraudulent. The service rep canceled the current card number and arranged to send us new cards. So far, so good. In discussions with the service rep, she suggested we set up a PIN number on the new cards so that only someone who knew the PIN could make ATM cash advances.

## An Illegitimate Extra User

Two days later, after receiving and activating the new cards, Mrs. Burt logged in to the online website account for that credit card to set up the PIN. When she selected that option, the website asked, “For which authorized user? And displayed a list with her name, my name, and the *third name of someone who lived in Iowa*. This provided the missing link as to how someone in Iowa had made an ATM cash withdrawal against our credit card. When they issued us new cards, they carried this illegitimate user over to the new card (and probably sent him a new card as well!).

We called the credit card company again, explained the issue, and connected to the security and fraud division service rep. She deleted the unauthorized user, but after conferring with a supervisor, she told us they would have to kill the newly issued card and issue us another new card. The security and fraud rep did some digging and advised us the illegitimate user had been added due to a telephone transaction. This was a surprise. We had gotten NO notice by email or phone that a new authorized user had been added to our card.

This person in Iowa came by Mrs. Burt’s card number and enough personal information to have a female accomplice call the credit card company and impersonate my wife well enough to get them to add his name and address to our card as an authorized user. So, they sent a card to his address in Iowa. Once he had it, he immediately started getting cash advances. Luckily, Mrs. Burt noticed these within a few days.

Our account with the credit card company is now back in operation with a PIN required for ATM cash advances. At the suggestion of the security rep, we have also added a “verbal password” that any caller must provide before they can do any transactions with a service rep.

## Secondary Consequences

Because we didn’t know the extent of the fraudster’s penetration of our security information, I had to immediately move to change the passwords on all our online financial accounts. This was a serious bit of work, but absolutely essential. Once we had a clean card with the credit card company, because we use it for recurring charges, I had to go to several websites (for example, Amazon.com) and update the credit card information. In all, I spent about 8 hours getting everything reworked. A lot of this time was spent meticulously recording all the changes in our LastPass password manager. As I write, I still have work to do to reconnect Quicken to our financial accounts to download transactions.

## Preventive Measures (*See also Jeff Wilkinson’s June 2021 article*)

Our Sun City Summerlin Computer Club offers members a lot of information on how to be more secure. You can find this material on the club website at <https://www.scscc.club/smnr>.

One key thing we did several years ago is to set up **security freezes** at all three of the major credit bureaus. This prevents a fraudster from opening new credit accounts in our name.

We avoid having merchants or service providers keep our credit card numbers on file with very few exceptions. You can’t depend on these merchants to keep your information secure.

We also make it a point to use **very strong passwords** on all our financial accounts and do not reuse the same passwords on different sites. It’s also essential to change these passwords from time to time, even if there’s no sign of fraud. If available, we use two-factor authentication.

It’s critical to monitor *all* financial accounts regularly to detect any fraudulent transactions. The sooner you detect a problem, the less grief you will experience.

We also keep personal information on social media sites to a bare minimum. That makes it harder for fraudsters to impersonate you.

## Conclusions

We don’t know how the fraudster came by our card number and the personal information used to convince a service rep at the credit card company to add him as an authorized user to our account. Most likely, it was picked up from the dark web after some merchant’s sales databases got hacked.

I’m bothered that the credit card company would add an authorized user in response to a phone call without sending an email alert. Also, we had never heard about adding a PIN for cash advances or a “verbal password” for phone transactions. We plan to put these in place, if available, on our other cards and accounts.

We, fortunately, incurred no significant economic losses from this incident, but it did eat up a lot of my time, and we were both feeling quite a lot of stress.