Esto Perpetua
MAY IT LIVE FOREVER
150TH ANNIVERSARY
GRANGE

# The Capitol Granger

*Regular news from your Grange lobbyist*

## Does super cyber hack reveal weakness in laws on credit reporting firms?

**by Craig Loughridge**
**Assistant Director for Governmental Affairs**

I'm going to go out on a limb a bit this month, and share a personal story. And one that's a little long. There's a point, so please bear with me.

I work in Salem not far from the capitol. As with many cities these days, you can't park your car without paying. And, as with many cities the size of Salem, that means using a parking meter that is as likely as not to take cash or coins. I've grown used to using my plastic to feed the meter.

I got an unusual response when I tried to feed the meter in a parking lot on July 12. Nothing happened. I tried again. Still nothing happened. On the third try, I watched the meter more closely. I waited, and waited. Then: "Card not authorized," read the reply on the meter's screen.

What? I thought. That can't be. I had checked my account balance early that day, and my account had far more than the mere $6 that the meter required. Let me try that again.

"Card not authorized," the machine insisted.

Now wait a minute, I thought. I'm going to call my bank. This is crazy.

After several minutes on hold, and a brief chat with one banker, I was now talking to a polite but mechanistic other banker in the fraud division. She wanted me to tell her if I had the card with me, if I remembered what my last couple of charges were, and whether I was in Maine.

"Maine?" I asked with astonishment. "I'm trying to use the card in Oregon."

"There's a $100 charge this morning at a JC Penney store in Maine," she said. "Is that yours?"


"No! I've never been to Maine."

The card, she explained, was canceled for suspected fraudulent activity.

I had no idea how any of this could have happened, but I worked with her to put through a one-time charge for the parking fee, then re-cancel the card and get a new one. She would send me a form to have the $100 charge in Maine taken off my account. And that was pretty much that. Score one for the fraud division; and I'd have my new card soon.

Or so I thought.

My new card did come. Things did get back to normal.

Then my wife received a robocall on Aug. 19. As with all robocalls we get, she hung up as soon as the computer voice started talking.

Later, as she was handling the phone in preparation for calling her mother, she noticed the name from the previous call.

"Clackamas FCU," the caller ID screen read.

That was odd, she thought. Could that robocall have been legitimate? Could it really have been our credit union? Why would they call us on a Saturday night?

After much Googling, and time on hold at numbers that never answered, there she was, finally on the phone with a real person—a mechanistic telephone banker in some dimly lit call center, asking if she'd made a $200 charge in someplace called Santa Clarita, Calif.

You can guess my wife's response.

The call ended with the result that her credit union debit card was canceled. She'd have to go into the branch on Monday to get a new one.

It began to dawn on me as my wife described her phone call that the problems with her card and mine might not have been just coincidence. They were different cards on different accounts at different financial institutions. Somewhere, I thought, there had to be a connection.

We thought and thought, but couldn't puzzle it out. The reality of our daily lives was that we almost never made purchases at the same places. The odds that someone locally had somehow gained access to both accounts just seemed so remote.

## The light bulb moment

As summer moved on, and Labor Day came and went, we were starting to feel more secure about our finances. We had taken out a small home equity loan with no credit report woes. The confounding existence of the mystery debit card thieves was starting to drift out of our conversations.

The first full week of school had ended, and I was taking a break from a weekend school board meeting when I started browsing news headlines on my phone. There amongst the reports of fire and deaths, political turmoil, and other tragedies was a partially visible headline about a computer hack.

Perhaps I would have seen more of the headline if I hadn't been on a phone. I almost didn't stop and read the article. When I decided to tap the headline, I saw news of a cyber attack against the giant credit reporting agency Equifax.

How boring, I thought. We see news reports of computer hacks virtually every week. What's unusual about this one?

I was about to stop reading and move on when it dawned on me: *This* was the connection. Sophisticated cyber criminals had gotten into our private, financial information on Equifax's computers. They had used our stolen account details to duplicate our debit cards.

A visit to the Equifax website a few days later confirmed my suspicions.

"Based on the information you provided, we believe that your personal information may have been impacted by this incident," said an automated reply on the website.

That information in hand, we now had to assess our future risk, and decide how to respond. I searched the Web, and found great information on several websites.

Armed with tips from the Federal Trade Commission's website, we worked out a plan to file an "Identity Theft Report" for each of us with the FTC before adding fraud alerts to our data at the three major credit bureaus. The instructions on the FTC website made it sound simple enough.


## What are computers for?

Computers are supposed to make our lives easier. You can do just about anything with a computer these days. Starbucks has my morning coffee ready for me when I walk in because I order, and pay for it, with my phone. I can buy groceries online, check theatre times, and even have a Big Mac and fries delivered. I can use one credit bureau's website to place a fraud alert in my file with all three credit bureaus—as long as I don't want it to last any longer than 90 days.

Keep in mind that a cyber criminal can keep all of my identification information forever. He can even post it on the Web for others to find and use. So, what

good is a 90-day fraud alert?

The credit bureaus also offer an "Extended Fraud Alert" that consumers can have placed in their files for seven years. The catch is, you can't submit your request with a computer, and you have to use regular mail to send the same personally identifying information that the credit bureaus have already proved they can't safely handle. And you have to submit the request separately to all three bureaus.

If a credit reporting company can share a 90-day fraud alert with its sister companies, why can't it share an extended fraud alert the same way? If a consumer isn't seeking to obtain information, but to submit it for the purpose of avoiding fraud, why does the consumer need to mail in paper copies of a photo ID and a social security card with the request? Since state-certified, government-run law enforcement agencies will take an ID theft report over the phone, and without any proof that an actual crime occurred, why do some credit bureaus insist on having a police report accompany the request?

The reality is there's no reason that putting a fraud alert or a credit freeze into your files at all three credit reporting agencies can't be done online in the span of 30 minutes. Instead, all three companies burden consumers with pointless steps and paperwork that literally draw the process out to days.

In a computer world, where almost every transaction involving money or credit can be completed instantaneously over the Internet, time counts. Demanding days to do something that can accurately and reliably be done online in minutes is nothing short of reckless.

*White Clover Grange #784, east of Nehalem in Tillamook County.*

But what can be done to make the credit reporting firms be more responsive? Does state government have the power to compel needed changes? Even if legislators or state agencies have the power, are they willing to use it?

I will explore this in the next issue of The Capitol Granger. Please keep your eyes on your email to get next month's edition.

Meanwhile, be sure to check the Equifax website to see if your personal data was compromised. Go to www.equifaxsecurity2017.com, then click the "Potential Impact" link under the headline near the top of the page.

## More Resources to Protect Yourself from the Equifax Data Breach

*Blog tips from the Federal Trade Commission:*
www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

*FTC website to report fraudulent use of your information:*
www.identitytheft.gov/Info-Lost-or-Stolen

*Email comments or questions about The Capitol Granger to: govaffairs@orgrange.org.*