Social Fraud Podcast Transcript

Welcome to the Golden 1 Credit Union Financial Wellness Podcast. I'm Martin, and I'm here with Rebecca. Today we are going to cover a topic that, unfortunately, too many people have experience with: Social Fraud.

Martin, social fraud happens all the time. Usually, we aren't aware that we are being tricked and so we willingly give up our information because these fraudsters are so good at making their scam seem like it is a real, quick, and easy way to earn a few extra dollars. Sometimes people engage in fraud without realizing they are actively participating in it. I know what our listeners are probably thinking, "This could never happen to me. I'm too smart to let anyone pull one over on me." Well, I'm here to tell you it could happen to you! The Better Business Bureau reports that in 2018 alone they received 50,559 scam reports. That's up from 47,827 in 2017. We are not getting more gullible, Martin, the fraudsters are getting smarter.

Those are some scary numbers, Rebecca, and you're absolutely right. These fraudsters run scams all day, every day. If they didn't work, they wouldn't keep doing them, right? Let me give you an example of how one of the most common forms of fraud happens: On social media - Facebook, Instagram, Snapchat, or something like that - a fraudster will reach out to you if they see that you just started following a certain financial institution, or maybe you commented on a social media post from your financial institution. They will start by trying to send you a direct message or a friend request and then propose a scam that seems too good to be true – just hand over all of your account information so the fraudster can mobile deposit a check directly into your account and you'll have hundreds of dollars for free! That should already be a red flag, right? But these fraudsters are so careful about who they reach out to, that most of the time the victim is more than willing to get involved.

That's right, Martin. So, once the check has been deposited and the money is available for withdrawal, the fraudster will ask you to buy gift cards or money orders for almost all of what the deposited check was worth, what's left you get to keep for yourself. You send the money orders to the fraudster, and buy the thing you've been wanting to buy with your left-over money. But, Martin, guess what happens a week later.

Nothing?

Wrong. A week later the check is returned to your financial institution because it's fake and now you, not the fraudster, are responsible to pay the entire amount of the returned check. Easy money for the scammer, and a huge headache for you.

Ok, but since it's obvious that fraud took place, the victim should not be held liable, right?

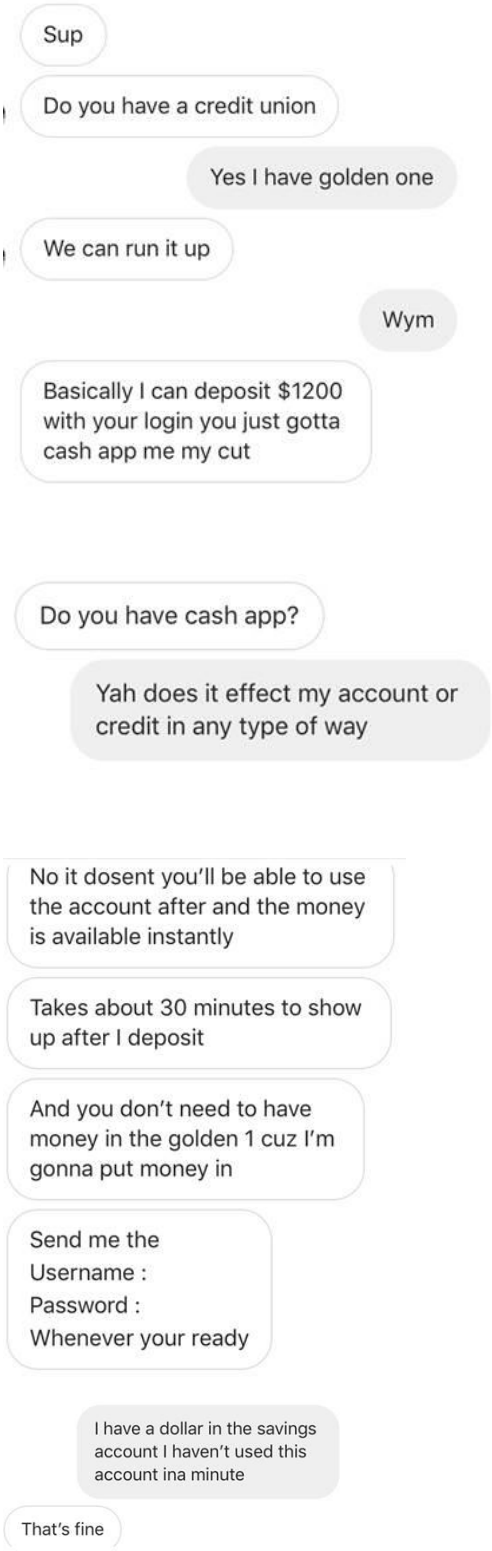
In the case we just discussed, you willingly gave your account information to the fraudster. Even if you didn't know for sure if the proposal was real, you gave your account information with all your passwords and security information. This puts the blame entirely on you, and you can't be protected. You, now owe that money. If your account gets hacked without your knowledge, and money is stolen from you, then, yes, you would be protected.

So, if I have a joint account with a family member, I have to pay for the mistake they made?

Most likely, yes you will have to pay. I mean if they're willing to give account information because they need money so badly, do you really think they would be able to cover the returned check?

Wow, it's scary how easy that is. Let's read an actual transcript from one of these fraud events that was reported to our fraud investigation department. This interaction is 100% real, but names and account info have been removed to ensure privacy. I'll be the fraudster, and Rebecca, you be the target. Ready?

Ready!



It really is as quick and easy as that, Rebecca. In this example, the victim was tapped for $10,000.

But we aren't here just to deliver doom and gloom. Of course there are steps our listeners can take to reduce the likelihood of becoming a victim of social fraud. The most important thing to know is that there is no such thing as quick, easy money, especially when it's being offered by someone you don't know through social media channels.

I mean, why would anyone go to work if it really was that easy to make a quick buck? Another thing to keep in mind is that you should never, under any circumstances, offer your account information to anyone, unless that person is a co-owner on the account, or course. That means you shouldn't give information out to your best friend, or your children, or your parents. The only person that needs to know your account information is you and you alone.

Unfortunately, this podcast might be reaching some of our listeners too late. Some of them may have already fallen victim to a fraud like this and they're wondering what to do now.

That's right, Rebecca. So sad and alarming. Well, hopefully we can help! If you have become the unfortunate victim of one of these fraudsters, the first thing to do is to contact your financial institution and let them know that your account has been taken over so that it can be flagged or put on hold and hopefully no more damage will be done.

If you can, try to return the money you took out to your bank account so that you will be covered when the bad check is returned. Reach out to the company that you used to send money to the fraudster and see if you can cancel your transaction before it's fully deposited into their account.

But, of course, the best protection, is to never get tricked in the first place. That is easier said than done. Always be cautious when someone contacts you out of the blue, especially if you don't know them!

Don't click on links or open any attachments that come from an email address you don't know.

This is just good advice all around, but especially good advice if you don't want to become the target of a fraudster: be careful about what you share on social media. The more the fraudsters know about you, the more they will be able to take advantage of you.

No one is perfect. We all make mistakes, and, for the most part, you can count on your financial institution to be up to date on all the latest ways people commit fraud and to be actively monitoring accounts for signs of fraud. If you want to do a little bit of research on your own, visit www.ftc.gov for a breakdown of every type of fraud they are aware of. Odds are, if you think you've been scammed, the scam is listed there.

Not to scare our listeners or anything, but engaging in fraud willingly is technically illegal and it's possible criminal charges could be filed. If you can't afford to pay back the money, it could get sent to collections, and you will likely get reported to ChexSystems, which will make it much harder to open a new account in the future.

We know that we just threw a bunch of frightening information at you, but we don't want to scare you off of social media, we just want you to be aware of what's happening out there so you know how to avoid becoming an unfortunate victim and another statistic.

That's right, Rebecca. We want everyone listening to be safe and smart when they are online. Be aware of who you're talking to and how much information you share.

Ask questions to verify who you are talking to, or, better yet, don't talk to anyone you don't know.

Keep your financial institution's phone number handy so that you can reach out to them in case you need to contact them.

And whatever you do (both together) **DON'T SHARE YOUR ACCOUNT INFORMATION WITH ANYONE!**

I hope we've made that point clear enough, Rebecca, what do you think?

I think so, Martin. If our listeners would like some more information about what they can do to avoid fraud, or what to do after fraud has occurred, they can head over to www.golden1.com/privacysecurity/fraud for online banking tips, phishing avoidance tips, identity theft avoidance tips, and more.

For more general financial education information please check out www.golden1.com/financialwellness where we've got videos, podcasts, and interactive modules that cover just about any topic.

And the best part is you don't have to be a Golden 1 Credit Union member to use these resources. They're free for everyone!

Be careful out there! Remember, there are hundreds of different techniques that fraudsters can use to take your hard-earned cash, and they're coming up with new ones all the time. If you want, share some of the information in this podcast with your loved ones so they can protect themselves, too.

With Golden 1 Credit Union, this has been Rebecca…

And Martin…

Wishing you financial health and happiness. Thanks for listening and (both) **STAY GOLDEN!**