BBB NEWS
Better Business Bureau
Serving Minnesota and North Dakota
220 S. River Ridge Circle
Burnsville, MN 55337
651-699-1111
651-699-7665 (Fax)

FOR IMMEDIATE RELEASE

Watch Out for Cellphone Porting Scam

Burnsville, Minnesota – March 13, 2018 – Did you know that someone could steal your cellphone number and 'port' that over to another carrier without your knowledge? This is a newer scam and it's been happening around the country - including the Twin Cities. It's also a new means through which scammers can steal your identity and withdraw funds from your bank accounts. The scariest part is that this type of scam, called cellphone porting or port-out scam, uses your safety protocols to gain access to your financial and personal accounts and logins. Better Business Bureau® of Minnesota and North Dakota (BBB) offers insight into this new scheme and tips to help people protect themselves from it.

"We've seen this scheme locally and reports of it are popping up nationally," said Susan Adams Loyd, President and CEO of BBB of Minnesota and North Dakota. "It's definitely something new, and we want people to both be aware of it and to take steps to avoid this scam."

Think of how many times you've set up an email address, social media account, or logged onto your bank account online or had to change your password. How many times did you have to verify your identity by being sent a one-time code via text message? Now what if you weren't the only one who was reading that message? This new type of scam could potentially bypass that layer of security and might open the door to your identity being stolen without your knowledge.

How does the cellphone porting or port-out scam work?

A scammer acquires your name and phone number and then attempts to gather as much personal identifiable information (PII) as they can about you. PII includes your name, address, Social Security number (Social Insurance number in Canada), date of birth, and other information that can be used for identity theft – including where you bank. They then contact your mobile provider, pretending to be you, and inform them that your phone was stolen. They request that the number be "ported" over to another provider and device. In some cases, if they were bold enough and in a retail location - and/or online - they might even try to buy a brand-new phone

which could give a sales representative enough assurance to quickly fulfill their request and forgo some formal verification procedures.

The scariest part? Once they have your number ported to a new device they can then start accessing and gaining entry to accounts that require additional authorization in terms of a code texted directly to your phone for security verification. Those added security measures are usually in place on accounts provided by email providers, social networks, tax preparation software, and even financial institutions. Victims of port-out scams may not know this has happened until they notice their mobile device has lost service, or when they receive unexpected text messages containing account authentication/access codes.

"Our understanding is that scammers might have a lot of sensitive information – including where people bank and so forth – from information gathered through online phishing schemes or previous hacks and data breaches," added Adams Loyd.

BBB offers these tips to help protect yourself from this type of scam:

- **Talk to your cellphone provider about port-out authorization.** Every major wireless provider has some sort of additional security for accounts or for port-out authorization that customers can set up, like a unique pin, or adding a verification question, which will make it more difficult for someone to port-out your phone. Contact your mobile provider and speak to them specifically about porting and/or port-out security on your account.
- **Watch out for unexpected "Emergency Calls Only" status.** Call your wireless provider if your phone suddenly switches to "emergency call service only" or something similar. That's what happens when your phone number has been transferred to another phone. Contact the police and your financial institutions as well.
- **Be vigilant about communications you receive.** Watch out for phishing attempts, alert messages from financial institutions, and unexpected texts in response to two-factor authentication requests you didn't initiate.

If you've fallen victim to this type of scam, BBB encourages you to take steps to recover your identity. It's also a good idea to file a report on BBB ScamTracker and help get word of this scam out to others.

Media Contact: Dan Hendrickson, Communications Manager
651-695-2463 / dan.hendrickson@thefirstbbb.org

The mission of Better Business Bureau is to be the leader in building marketplace trust by promoting, through self-regulation, the highest standards of business ethics and conduct, and to instill confidence in responsible businesses through programs of education and action that inform, assist and protect the general public. We are open 8 a.m. to 5 p.m. Monday through Friday. Contact BBB at bbb.org or 651-699-1111, toll-free at 1-800-646-6222.

# # #