HOW YOUR CELL PHONE CAN MAKE YOU VULNERABLE TO IDENTITY THEFT

By: William F. Hess, J.D., MBA, CFP® Vice President, Wealth Management Consultant

Your cell phone holds some of your most sensitive personal and business information—passwords, account numbers, contacts, emails, texts, photos, social media posts, and more. If your phone ends up in the wrong hands, you're a prime candidate for phone identity theft and fraud. Crooks who specialize in these crimes can have a particularly devastating impact on the finances and reputations of the individuals they target—and the wealthy are particularly vulnerable.

HOW DOES CELL FRAUD HAPPEN?

Whether you like it or not, there's a pretty good chance your personal information is already available to criminals online. With the large number of system breaches over the past few years, hackers likely have stolen and are selling your sensitive key information on the dark web: your Social Security number, date of birth, driver's license number, address, place and length of employment, salary, names of family members, and various other details.

Crooks use your personal history to open all kinds of accounts in your name, including cell-phone accounts. Unlike bank or credit card accounts, cell-phone accounts are relatively easy to open because carriers don't always perform thorough background checks. Also, it's not unusual for customers to have more than one account in their name already.

IDENTITY THEFT TAKES ITS TOLL ON PEOPLE AND THE ECONOMY[1]

On average, identity theft finds a new victim every two seconds. Overall, 33% of adults living in the U.S. have experienced identity theft—twice the global average.

In 2018, the instances of mobile phone account takeovers rose to 679,000; the previous year's number was 380,000.

In 2019, a total of $16.9 billion was lost due to fraud, and 164.7 million sensitive.

Criminals can take your current cell phone number then transfer it to a fake account in a practice known as porting. It allows identity thieves to use your phone number to access sensitive information, including bank, retirement, and cryptocurrency accounts. You probably won't know it is happening because the verification code that financial institutions send to the number on the account doesn't come to you. It goes to the thief's device, according to an article in Consumer Reports.[2]

WHAT'S THE IMPACT OF CELL-PHONE ACCOUNT FRAUD?

With a fraudulent cell phone account in your name, criminals can tap into you your bank accounts, request credit cards, or sell the number to other criminals. You may not know this has happened until the fake accounts go into default, your authorized services are disconnected, or you see negative changes in your account.

"You have a new and quickly growing form of crime, the objectives of which go well beyond financial loss," said Edward McAndrew, a former federal cybercrime prosecutor to *Consumer Reports*. "In many ways we're seeing the

weaponization of digital technology—infrastructure, platforms, devices, and data. And this type of fraud is an illustration of that."[2]

Unlike other types of fraud, this type of theft can become a huge problem for victims. There's no infrastructure to resolve these situations and few consumer protections in place from cell-phone companies. This type of fraud can go on for months because it is hard to detect. Victims may be alerted to the crime when their accounts are drained, credit card companies seek payment for unpaid bills, or they are notified of an investigation for crimes committed in their name.[2]

HOW CAN YOU PROTECT YOUR PHONE AND THE DATA ON IT?

The Federal Trade Commission recommends four things you can do to protect the data on your phone:[3]

LOCK YOUR PHONE. Set your phone to lock when you're not using it. Create a PIN or passcode to unlock it. Use at least a six-digit passcode. You also may be able to unlock your phone with your fingerprint, your retina, or your face.

UPDATE YOUR SOFTWARE. Enable auto updates for your operating system. These updates often include critical patches and protections against security threats. Make sure your apps also auto-update.

BACK UP YOUR DATA. On a regular basis, back up the data on your phone. If you lose your phone, you'll still have access to your personal information.

GET HELP FINDING YOUR LOST PHONE. Mobile operating systems have programs that help you find your phone if you lose it. They also let you lock or erase all the data on your phone in case you think someone stole it.

Check with your cell-phone carrier for more specific direction on the steps above. As an additional security measure, you may want to subscribe to an identity monitoring service that will alert you to any suspicious activity on your accounts so you can know sooner rather than later that your data has been compromised.

WHAT SHOULD YOU DO IF YOUR CELL PHONE HAS BEEN STOLEN OR YOU ARE A VICTIM OF OTHER TYPES OF IDENTITY THEFT OR FRAUD?

- Close accounts you suspect have been breached, misused, or opened illegally.
- Contact the fraud departments for each of your creditors.
- Create a log of all contacts you make regarding the theft (name, title, phone number, date, and time of conversation).
- Call the Federal Trade Commission (FTC) Identity Theft Hotline at 1-877-438-4338 or report online at www.ftc.gov/idtheft.
- Create an Identity Theft Affidavit, which is a detailed list of the accounts affected by fraud. Print a copy and keep it in a safe place.
- Contact the three national credit bureaus (Equifax, Experian, and TransUnion) to place fraud alerts on your files. Request a free copy of your credit reports.
- Take your Identity Theft Affidavit to your local police department and file a report. Get the police report number and a copy of the report; keep this information with your Identity Theft Affidavit.
- Change all account passwords—each one should be different.
- Depending on the severity of the impact, you may want to change all your bank account numbers. You also may want to contact the Social Security Administration at 1-800-772-1213 or www.ssa.gov about a new SSN.

Contact Commerce Trust Company today if identity theft or fraud is affecting your personal financial circumstances. With our team of professionals, you can feel comfortable discussing topics ranging from cash flow management to having access to your wealth in an emergency.

[1]Source: Copyright©2020 CompareCamp. Arthur Zuckerman, "55 Identity Theft Statistics: 2019/2020 Data, Trends & Predictions," https://comparecamp.com/identity-theft-statistics/. May 22, 2020.

[2]Source: Octavia Blanco, "A Growing Threat to Your Finances: Cell-Phone Account Fraud," https://www.consumerreports.org/scams-fraud/cell-phone-account-fraud/. Last updated June 12, 2019.

[3]Source: Federal Trade Commission Consumer Information, "How to Protect Your Phone and the Data on It," https://www.consumer.ftc.gov/articles/how-protect-your-phone-and-data-it. September 2019.

The opinions and other information in the commentary are provided as of October 20, 2020. This summary is intended to provide general information only, and may be of value to the reader and audience.

This material is not a recommendation of any particular investment or insurance strategy, is not based on any particular financial situation or need, and is not intended to replace the advice of a qualified tax advisor or investment professional. While Commerce may provide information or express opinions from time to time, such information or opinions are subject to change, are not offered as professional tax, insurance or legal advice, and may not be relied on as such.

Data contained herein from third-party providers is obtained from what are considered reliable sources. However, its accuracy, completeness or reliability cannot be guaranteed.

Commerce Trust Company is a division of Commerce Bank.

1-855-295-7821 | commercetrustcompany.com

NOT FDIC INSURED | MAY LOSE VALUE | NO BANK GUARANTEE

ABOUT THE AUTHOR

WILLIAM F. HESS, J.D., MBA, CFP®

Vice President, Wealth Management Consultant

Bill is a wealth management consultant for Commerce Trust Company. He facilitates the introduction of our prospective clients to a comprehensive service team which includes private banking, investment management, trust administration, and financial planning. Bill provides an integrated and seamless client experience as we partner with clients to meet their long-term goals and objectives. Prior to joining Commerce in 2001, he practiced law for five years with Holman Hansen & Colville in Overland Park, Kansas. His practice focused on the areas of estate planning, probate administration, taxation, and corporate law. In 1992, Bill graduated cum laude with a bachelor of science degree in finance and economics from Rockhurst University. In 1995, he earned his juris doctor and master of business administration degrees from Creighton University. He is a member of the Kansas Bar and the Missouri Bar. In 2008, he obtained his CERTIFIED FINANCIAL PLANNER™ designation. Bill currently serves on the board of the Catholic Foundation of Northeast Kansas.