The Rise of Identity Fraud for High-Net-Worth Individuals.

A PRACTICAL INSIGHTS GUIDE FROM HUNTINGTON

We are in the midst of the biggest technology boom in the history of the planet.

As each day passes, computers, tablets and smartphones are enabling us to do more than we ever imagined. Today, we can make bank deposits from our phones. We can have food delivered with the tap of a button. We can even communicate with our pets when we're out of the house.

However, with these added conveniences come added risks. News of data breaches have become so commonplace that we as consumers are virtually numb to the threat.

Cyberthieves are constantly developing new ways to commit fraud. "Fraudsters are relentless, and they're smart," says Don Boian, director of cybersecurity outreach for Huntington. "With each new safeguard institutions put into place, cyberthieves are devising new methods to crack them."

The explosive growth of mobile devices has created an expansive new hunting ground for fraudsters. And with our cars, home security systems and even thermostats connected to networks, we have even more ways in which we can be compromised.

Nobody is immune to the risk.

$445 TO $608 BILLION

According to McAfee, the Center for Strategic and International Studies (CSIS) estimated that cybercrime cost the world between $445 billion and $608 billion in 2017†.

"Fraud has impacted people of every demographic and socioeconomic category—from retirees on a fixed income to business owners." Boian explains. "High-net-worth individuals are specifically targeted."

UNIQUE CHALLENGES FOR HIGH-NET-WORTH INDIVIDUALS

While fraudsters will attack everybody and anybody, they are beginning to pay more attention to high-net-worth individuals.

"Fraudsters know the payoffs can be enormous," notes Boian. "And they've found that it typically takes longer for this particular group to discover they have been hacked."

Reasons high-net-worth individuals are targeted:

They typically deal with larger transactions, so smaller fraudulent ones often go unnoticed.

They tend to have more accounts, making it more difficult to monitor them all effectively.

They don't have the time to monitor their accounts diligently.

They often assume their financial advisor is handling fraud detection for them.

Protection starts with knowledge.

In this guide, we will help you understand some of the more common strategies used by fraudsters and the various types of fraud perpetuated on high-net-worth individuals. We will also offer some common-sense tips to help you better protect your identity and your assets.

CRIMINAL METHODS

The key to every cybercrime is the ability to obtain a potential victim's personal information.

With social media, electronic communications and malware, cyberthieves are able to mine information more easily than ever before. We have outlined a few of the common practices fraudsters use today.

Social Media

Nowadays, we all like to share. We share pictures. We share updates on family events. We share personal news. Our friends know our birthdays, our pet names, our alma maters, and where and when we're going on vacation.

On social media, we take seemingly benign quizzes that divulge important information about ourselves. Diligent fraudsters collect personal data from a variety of these sources and use it to figure out passwords that will help them perpetuate their crimes.

Apps

When you download an app, you may be unknowingly giving up important data about yourself. The terms and conditions of these apps, which most consumers don't read, often give the developers broad access to a wide range of information about you. Apps are also susceptible to hacking, allowing cyberthieves to track your whereabouts.

Phishing

When "phishing," fraudsters cast a broad net in an attempt to catch as many unwitting victims as possible. Typically, the phishing expedition is started through the use of fraudulent emails. Fraudsters pose as legitimate entities and, over time, encourage individuals to reveal personal information such as passwords and credit card numbers. Emails can also deliver malware to a person's device that will enable criminals to more easily gather intelligence.

Spear Phishing

Spear phishing is a targeted form of phishing, directed at a specific individual or organization. It is often the first step in a masquerading scheme in which the fraudsters pose as someone prominent in the organization, such as a CEO or CFO. Once access to a person's email is acquired, the fraudster can review all of his or her information, including email history, calendars, signatures and more. With a good understanding of this person's email habits, writing style and schedule, they are able to successfully pose as that person. It is at this point that they can begin conning coworkers and colleagues into transferring money and making payments on their behalf.

PERSPECTIVE

> ***"Never give your personal information out over unsolicited phone calls or emails. Fraudsters are very good at posing as legitimate banks, hospitals, medical providers, etc. If you receive a call you weren't expecting asking for your information, tell them that you will call back using a known number (such as the number on the back of your debit or credit card), to ensure you are giving your information to a trusted service provider."***
>
> *— Don Boian, director of cybersecurity outreach, Huntington*

Common types of identity theft.

Cyberthieves use a wide range of tactics to access their victims' personal data. Some of the strategies are intended for a more immediate "payout," while others can take years to bear fruit.

Tax Identity Theft

Tax identity theft occurs when a fraudster files a fraudulent tax return and claims its benefits. Tax identity theft is rampant and lucrative for criminals. According to the United States Government Accountability Office, at least $12.24 billion in tax identity theft refund fraud was attempted in 2016*.

Medical Identity Theft

Medical identity theft happens when someone uses your personal information to submit fraudulent claims, obtain prescription drugs or even receive care. It can also be used to acquire government benefits such as Medicare or Medicaid.

Senior Identity Theft

A good number of high-net-worth individuals are seniors. They're people who've had long, successful careers and have accumulated substantial assets. This group is more vulnerable to identity theft because they are less likely to closely monitor their credit and financial accounts.

Child Identity Theft

You may not think your young children are at risk. But as soon as they are issued a social security number, they're vulnerable. What's worse, most people won't realize they've been victimized until years after the crimes have been committed.

DOS

- Do review your account statements regularly.
- Do report any unauthorized charges as soon as you discover them.
- Do consider an identity theft insurance rider.

DON'TS

- Don't provide information to unsolicited requests.
- Don't provide passwords over phone or email.
- Don't overlook the little charges on your account statement. Fraudsters may be using these purchases as a test.
- Don't purchase anything with your credit card using a public hotspot, like a coffee shop.

HOW TO MAKE YOUR PASSWORD MORE SECURE

Use a different password for every site you visit

Make your password long and complex

Avoid using names, dates and common phrases in your passwords

Avoid keeping passwords in electronic documents

Use a password management app to store and protect your passwords

See CNET's 2018 directory for their overview of the best password managers: https://www.cnet.com/news/the-best-password-managers-directory

Action items for fraud victims.

Contact your financial institutions.

If your bank accounts or existing credit lines have been affected, act swiftly to close them.

Place a fraud alert on your credit report.

Contact one of the three reporting agencies (Experian[§], Equifax[‖], or TransUnion[#]) immediately. By doing so, lenders and creditors will be alerted to take additional steps to verify your identity.

File an Identity Theft Report at IdentityTheft.gov.

This site was set up by the federal government to help victims set up a personal recovery plan. Here, you can put a plan in place and track your progress.

File a police report.

To complete the Identity Theft Report, you must also report the crime to local law enforcement. Make sure you obtain a copy of the police report as well as the report number.

Add an identity theft rider to your homeowners or renters insurance.

With most policies, this additional coverage will help pay for the cost of restoring your identity and may cover additional expenses that you incur as a result of the crime.

In addition to these steps, you should also change all of your existing passwords, get a new driver's license and contact the social security fraud hotline.

HUNTINGTON. YOUR PROTECTION IS OUR PRIORITY.

At Huntington, we are working on multiple fronts to help protect our high-net-worth customers' identities and assets. We are collaborating with government agencies to develop new solutions. We are creating educational tools, including videos, articles and quizzes, to help keep our customers informed. And we are continually developing technologies, like check block alerts, that help keep you protected and aware.

Most important of all, our Private Bank Advisors are here for you should you ever have a question or a concern.

HOW TO HELP PROTECT YOURSELF

While nobody can be completely immune from identity theft, you can make the process more difficult for potential fraudsters by completing this checklist.

- ☐ Update your operating systems, browser and software patches to ensure you're running the most up-to-date technology.
- ☐ Establish a secure firewall.
- ☐ Install and maintain antivirus solutions.
- ☐ Require dual approval on monetary transactions and administrative changes.
- ☐ Keep your login credentials secure.
- ☐ Be aware of and use your banks' security measures, such as text and email alerts.

See how Huntington Private Bank is helping protect and grow the assets of high-net-worth individuals.

Visit **huntington.com/PrivateBank** to learn more about the services available to you.

About Huntington

Huntington Bancshares Incorporated is a regional bank holding company headquartered in Columbus, Ohio, with $109 billion of assets and a network of 950 branches and 1,770 ATMs across eight Midwestern states. Founded in 1866, The Huntington National Bank and its affiliates provide consumer, small business, commercial, treasury management, wealth management, brokerage, trust, and insurance services. Huntington also provides auto dealer, equipment finance, national settlement and capital market services that extend beyond its core states. Visit huntington.com for more information. The Huntington National Bank is Member FDIC.

Huntington Private Bank® is a team of professionals dedicated to delivering a full range of wealth and financial services. The team is comprised of Private Bankers, who offer premium banking solutions; Wealth and Investment Management professionals, who provide, among other services, trust and estate administration and portfolio management from The Huntington National Bank; and licensed investment representatives of The Huntington Investment Company, who offers securities and investment advisory services. Huntington Private Bank® is a service mark of Huntington Bancshares Incorporated.

---

†*McAfee. Economic Impact of Cybercrime—No Slowing Down. February 2018.*

‡*United States Government Accountability Office. Tax Fraud and Noncompliance. January 2018.*

§*Experian.com, (888) 397-3742*

‖*Equifax.com, (866) 349-5191*

#*Transunion.com, (800) 888-4213*
