A New Threat to Your Finances: Cell-Phone Account Fraud

Consumers have a new privacy threat to worry about. It's known as cell-phone account fraud, where crooks open up a phony cell-phone account in your name and use it to access your bank account, sign up for credit cards, or sell the phone number for other criminals to use.

While little known among consumers, cell-phone account fraud can have a devastating impact on your finances—and your reputation.

"It's a rude awakening," says Kyle Marchini, senior fraud management analyst at Javelin Strategy and Research, an advisory firm for the financial industry. "Cell-phone account fraud can become a huge mess that, unlike credit card fraud, doesn't have infrastructure in place to resolve."

Unlike other types of fraud, there are fewer consumer protections. It's also harder to detect, so it can go unnoticed for months. By then, your bank account may be drained, credit card companies may be after you for unpaid bills, and the police may be investigating you for crimes committed in your name.

"Sometimes you may not find out about it until the account goes into arrears, and it can take months or years to fix that, not to mention the monetary expense usually entailed," says Brian Krebs, who runs KrebsOnSecurity.com, a website focused on cybercrime and security. "The hassle of trying to recover from this kind of ID theft is a lot worse than the few steps that people need to take to prevent it."

The biggest step you can take is to put a freeze on the credit information that is used to open a cell-phone account. This information doesn't come from the big credit rating agencies like Equifax but from little known companies such as the National Consumer Telecommunications and Utilities Exchange (NCTUE), a credit reporting agency fed by data supplied by phone, pay-TV companies, and utility service providers.

You can also get a PIN for your cell-phone account to prevent criminals from transferring your phone number to a new account without your knowledge. Finally, you'll need to pay closer attention to your cell-phone bill, bank account, and other financial transactions. All these preventative measures are outlined below.

Though relatively unknown, cell-phone account fraud is growing rapidly. In 2017 the number of victims of fraudulent mobile-phone accounts jumped 63 percent from a year earlier, to about 340,000, according to Javelin.

"These are relatively new crimes, and there's no reason to think that this is close to plateauing," says Edward McAndrew, a former federal cybercrime prosecutor who is now a partner at Ballard Spahr, a law firm.

According to Javelin, about 12 percent of fraudulent cell-phone account victims found out about the problem when they were contacted by the police or some other law enforcement agency. Many people find out only when the phony accounts tied to their names go into default, when they notice their service stops working, or when their accounts are drained.

"You have a new and quickly growing form of crime, the objectives of which go well beyond financial loss," says McAndrew. "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."

How the Fraud Works

You may not like it, but your personal information is widely available to criminals online. They can glean it from a number of different sources, including what you share on social media. They can also buy it from hackers who've stolen your data from companies such as Equifax.

Often these breaches involve the theft of key personal information: your Social Security number, driver's license number, phone number, address, and other personal details. This information is used to open all kinds of fake accounts in your name, including a cell-phone account.

But unlike a bank or credit card account, cell-phone accounts are relatively easy to open. Some experts we spoke with believe that carriers don't always do thorough background checks. So even if you open an account with a major carrier, it's possible for a crook to open up another account in your name.

Consumers usually don't realize this is happening for months, or until they are contacted by the authorities or a debt collector seeking payment.

Porting Your Phone Number

Crooks can also take your existing cell-phone number and transfer it to a fake account. This practice, known as "porting," lets criminals use your phone number to access your bank accounts, retirement accounts, or even cryptocurrency accounts.

You may not even realize it's happening. When the financial institutions text a verification code to the phone number associated with the account—what's known as two-factor identification—that code is sent to the criminal's device, not yours.

Once that cell-phone number is ported to a new carrier, you will no longer have any phone service. Sometimes consumers who don't make many calls or who aren't constantly connected to their phones don't immediately notice that their phone service has been cut off, giving criminals time to conduct fraud.

|Other Crimes Done in Your Name

- Instead of using your real address, criminals have the cell-phone bill sent to a different address. Once the account is established, they use the phone and pay their cell-phone bills long enough to establish a credit history. Then the criminals apply for credit cards and other loans in your name, opening you up to a mountain of bills.

- Crooks also sell the new phone number to other criminals engaged in drug dealing, human trafficking, or other schemes. “It could implicate people in suspected criminal activity because someone involved in it has stolen their identity,” says McAndrew.
- Using your name and personal information, crooks can also sign up for a phone plan and agree to finance the cost of a new, expensive phone. They then sell the phone and abandon the account, leaving you on the hook for around $1,000 if it's the iPhoneX or Samsung Galaxy Note 8.

What Your Liability Is

While banks and credit card issuers usually limit your liability from fraud, consumer protections are not well defined for cell-phone companies.

“Currently there aren’t regulatory protections for consumers in the same way that exists within the banking industry,” says Steven Weisman, an attorney and senior lecturer in white-collar crime at Bentley University in Waltham, Massachusetts.

In addition, “most consumers are having to spend a lot of time proving the fraud to the service providers,” McAndrew says. He hopes cell-phone service providers get more adept to prevent fraud and make it easier for consumers to remedy these issues.

“Much like credit cards are making efforts to prevent fraud—because they’re on the hook for the loss—so should cell-phone service providers,” McAndrew says.

The sooner you identify and report the fraud, the sooner fraudulent charges will stop and the less likely you’ll be held liable for damages.

How to Protect Yourself

There are a number of things you can do to keep criminals from opening or using a cell-phone account in your name.

Get a PIN for Your Account
Most cell-phone service providers have security measures, such as PINs, that can prevent unauthorized people from using your account. But these steps are often voluntary.

Of the cell-phone providers contacted by Consumer Reports, only Verizon said a PIN was mandatory on customer accounts to prevent “porting.”

“Verizon requires an account password/PIN to authenticate before the switch happens,” the company said in an email.

T-Mobile says it has included alerts in its customer app and on MyT-Mobile.com, and reminds customers they can call 611 at any time from their mobile phone to have a PIN/passcode added to their accounts.

“Port out fraud has been an industry problem for a long time, but recently we’ve seen an uptick in this illegal activity,” a T-Mobile spokesperson wrote in an email. “We have been encouraging customers to add extra security features to their accounts.”

Cricket Wireless referred Consumer Reports to the Communication Fraud Control Association website and to its own privacy policy page.

AT&T referred us to a blog post by Brian Rexroad, the company’s vice president of security platforms, which included a link to additional security measures you can add to your phone accounts if you choose.

Sprint did not respond to an email seeking comment for this report.

Freeze Your Credit Information

You can freeze their information at the big four credit reporting agencies—Experian, TransUnion, Equifax, and Innovis—to prevent crooks from opening bank or credit card accounts in your name. However, that’s not enough to protect yourself from having fake cell-phone accounts opened.

For greater security, freeze your credit reports at NCTUE. Most cell-phone service providers use NCTUE to determine new customers’ credit risk.

There are three ways to freeze your NCTUE information: online; by telephone (866-349-5355); and by mail (NCTUE Security Freeze, P.O. Box 105561, Atlanta, GA 30348). You can also opt out of data collection or set up NCTUE fraud alerts here.

Currently, there is no charge to freeze and unfreeze an NCTUE credit file. Make sure to have a pen and paper on hand because you will be given a PIN. Keep this in a safe place in case you need to change your preferences in the future, such as if you are changing a cell-phone, cable, gas, or electric utilities provider.

But NCTUE is just one of dozens of smaller credit reporting agencies that tailor data collection for myriad industries including landlords, subprime lenders, and other companies that subscribe to these services.

“We recommend consumers freeze their credit at the major credit bureaus, and where possible, at these smaller, less well-known companies as well,” says Anna Laitin, director of financial policy at Consumers Union, the advocacy division of Consumer Reports. “And consumers need to be vigilant, even when credit freezes have been placed at the less-familiar credit reporting agencies.”

Laitin reminds consumers to take advantage of their right under the Fair Credit Reporting Act (FCRA) to receive a free credit report from each credit bureau—including from these smaller, less well known ones—once per year.

However, freezing your accounts with all the various credit reporting agencies is time-consuming, says Eva Velasquez, CEO of the San Diego-based Identity Theft Resource Center, a nonprofit consumer advocate funded by grants, donations, and industry sponsors.

This fall, the major credit reporting companies will be required to let consumers freeze and unfreeze their credit files free of charge. Currently, consumers can pay up to $10 to freeze their credit reports depending on the state and the company where they are trying to freeze the reports.

Other Ways To Protect Yourself

- If you stop receiving calls or texts, contact your wireless provider immediately. The CTIA, a trade organization representing the telecom industry, recommends that you regularly check for provider and account alerts, even if you don't use your phone often.
- Never disclose your banking or other online passwords or personal identification numbers to anyone.
- Be on the lookout for "phishing" attempts. Contact your provider directly if you receive a call, email, or text message asking you for personal information like your Social Security number, your bank account number, your driver's license number, or other financial details.
- Guard personal details—such as your phone number, date of birth, or your first car and maiden name—and keep them off social media.
- Request that your bank or financial institution give you notice of every financial transaction through two different channels—for example, through text and email.
- Try using separate emails, one for your online banking account and financial transactions, and one for your social media accounts.