Cell Phone Fraud

Cellular fraud is defined as the unauthorized use, tampering or manipulation of a cellular phone or service. Types of cellular fraud include SIM swapping, cloning and subscriber fraud.

What is SIM Swapping or a Port-Out Scam?

Your mobile phone number may be the key to your most important financial accounts. Text messages are often used by banks, businesses and payment services to verify your identity when you request updates to your account.

Mobile phone numbers can legally be ported from one provider to another when you switch your mobile phone service, and can also be ported from one mobile phone to another when you upgrade or change devices. But with enough of your personal information, scammers can have your number ported to a device they possess.

When scammers initiate a porting request, they con the victim's mobile phone company into believing the request is from the authorized account holder. If the scam is successful, the phone number will be ported to a different mobile device controlled by the scammer.

Another way to perpetrate this scam is to physically steal the victim's SIM card, a removable device in some mobile phones that carries a unique ID and stores the consumer's personal data. The scammer can then use the stolen SIM card in their own mobile device.

In either case, the scammer can gain control over the victim's private texts and calls, and may then try to reset credentials for the victim's financial data and social media accounts. If successful, the scammer can drain the victim's bank accounts and sell or ransom their social media data.

Learn more about this scam and how to protect yourself.

eSIM May Decrease SIM Swap Risk

Embedded SIM cards – eSIM cards for short – have replaced traditional SIM cards in newer cell phone models. The eSIM cards are much smaller and hardwired inside the phone, so they're not removable, eliminating some of the security risk for physical SIM swaps. However, port-out scams remain a security concern.

Also, consumers should always wipe their eSIM data when they replace their phones. Learn more in our eSIM consumer FAQ.

What is cell phone or SIM cloning fraud?

Every cell phone should have a unique factory-set electronic serial number (ESN) and a mobile identification number (MIN). A cloned cell phone is one that has been reprogrammed to transmit the ESN and MIN belonging to another cell phone. Scammers can steal ESN/MIN combinations by illegally monitoring the radio wave transmissions from the cell phones of legitimate subscribers. After cloning, both the legitimate and the fraudulent cell phones have the same ESN/MIN combination and cellular providers cannot distinguish the cloned cell phone from the legitimate one. Scammers can then run up

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau

expensive toll charges and the legitimate phone user gets billed for the cloned phone's calls. Alert your service provider if you see unauthorized calls or charges on your account.

What is subscriber fraud?

Subscriber fraud occurs when a scammer signs up for cellular service with fraudulently obtained customer information or false identification. Criminals can obtain your personal information and use it to set up a cell phone account in your name. It may take time to discover that subscriber fraud has occurred, and even more time to prove that you did not incur the debts. Millions of dollars are lost each year due to subscriber fraud.

If you think you have been a victim of subscriber fraud:

- Contact local law enforcement and file a police report. You can also file an identity theft report with the Federal Trade Commission.
- Notify your current service provider as well as the service provider for the fraudulent account.
- Place a fraud alert on any of the three major credit reporting bureaus -- Equifax, Experian or TransUnion. The one you notify will share the alert with the other two.
- Continue to monitor your credit report at each credit bureau at least once a year. Consider checking a different credit bureau report every four months for free at annualcreditreport.com.

Consumer Help Center

For more information on consumer issues, visit the FCC's Consumer Help Center at www.fcc.gov/consumers.

Alternate formats

To request this article in an alternate format - braille, large print, Word or text document or audio - write or call us at the address or phone number at the bottom of the page, or send an email to fcc504@fcc.gov.

Last Reviewed 04/21/20

Federal Communications Commission · Consumer and Governmental Affairs Bureau · 45 L Street NE, Washington, DC 20554
1-888-CALL-FCC (1-888-225-5322) · TTY: 1-888-TELL-FCC (1-888-835-5322) · www.fcc.gov/consumer-governmental-affairs-bureau