PROTECT YOURSELF FROM FRAUD

PART 1: GENERAL FRAUD PREVENTION AWARENESS

Boost Mobile is committed to protecting you from bad actors. It takes a team effort and vigilance every day in our interactions online and with email to protect against fraud.

We want to help you stay safe when you use our products and services.

Protect your Boost Mobile account using the following tips:

- **Be alert:** Boost Mobile will never ask you for sensitive information via call, text, or email. Never give out your name, address, Social Security or tax ID numbers, credit card information, account passwords, or banking details.
- **Use the authorized BoostOne App and website:** Use the BoostOne Mobile App or log in to your account at boostmobile.com to service your account or communicate with us. Boost Mobile will not direct you to illegitimate links. Scammers often send links to phish for your personal and financial information. If a link looks suspicious, don't click!
- **Report any suspicious activity:** If you notice unauthorized activity on your Boost Mobile account , call us at 833-50-BOOST (833-502-6678) or contact us through the BoostOne App.
- **File a complaint:** Report fraud and identity theft by filing a complaint with the Federal Trade Commission (FTC) by clicking here or call the FTC at 1-877-FTC-HELP. You can also report fraud to the Federal Communications Commission (FCC) by clicking here.

PART 2: TYPES OF FRAUD

BE ALERT: KNOW

1.Port-Out Scam:
Boost Mobile phone numbers can be ported from one provider to another when switching phone service. Scammers can hijack your phone number by fraudulently porting your number to a device they control.

Scammers imitate an authorized account holder by using personal information, such as a name, address, birth date, PINs or passwords, or Social Security number to make it seem as if they are the authorized account holder. If they succeed in passing an account authentication process, they can then initiate an unauthorized porting request.

If the scam is successful, scammers will attempt to use the ported number to bypass multi factor authentication and drain the victim's bank accounts. Scammers may change login details and attempt to sell personal information.

You'll know you're a victim of port-out fraud if you suddenly lose service on your device. If you lose service, your phone may go dark or only allow 911 calls.

Take these steps to protect yourself from Port-Out Fraud:

- Do not share your personal information with anyone. Keep information like your Social Security number, phone number, birth date, PINs and passwords secure.
- Be alert: Boost Mobile will never call you or text you asking for your personal information. If someone calls or texts you asking for your personal information claiming to be Boost, do not share any information and contact us immediately at **833-64-BOOST (1-833-502-6678)**.
- Port Out PIN: If you leave Boost Mobile for another carrier, Boost Mobile will provide you with your port-out PIN when you contact us at **833-64-BOOST 1-833-502-6678**. Keep your port-out PIN secure and not share it.
- Additional Steps: If you are a victim of port-out fraud, contact your bank or other financial institutions and place a fraud alert on your credit reports.

2. SIM Swapping

SIM cards carry unique IDs and are tied to mobile phone numbers. If a scammer gains control of your SIM card, they can hijack communications meant for you and reroute them to a device they control.

Financial institutions and other businesses may use multifactor authentication to verify your identity when you log into your accounts by sending a text to your mobile phone. Scammers can use a SIM swapping tactic to outsmart multifactor authentication and gain unauthorized access to your accounts.

Scammers initiate SIM swapping by physically removing a victim's SIM card from their mobile device and using it in a device they control. Scammers may also impersonate customers and trick mobile service providers into switching your phone number from the SIM card in your device to a SIM card that they control. Scammers might also engage in a similar practice called SIM Cloning, where software is used to duplicate your original SIM card. Scammers can then use the stolen SIM card in their own device and perpetrate fraud.

Here are several steps you should take to protect yourself from Sim Swapping;

- Do not share your personal information with anyone. Keep information such as your Social Security number, phone number, your date of birth, PINs and passwords secure.
- Be alert: Boost Mobile will never call you or text you asking for your personal information. If someone calls or texts you asking for your personal information claiming to be Boost Mobile, do not share any information and contact us immediately at **833-50-BOOST** (**833-502-6678**).
- Get an eSIM: An eSIM is a digital SIM that eliminates the need for a physical SIM card. An eSIM is hardwired into the phone itself and provides significant security benefits because it cannot be taken from a device. If you have an eSIM-capable

device and would like to utilize the eSIM capabilities, please call Boost Mobile Customer Care at **833-50-BOOST** (**833-502-6678**) to make the switch. **Learn more about eSim here.**

- Report fraud: If your device is lost or stolen, please contact Boost Mobile Customer Care at **833-50-BOOST (833-502-6678)**.
- Additional Steps: If you suspect you're a victim of SIM swapping, contact your bank or other financial information and place a fraud alert on your credit reports.

3. Smishing

Scammers can send deceptive messages to your phone. These messages appear to be from a trusted source like your bank or the IRS. The messages seem urgent and may promise you a reward or money in exchange for clicking a link or submitting information.

An example of a smishing text message could be a text message claiming to be from your telecom provider, warning you that your account has been locked. The text message could contain a link directing you to a website and prompt you to enter your personal information such as your username, passwords and one-time passcodes, which scammers could use to gain access to your accounts.

Interacting with the message, such as clicking on the link sent or calling the phone number in the message, can give scammers access to your personal information or install malware on your device. Scammers may sell your information or use it to perpetrate fraud.

Here are several steps you should take to protect yourself from Port-Out Fraud;

- Do not Act: If a text message seems suspicious, delete it immediately. Do not respond to the message or click on any link that it contains, even if the message requests that you "text STOP" to end messages.

- Confirm before clicking: Boost Mobile will never ask for personal or account information by text message.If you get a text message that seems to be from Boost with a link to click or number to call, contact Boost Mobile directly **833-50-BOOST (833-502-6678)** to confirm before acting on the message.

- Report it: If you receive a suspicious text message claiming to be from Boost Mobile, please forward the text message to us right away at **833-50-BOOST (833-502-6678).** Remember, do not click suspicious links. If you shared any personal information or clicked on any suspicious link, contact us right away at **833-50-BOOST (833-502-6678).**

4. One Ring Scam/Wangiri

When you get a call from a number you do not recognize that stops after one ring and doesn't continue, you may be a target of a "one-ring" scam. Do not answer or return these calls. Getting you to call these numbers back at premium rates is the goal for "one ring" or "wangiri" scammers. The term wangiri means "one ring and cut" and comes from Japan, where the scam originated.

One-ring scammers may mask the number they call from, making it difficult to obtain the identity or location of the caller. These numbers may appear as premium or international numbers that generate curiosity leading you to return or pick up the call.

Once you pick up or return the call, the scammers will try to keep you on the line leading to high fee charges or connection charges on your account. The longer you stay on the call, the more money the scammer makes.

Here are several steps you should take to protect yourself from Port-Out Fraud;

- Be alert: Do not answer a number you do not recognize. If a suspicious unrecognized number repeatedly calls with a one ring and hangs up, do not answer it, do not share any information with the caller and contact Boost Mobile immediately at **833-50-BOOST (1-833-502-6678)**.

- Confirm the legitimacy of a phone number before calling back or answering: If you do not recognize the number that called, try confirming from other trusted sources that it is a legitimate phone number or from a trusted source before picking up or calling back.

- Report it: If you suspect that you are being targeted by a one-ring scammer, do not pick up or call back. Instead, report it to Boost Mobile immediately at **833-50-BOOST (1-833-502-6678).** You can also file a complaint with FTC

5. **Post-Disaster Scam**

The after effects of natural disasters may leave people vulnerable to scammers. Scammers target the good conscience of people looking to make a positive impact and people trying to recover.

Getting you to pay for charities or services are the most common ways scammers target innocent victims.

Here are several steps you should take to protect yourself from Post-Disaster Scam;

- Be alert: Verify the information of any person or organization asking you to pay for services or donate to charity. Credible relief organizations will not ask for payment before granting any kind of relief or services.

- Do not share Personal information: If you get a call or text asking for your personal information, such as, your Social Security or tax ID numbers,, date of birth, car

registration number, financial account numbers, or usernames and passwords, do not share it.

- Confirm before clicking: Scammers could ask you for donations and send links or attachments that download malware or direct you to fraudulent websites. Scammers use these attempts to phish for your personal and financial information., do not click on any suspicious links. Confirm that organizations are legitimate and trustworthy by visiting their website or calling them directly. If you suspect you've been targeted by a post-disaster scam, you can also file a complaint with the FTC .