

<Date>

<First Name> <Last Name>
<Address 1 >
<Address 2>
<City>, <State Code> <ZIP>

Dear <First Name>,

Sprint is writing to inform you of a recent security incident that may affect you. We take this matter, and all matters involving customer privacy, very seriously.

Sprint determined that a fraudulent device insurance claim was attempted on your account between May 7 and July 22, 2017. Information that may have been compromised as a result of this incident are your Sprint account Personal Identification Number (PIN) and/or security questions/answers. Please note that the fraudulent device insurance claim did not result in any cost to you, and no other personal information about you was available to the person filing the improper claim. Your account was not charged or, if your account was charged, an appropriate credit was applied to the account.

Sprint sent you SMS notifications prompting you to change your PIN and security questions/answers beginning on or about August 22, 2017. If you updated your Sprint account's PIN and security questions/answers on or after August 22, 2017, no further action is needed at this time regarding your Sprint account.

On or about August 24, 2017, Sprint reset your PIN and security questions/answers if you did not update them yourself by that date to better ensure your account's protection. If you have not updated your Sprint account's PIN and security questions/answers since August 22, 2017, we recommend that you contact our customer care representatives at 844-804-8692, Option 1, who will help you re-establish and personalize the PIN and security questions/answers on your Sprint account. You'll be asked to select a new 6 to 10 digit number for your PIN. If you used your Sprint account PIN or security questions/answers for other accounts, we also recommend that you change your PIN or security questions/answers for those other accounts.

At this time, we have no reason to believe that information compromised in this incident is likely to be further misused. However, for your general protection, we urge you to take the preventative measures that are recommended by the Federal Trade Commission (FTC) to help protect you from fraud and identity theft. For your convenience, we have included the FTC's recommendations within this letter. You also may access information on the FTC's website at www.ftc.gov/idtheft.

We apologize for the inconvenience that this may cause you. Please be assured that our customers' privacy is important to us and we will continue to take measures to safeguard your personal information. Please contact us at 844-804-8692, Option 1, if you have any questions or concerns regarding this matter.

Sincerely,

Sprint Customer Care

What can you do to safeguard against identity theft or fraud?

If you suspect that your personal information or that of a family member has been misused to commit identity theft, take the following steps and keep a record of all your actions. You can obtain information from the FTC and the consumer reporting agencies listed below about establishing fraud alerts and security freezes.

1. Place a fraud alert on your credit reports, and review your credit reports.

Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

TransUnion:	1-800-680-7289	www.transunion.com
Equifax:	1-800-525-6285	www.equifax.com
Experian:	1-888-EXPERIAN (397-3742)	www.experian.com

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies. If you find fraudulent or inaccurate information, get it removed.

2. Close the accounts that you believe have been tampered with or opened fraudulently.

Speak with someone in the security or fraud department of each company. Follow up in writing, and include copies of supporting documents. Send your letters by certified mail, return receipt requested. Keep a file of your correspondence and enclosures.

When you open new accounts, avoid creating passwords or other account credentials using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers. You should also avoid reusing passwords and other account credentials that you know have been compromised.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions. Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts.

3. File a report with your local police or the police in the community where the identity theft took place.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. When you go to your local police department to file your report, bring a printed copy of your FTC ID Theft Complaint form, your cover letter, and your supporting documentation. Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report to dispute the fraudulent accounts and debts.

4. Visit the Federal Trade Commission's Identity Theft website—[IdentityTheft.gov](https://www.ftc.gov/identitytheft)—for more information on reporting and recovering from identity theft.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces. You can also contact the FTC by phone at 1-877-438-4338 or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.