July 9, 2019

VIA EMAIL TO: SecurityBreach@atg.wa.gov

RE: Security Incident Notification

Dear Attorney General Ferguson,

Pursuant to Washington statute Wash. Rev. Code § 19.255.010, we are writing to notify you of a recent security incident involving Sprint Corporation ("Sprint") customer information. The following information provides more detail regarding the incident.

General Description of the Incident: On June 22, 2019, Sprint was informed of unauthorized access to Sprint accounts using account credentials via the Samsung.com "add a line" website. Subsequently, Sprint proceeded to re-secure the Sprint accounts by resetting the affected customer account PIN codes. The re-securing of the accounts was completed on June 25, 2019. There were 26,801 customers impacted of which 596 are residents of Washington. Attached please find the letter that will be mailed to customers beginning July 11.

Sprint Contact Information:

Sprint Contact Person: Laura LaPlante
Title: Privacy Compliance Manager, Office of Privacy
Telephone number: (913) 794-6304
Email: Laura.2.LaPlante@sprint.com

Dated: July 9, 2019
Submitted by: Laura LaPlante
Title: Privacy Compliance Manager, Office of Privacy
Address: 900 7th Street NW, Washington DC 20001
Email: Laura.2.LaPlante@sprint.com
Telephone: (913) 794-6304
Fax: (202) 585-1940

Please do not hesitate to contact me at the Sprint Legal Department, Office of Privacy, or Maureen Cooney, Head of Privacy, Sprint Office of Privacy (Maureen.cooney@sprint.com) should you have any further questions regarding this notification.

Sincerely yours,

Laura L. LaPlante

Laura LaPlante

[System populated date]

[Name]
[Street]
[City], [State] [ZIP]

Important Notice

Dear [Name],

On June 22, Sprint was informed of unauthorized access to your Sprint account using your account credentials via the Samsung.com "add a line" website. We take this matter, and all matters involving Sprint customer's privacy, very seriously.

What Information Was Involved?
The personal information of yours that may have been viewed includes the following: phone number, device type, device ID, monthly recurring charges, subscriber ID, account number, account creation date, upgrade eligibility, first and last name, billing address and add-on services. No other information that could create a substantial risk of fraud or identity theft was acquired.

What We Are Doing.
Sprint has taken appropriate action to secure your account from unauthorized access and has not identified any fraudulent activity associated with your account at this time. Sprint re-secured your account on June 25, 2019 with the following notification to your Sprint phone device:

- ***Your account PIN may have been compromised, so we reset your PIN just in case in order to protect your account.***

This letter also includes ways to protect your personal information along with important websites and phone numbers for your further information.

Other Important Information.
As a precautionary measure, we recommend that you take the preventative measures that are recommended by the Federal Trade Commission (FTC) to help protect you from fraud and identity theft. These preventative measures are included at the end of this letter. You may review this information on the FTC's website at www.ftc.gov/idtheft and www.IdentityTheft.gov or contact the FTC directly by phone at 1-877-438-4338 or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

We apologize for the inconvenience that this may cause you. Please be assured that the privacy of your personal information is important to us. Please contact Sprint at 1-888-211-4727 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.

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
TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
www.transunion.com

Equifax:
1-800-465-7166
Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian:
1-888-EXPERIAN (397-3742)
Experian
PO Box 9701, Allen, TX 75013
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.

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, or 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 directly by phone at 1-877-438-4338 or by mail at 600 Pennsylvania Avenue, NW, Washington, DC 20580.

Residents of Maryland, North Carolina and Rhode Island can also obtain information about steps you can take to avoid identity theft from your state's Office of the Attorney General.

- Maryland: http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx
  200 St. Paul Place
  Baltimore, MD 21202
  Toll Free: 1-888-743-0023

- North Carolina: http://www.ncdoj.gov/Protect-Yourself/2-4-3-Protect-Your-Identity.aspx
  9001 Mail Service Center
  Raleigh, NC 27699-9001
  Toll Free: 1-877-5-NO-SCAM

- Rhode Island: http://www.riag.ri.gov/index.php
  Office of the Attorney General
  150 South Main Street
  Providence, RI 02903
  Toll Free: (401) 274-4400

5. Contact your state's Attorney General or Consumer Protection Agency for more information on reporting and recovering from identity theft.

By sharing your identity theft complaint with state Attorney Generals or other Consumer Protection Agencies, you will provide important information that can help law enforcement officials.