May 9, 2019

Attorney General Gordon MacDonald
33 Capitol Street
Concord, New Hampshire 03302
FAX (603) 271-2110

Re: Security Incident Notification

Dear Attorney General MacDonald:

Pursuant to the New Hampshire's Right to Privacy Act, § 359-C:20 et seq, we are writing to notify you of a recent security incident involving Sprint Corporation ("Boost Mobile") customer information. The following information provides more detail regarding the incident.

General Description of the Incident: On March 14, 2019 Boost Mobile, a Sprint brand, was the target of a brute force style attack. The Boost IT team identified a high volume of activity on the Guest Payment page of the Boost.com website which included both unsuccessful and successful attempts to log on to customer accounts. On March 18, 2019 access was blocked immediately and a permanent solution went live on April 1, 2019. Boost Mobile has reset PIN codes for all the affected accounts and a dedicated Care Team has been established to assist affected customers. There were 25,909 customers impacted of which 17 are New Hampshire residents. Attached please find the Boost Mobile notice that will be sent to customers.

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: 5/9/19
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, should you have any further questions regarding this notification.

Sincerely yours,

Laura L. LaPlante

Laura LaPlante

CPNI Notice SMS

BSTFreeMsg: A recent security incident may have affected your account. For details click here: https://www.boostmobile.com/cbm/Notification.

For Spanish: https://espanol.boostmobile.com/cbm/Notification

CPNI WAP Notice – No Boost.com log on required

Dear Valued Customer

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

On March 14, 2019, Boost.com experienced unauthorized online account activity in which an unauthorized person accessed your account through your Boost phone number and Boost.com PIN code.

The Boost Mobile fraud team discovered the incident and was able to implement a permanent solution to prevent similar unauthorized account activity.

Boost Mobile sent you a text notifying you that a new temporary PIN code had been established for your account with a link to the Boost.com site so you could change your PIN code and contact number to call if you had questions. If you have already changed your PIN code there is no further action necessary. If you have not reset your PIN code we recommend that you reset it now. As a reminder, we recommend that PIN codes such as [redacted] or [redacted] are to be avoided.

It is important that you regularly review your Boost Mobile account to ensure that no unauthorized activity occurs on your account. We also 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. You may access information on the FTC's website at www.ftc.gov/idtheft.gov or contact the FTC directly by phone at 1-844-282-8211 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 our customers' privacy is important to us and we will continue to take measures to safeguard your account and personal information. Please contact Boost Mobile Customer Care at 1-866-402-7366 if you have any questions or concerns regarding this matter.

Sincerely,

The Boost Mobile Team

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 and North Carolina 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

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 the FTC, you will provide important information that can help law enforcement officials.