

NOTICE OF DATA BREACH

Dear Customer,

We want to let you know about a sophisticated attack that we recently identified and quickly shut down, which may have impacted some of your personal information.

What Happened?

Our Cybersecurity team recently identified and shut down a malicious attack against our email vendor that led to unauthorized access to certain T-Mobile employee email accounts, some of which contained account information for T-Mobile customers and employees. An investigation was immediately commenced, with assistance from leading cybersecurity forensics experts, to determine what happened and what information was affected. We immediately reported this matter to federal law enforcement and are actively assisting their investigation. T-Mobile is in the process of notifying customers.

What Information Was Involved?

The personal information accessed between November 26, 2019 and December 25, 2019 and could include names and addresses, Social Security numbers, financial account information, and government identification numbers, as well as phone numbers, billing and account information, and rate plans and features.

What We Are Doing

We are offering you free credit monitoring and identity theft detection services, provided by TransUnion. Please refer to the Credit Monitoring section of this letter for more information about these credit monitoring services and how to sign up.

We regret that this incident occurred. We take the security of customer information very seriously and while we have a number of safeguards in place to protect customer information from unauthorized access, we are also always working to further enhance security so we can stay ahead of this type of activity.

What You Can Do

We do not have any evidence that personal information contained in the affected accounts was used to commit fraud or otherwise misused. It is always a good idea to review your account information and update the personal identification number (PIN/passcode) on your T-Mobile account. To do so, you can reach us by dialing 611 from your T-Mobile phone or by calling 1-

800-937-8997 from any phone. For additional resources regarding security on your account, please review our Privacy Resources at: <https://www.t-mobile.com/responsibility/privacy>.

We also encourage you to consider the following:

- It is always a good idea to remain vigilant against threats of identity theft or fraud, and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.
- While we have no evidence that information accessed in this attack is being misused, if you ever suspect that you are the victim of identity theft or fraud, you have the right to file a report with the police or law enforcement. In addition, you may contact the FTC or your State Attorney General to learn more about the steps you can take to protect yourself against identity theft. The attachment following this letter has more information about steps you can take to protect yourself against identity theft or fraud.
- It is always a good idea to be alert for “phishing” emails by someone who acts like they know you or are a company that you may do business with and requests sensitive information over email, such as passwords, Social Security numbers, or bank account information. We do not ask for this type of information over email.

More information about how to protect yourself is available in the Additional Information Section of this letter.

For More Information

If you have additional questions, feel free to contact us online, in a store or through our customer service team at 800-937-8997. Additional information regarding this event is also available here www.t-mobile.com/corporate/responsibility/consumer-info/pii-notice

Sincerely,

Matt Staneff
Chief Marketing Officer
T-Mobile USA

ATTACHMENT A

How to Sign up for Credit Monitoring Services

We have arranged for you to enroll, at no cost to you, in an online credit monitoring service (myTrueIdentity) for two years provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go to the myTrueIdentity website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the following 6-digit telephone pass code <<xxxxxxx>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and May 31, 2020. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion, or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes access to an identity restoration program that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

ATTACHMENT B

Additional Information to Protect Yourself

In addition to considering enrolling in credit monitoring services, it is always a good idea to remain vigilant, to review your account statements and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft, you should contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission.

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 726-1014.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing or other services.

A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax: Consumer Fraud Division P.O. Box 740256 Atlanta, GA 30374 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000 (800) 680-7289 www.transunion.com
---	--	--

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your State Attorney General, or the FTC. Contact information for certain state attorneys general is included below. Contact information for other attorneys general is located here [hyperlink to www.t-mobile.com/corporate/responsibility/consumer-info/pii-notice]

California Residents: Visit <https://www.oag.ca.gov/privacy> for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, (515) 281-5164, www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or www.oag.state.md.us.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, RI 02903; (401) 274-4400; or <http://www.riag.ri.gov>. You may also file a police report by contacting local or state law enforcement agencies.