



October 11, 2021
STATE OF IOWA

RCVD OCT 12 2021

RE: Notice of Data Breach

NOTICE OF DATA BREACH

This notice is to inform you of a recent cybersecurity attack against T-Mobile systems that resulted in unauthorized access to some personal information.

What happened: On August 17, 2021, T-Mobile learned that a bad actor illegally accessed personal data from T-Mobile systems, to which the criminal gained access on or before July 19, 2021. Our cybersecurity team has quickly responded to the security incident, began a deep technical review with leading cybersecurity forensics experts, and engaged with federal law enforcement to assist in the investigation.

Information involved: While we have no indication that personal financial or payment information or credit/debit card information was accessed, we have determined that *unauthorized access to your personal information has occurred, including your name, driver's license/ID information, date of birth, and Social Security number.*

What we're doing: T-Mobile is taking proactive steps to notify and protect current, former, and prospective customers whose information may have been exposed, including an offer for two years of free identity protection services with McAfee's ID Theft Protection Service to all persons who may have been affected. More details on the incident can be found at <https://www.t-mobile.com/brand/data-breach-2021/general-information> and details on how to access the McAfee services can be found at <https://www.t-mobile.com/brand/data-breach-2021/general-information/enroll>.

What you can do: Visit our resource page <https://www.t-mobile.com/brand/data-breach-2021/general-information> for contact information for the three major U.S. credit bureaus and additional information about steps you can take to protect yourself and credit. Additional resources are also available at <https://www.t-mobile.com/support/account/additional-steps-to-protect-yourself>.

Sincerely,

T-Mobile

More details:
<https://www.t-mobile.com/brand/data-breach-2021/general-information>
1-844-546-5367
PO Box 37380 Albuquerque, NM 87176-7380

Appendix A – Information for U.S. Residents

CREDIT MONITORING

We are providing you with access to McAfee ID Theft Protection Service free for two years from T-Mobile. This service provides you with dark web and credit monitoring, full-service ID resolution, \$1 million identity insurance*, lost wallet recovery, and more. This service will notify you of changes in a credit report, such as loan data, inquiries, new accounts, judgments, liens, etc., and in real time when hard inquiries are detected on your Experian credit file, for two years starting from the date of enrollment.

To enroll in McAfee ID Theft Protection Service at no charge, please log on to <https://www.t-mobile.com/brand/data-breach-2021/general-information> and follow the instructions provided.

In order for you to receive the services, you must enroll within 60 days of the date of this letter.

ADDITIONAL INFORMATION

To protect against possible fraud, identity theft or other financial loss, you should always 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 can contact your local law enforcement agency, your state's attorney general or the Federal Trade Commission (FTC). Please know that contacting us will not expedite any remediation of suspicious activity.

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 from the U.S. at +1 (877) 322-8228.

Information on Implementing a Fraud Alert or Security Freeze

You may contact any one of 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 +1 (888) 766-0008 www.equifax.com	Experian: Credit Fraud Center P.O. Box 9554 Allen, TX 75013 +1 (888) 397-3742 www.experian.com	TransUnion: TransUnion LLC P.O. Box 2000 Chester, PA 19016-2000 +1 (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 (5) 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 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; by telephone at +1 (877) 382-4357; or at 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.

California Residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

Iowa Residents: You are advised to report any suspected identity theft to law enforcement or the Iowa Attorney General. The Attorney General can be contacted at the Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319; by telephone at +1 (515) 281-5164; or at www.iowaattorneygeneral.gov.

Kentucky Residents: The Attorney General can be contacted at the Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601; by telephone at +1 (502) 696-5300; or at www.ag.ky.gov.

Maryland Residents: The Attorney General can be contacted at the Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; by telephone at +1 (888) 743-0023; or at www.oag.state.md.us.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, North Carolina 27699-9001; by telephone at +1 (919) 716-6400; or at 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.

New York Residents: Visit the New York Attorney General's Office website on data breaches (<https://ag.ny.gov/internet/data-breach>) for additional information on protection against identity theft.

Oregon Residents: You are advised to report any suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission. The Attorney General can be contacted at the Oregon Department of Justice, 1162 Court Street NE, Salem, Oregon 97301-4096; by telephone at +1 (877) 877-9332 (toll-free in Oregon) and +1 (503) 378-4400; or at www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; by telephone at +1 (401) 274-4400; or at www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

Washington DC Residents: The Attorney General can be contacted at the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington DC 20001, by telephone at (202) 727-3400, or by email at oag@dc.gov.

* Identity theft insurance is not available in New York due to regulatory requirements. All other features (dark web and credit monitoring, full-service ID resolution, etc.) are available in New York.