

<https://www.t-mobile.com>Log in 

AUGUST 19, 2021

NOTICE OF DATA BREACH: Keeping you safe from cybersecurity threats.

What you need to know and how we're protecting you.

What you can do



Customers trust us with their private information and we safeguard it with the utmost concern. A recent cybersecurity incident put some of that data in harm's way, and we apologize for that. We take this very seriously, and we strive for transparency in the status of our investigation and what we're doing to help protect you.

What happened:



On August 17, 2021, T-Mobile learned that a bad actor illegally accessed personal data. Our investigation is ongoing, but we have verified that a subset of T-Mobile data had been accessed by unauthorized individuals and the data stolen from our systems did include some personal information. The latest details about the affected data are available [here \(https://www.t-mobile.com/news\)](https://www.t-mobile.com/news).

Information involved:

Our investigation is ongoing and this information may be updated. The exact personal information accessed varies by individual. We have determined that the types of impacted information include: names, drivers' licenses, government identification numbers, Social Security numbers, dates of birth, T-Mobile prepaid PINs (which have already been reset to protect you), addresses and phone number(s). **We have no indication that personal financial or payment information, credit or debit card information, account numbers, or account passwords were accessed.**

What we're doing:

We're relentlessly focused on taking care of our customers—that has not changed. We've been working around the clock to address this event and continue protecting you, which includes taking immediate steps to protect all individuals who may be at risk.

What you can do:

As we move quickly to protect you, we also want to equip you to protect yourself. It's recommended that you take proactive steps regularly to protect your data and identity, and now's a great time to do that. To be clear, **we have no information that indicates any passwords, postpaid PIN numbers, or financial or payment information have**

been compromised. Still, the following steps are always smart practices to help keep your account more secure. We encourage you to complete these actions as soon as possible:

Protect your identity with McAfee

Sign up for McAfee® ID Theft Protection Service FREE for two years provided by T-Mobile.

Claim now >

Activate Scam Shield™

Tap into our network's advanced scam-blocking protection and use anti-scam features such as Scam ID, Scam Block, and Caller ID—FREE to all T-Mobile customers.

Get more details >

Further protect your T-Mobile account

Use our free Account Takeover Protection service to help protect against an unauthorized user fraudulently porting out and stealing your phone number (postpaid only).

See how >

Additional resources

Check out more ways to protect yourself.

See how >

If you have additional questions, feel free to contact us online, in a store or through our Customer Care team at 611 from your phone or at 1-800-937-

8997.

Connect with T-Mobile

@(https://www.instagram.com/tmobile/) **f** (https://www.facebook.com/TMobile) **🐦** (https://twitter.com/TMo

English (//www.t-mobile.com) Español (es.t-mobile.com)

Shop phones by brand (//www.t-mobile.com/cell-phones) 

New featured phones 

Apps & connected devices (https://www.t-mobile.com/apps/t-mobile-apps) 

Plans & information (https://www.t-mobile.com/cell-phone-plans) 

Switch to T-Mobile (https://www.t-mobile.com/resources/how-to-join-us) 

T-Mobile benefits (https://www.t-mobile.com/brand/benefits) 

Order info (https://www.t-mobile.com/order-status) 

Support (https://www.t-mobile.com/support) 

My account (https://my.t-mobile.com/account/account-overview) 

More than wireless (https://www.t-mobile.com/brand/benefits) 

About T-Mobile (https://www.t-mobile.com/about-us) 


Corporate responsibility (https://www.t-mobile.com/responsibility) 


Careers (https://www.t-mobile.com/careers) 



 (<https://www.t-mobile.com>)

 (<https://www.instagram.com/tmobile/>)

 (<https://www.facebook.com/TMobile>)

 (<https://twitter.com/TMobile>)

© 2002–2021 T-Mobile USA, Inc.

About (<https://www.t-mobile.com/about-us>)

Investor relations (<https://investor.t-mobile.com/investors/default.aspx>)

Press (<https://www.t-mobile.com/news>)

Careers (<https://www.t-mobile.com/careers>)

Deutsche Telekom (<https://www.telekom.com/en>)

Puerto Rico (<https://www.t-mobilepr.com/>)

Privacy notice (<https://www.t-mobile.com/privacy-center/our-practices/privacy-policy>)

Interest-based ads (<https://www.t-mobile.com/privacy-center/education-and-resources/advertising-analytics>)

Privacy Center (<https://www.t-mobile.com/privacy-center>)

Consumer information (<https://www.t-mobile.com/responsibility/consumer-info>)

Public safety/911 (<https://www.t-mobile.com/responsibility/consumer-info/safety/9-1-1>)

Terms & conditions (<https://www.t-mobile.com/responsibility/legal/terms-and-conditions>)

Terms of use (<https://www.t-mobile.com/responsibility/consumer-info/policies/terms-of-use>)

Accessibility (<https://www.t-mobile.com/responsibility/consumer-info/accessibility-policy>)

Open Internet (<https://www.t-mobile.com/responsibility/consumer-info/policies/internet-service>)

Do Not Sell My Personal Information





SUPPORT

Additional Steps to Protect Yourself

At this time, we have *no* information that indicates any passwords, postpaid PIN numbers, or financial or payment information have been compromised but it's always a good practice to regularly **update your PIN/Passcode** to help keep your account secure.

Provided below are some general recommendations for protecting yourself, as well as information on how to obtain a free credit report and place a fraud alert or security freeze on your credit report.

On this page:

- **[General Recommendations for Protecting Yourself](#)**
- **[Information on Obtaining a Free Credit Report](#)**
- **[Information on Implementing a Fraud Alert or Security Freeze](#)**
- **[FTC Contact Information](#)**
- **[Additional Resources](#)**

General Recommendations for Protecting Yourself

- 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.

- 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's attorney general to learn more about the steps you can take to protect yourself against identity theft. Please see below for information on how to **contact the FTC**, and your **state's attorney general**.
- 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.
- 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



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



Chester, PA 19022-2000

+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,



Iowa Residents: 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 118Frankfort, 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.



Take our survey

Can't find what you're looking for?

 **Contact Us**



 **Ask our community**



My account



More than wireless



About T-Mobile



Corporate responsibility



Careers

