Notice To Customers of Data Security Incident

Notice of Data Security Incident
We are notifying you of a recent data security incident involving your personal information. This notice explains the incident, steps Xfinity has taken to address it, and guidance on what you can do to protect your personal information.

What Happened? On October 10, 2023, one of Xfinity's software providers, Citrix, announced a vulnerability in one of its products used by Xfinity and thousands of other companies worldwide. At the time Citrix made this announcement, it released a patch to fix the vulnerability. Citrix issued additional mitigation guidance on October 23, 2023. We promptly patched and mitigated our systems.

However, we subsequently discovered that prior to mitigation, between October 16 and October 19, 2023, there was unauthorized access to some of our internal systems that we concluded was a result of this vulnerability. We notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, it was determined that information was likely acquired.

What Information Was Involved? On December 6, 2023, we concluded that the information included usernames and hashed passwords. For some customers, other information was also included, such as names, contact information, last four digits of social security numbers, dates of birth and/or secret questions and answers. However, our data analysis is continuing, and we will provide additional notices as appropriate.

What We Are Doing. To protect your account, we have proactively asked you to reset your password. The next time you login to your Xfinity account, you will be prompted to change your password, if you haven't been asked to do so already.

What You Can Do. We strongly encourage you to enroll in two-factor or multi-factor authentication. While we advise customers not to re-use passwords across multiple accounts, if you do use the same information elsewhere, we recommend that you change the information on those other accounts, as well. You can review the "Additional Information" section below for information on how you can further protect your personal information.

More Information. If you have additional questions, please contact Xfinity Customer Service at 1-800-xfinity. More information is available on the Xfinity website at www.xfinity.com/dataincident.

We know that you trust Xfinity to protect your information, and we can't emphasize enough how seriously we are taking this matter. We remain committed to continue investing in technology, protocols and experts dedicated to helping to protect your data and keeping you, our customer, safe.

Sincerely,

Xfinity

Additional Information

In general, you should remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You are entitled to a free copy of your credit report annually. To obtain your credit report, visit www.annualcreditreport.com, call toll-free 1-877-322-8228, or mail an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You can also purchase a copy of your credit report or contact the three major credit reporting bureaus at:

Equifax	Experian	TransUnion
PO Box 740241	PO Box 2002	PO Box 1000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
888-378-4329	888-397-3742	800-888-4213

You should report any actual or suspected identity theft to the Federal Trade Commission and law enforcement. You can obtain information from the Federal Trade Commission and the three major credit bureaus about additional steps you can take to protect yourself against identity theft and fraud, as well as information on placing security freezes and fraud alerts on your credit report. You can contact the Federal Trade Commission at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; and 1-877-ID-THEFT (1-877-438-4338). This notice was not delayed as a result of a law enforcement investigation.

You may place a security freeze on your credit reports, free of charge. 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. You will need to place a security freeze separately with each of the three major credit bureaus if you wish to place a freeze on all of your credit files. In order to request a security freeze, you will need to supply your full name, address, date of birth, Social Security number, current address, all addresses for up to five previous years, email address, a copy of your state identification card or driver's license, and a copy of a utility bill, bank or insurance statement, or other statement proving residence. To find out more on how to place a security freeze, contact the credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
888-298-0045	888-397-3742	800-916-8800
equifax.com/personal/credit-report-services/credit-freeze/	experian.com/freeze/center.html	transunion.com/credit-freeze

At no charge, you can also have the three major credit bureaus place a fraud alert on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact the credit reporting agencies:

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19106
888-836-6351	888-397-3742	800-916-8800
equifax.com/personal/credit-report-services/credit-fraud-alerts/	experian.com/fraud/center.html	transunion.com/fraud-alerts

For New York residents, the New York Office of the Attorney General can be contacted at The Capitol, Albany, NY, 12224, ag.ny.gov, or 1-800-771-7755.

For North Carolina residents, the North Carolina Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699, ncdoj.gov, or 919-716-6000.

How will customers know to change their passwords?
The next time a customer logs in to their Xfinity account, they will be prompted to change their password, if they haven't been asked to do so already.

How will customers know if communications from Xfinity about the data incident are legitimate?
We will not reach out directly to customers over the phone, in email or via text message to update their passwords and will not ask customers to update their payment information in connection with this data incident. Customers are advised that any direct reach out via email or text message to update their passwords, or to update their payment information, could be a phishing attempt. Learn more about how to protect yourself from phishing here.

Why are you sending notifications to customers about a data breach?
Xfinity is providing notice of a recent data security incident. Starting today, customers are being notified through a variety of channels, including through the Xfinity website, email, and news media.

How did this happen?
Between October 16 and October 19, 2023, there was unauthorized access to our internal systems that we concluded was a result of the Citrix vulnerability.

What is Citrix?
Citrix Systems, Inc. is a multinational cloud computing and virtualization technology company used by thousands of companies worldwide that provides server, application and desktop virtualization, networking, software as a service, and cloud computing technologies.

Who is IDX?
IDX was Xfinity's incident response provider managing customer notifications and call center support immediately following the incident.

What does it mean to have a password hashed?
Password hashing uses an algorithm to turn your password into a short string of different numbers and letters for security purposes.

What information does Xfinity have about its customers?
Visit www.xfinity.com/privacy.

How will Comcast prevent another incident from occurring?
In today's environment, large companies face cybersecurity threats constantly. We have robust security programs in place which help us to discover criminal activity such as this one and to quickly mitigate it. Customers trust us to protect their information, and the company takes this responsibility seriously. We remain committed to investing in technology, protocols and experts dedicated to helping protect our customers.