

Holland & Knight

1650 Market Street, Suite 3300 | Philadelphia, PA 19103 | T 215.252.9600 | F 215.867.6070
Holland & Knight LLP | www.hklaw.com

Paul Bond
+1 215-252-9535
Paul.Bond@hklaw.com

January 19, 2024

VIA EMAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Incident Notification

To Whom It May Concern:

We represent Comcast Cable Communications LLC (“Comcast”) and are writing to provide you with notice of an incident that may impact the personal information of Maryland residents.

By providing this notice, Comcast does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction. The investigation into this incident is ongoing and this notice will be supplemented, if necessary, with any materials facts learned subsequent to its submission. We respectfully submit that this letter and its contents constitute confidential and proprietary information and, therefore, are exempt from public disclosure.

Background

On October 10, 2023, one of Comcast’s software providers, Citrix, announced a vulnerability in one of its products used by Comcast and thousands of other companies worldwide. Citrix issued additional mitigation guidance on October 23, 2023. Comcast promptly patched and mitigated the Citrix vulnerability within its systems. However, Comcast subsequently discovered that, between October 16 and October 19, 2023, there was unauthorized access to some of Comcast’s internal systems that Comcast concluded was a result of the vulnerability. Comcast notified federal law enforcement and conducted an investigation into the nature and scope of the incident. On November 16, 2023, the investigation determined that information was likely acquired.

Username and Hashed Password Notice

After an additional review of the affected systems and data, on December 6, 2023, Comcast concluded that the information included username and hashed password for 1,388,883 Maryland customers. For some Maryland customers, other information was also included, such as name, last four digits of Social Security number, date of birth, and/or secret questions and answers. Please note this number represents the total number of unique usernames at issue for residents and a single resident may have more than one username.

Atlanta | Austin | Birmingham | Boston | Century City | Charlotte | Chattanooga | Chicago | Dallas | Denver | Fort Lauderdale
Houston | Jacksonville | Los Angeles | Miami | Nashville | Newport Beach | New York | Orlando | Philadelphia
Portland | Richmond | San Francisco | Stamford | Tallahassee | Tampa | Tysons | Washington, D.C. | West Palm Beach

Algiers | Bogotá | London | Mexico City | Monterrey

Comcast issued notice to these customers starting on December 18, 2023 through a variety of channels, including through the Xfinity website, email, and news media. Notice was provided in substantially the same form as the notice attached as *Attachment 1*.

Comcast is requiring these customers to reset their password to protect affected accounts. While Comcast advises customers not to re-use passwords, Comcast is recommending that customers change passwords for other accounts for which customers use the same username and password or security question.

Social Security Number / Driver's License Number Notice

After further review of affected systems and data, on January 18, 2024, Comcast concluded that the information also included the Social Security number and/or driver's license number for 300 Maryland customers. Comcast intends to issue written notice to these customers on or around January 29, 2024 in substantially the same form as the notice attached as *Attachment 2*. Comcast is offering these customers 24 months of complimentary credit monitoring and identity restoration services through IDX, as well as additional information on how to protect against identity theft and fraud should they feel it appropriate to do so.

Contact

Should you have any questions regarding this notification or other aspects of this incident, please contact the undersigned at paul.bond@hklaw.com or 215.252.9535.

Sincerely,

HOLLAND & KNIGHT LLP

A handwritten signature in black ink, appearing to read "Paul Bond", written over a light blue rectangular background.

Paul Bond

Attachment 1

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 IDX, Xfinity's incident response provider managing customer notifications and call center support, at 888-799-2560 toll-free 24 hours a day, seven days a week. 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 PO Box 740241 Atlanta, GA 30374 www.equifax.com 888-378-4329	Experian PO Box 2002 Allen, TX 75013 www.experian.com 888-397-3742	TransUnion PO Box 1000 Chester, PA 19016 www.transunion.com 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 P.O. Box 105788 Atlanta, GA 30348 888-298-0045 equifax.com/personal/credit-report-services/credit-freeze/	Experian P.O. Box 9554 Allen, TX 75013 888-397-3742 experian.com/freeze/center.html	TransUnion P.O. Box 160 Woodlyn, PA 19094 800-916-8800 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 P.O. Box 105069 Atlanta, GA 30348 888-836-6351 equifax.com/personal/credit-report-services/credit-fraud-alerts/	Experian P.O. Box 9554 Allen, TX 75013 888-397-3742 experian.com/fraud/center.html	TransUnion P.O. Box 2000 Chester, PA 19106 800-916-8800 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.

Attachment 2

Re: Supplemental Notice of Data Breach

Dear <<name>>:

We are writing to provide you with an update on the recent 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 the Citrix 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.

On December 18, 2023, we issued an initial notification to customers through a variety of channels, including through the Xfinity website, email, and news media. We continued our investigation after we issued this notice.

What Information Was Involved? As part of our ongoing investigation, on January 18, 2024, we determined additional information of yours was involved in the incident. This additional information includes your [name/Social Security number/driver's license number].

What We Are Doing. In addition to taking the steps detailed above, we are offering you complimentary credit monitoring and identity restoration services through IDX, a ZeroFox Company. IDX identity protection services include 24 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services.

What You Can Do. We recommend you review the "Steps You Can Take To Protect Your Information" section included with this letter, which includes instructions on how to enroll in the credit monitoring services, as well as additional information on how you can further protect your personal information.

More Information. If you have additional questions, please contact IDX, Xfinity's incident response provider managing credit monitoring enrollment, customer notifications, and call center support, at XXX-XXX-XXXX toll-free 24 hours a day, seven days a week.

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

Steps You Can Take To Protect Your Information

Enroll in credit monitoring: To enroll in the complimentary credit monitoring and identity restoration services, call [number], go to <https://response.idx.us/xfinity>, or scan the QR image. Please note the deadline

to enroll is **Enrollment Deadline**. The monitoring included in the membership must be activated to be effective. You must have established credit and access to a computer and the internet to use this service.

Review account statements: You should remain vigilant against incidents of fraud and identity theft by reviewing your account statements and monitoring your free credit reports for suspicious activity or errors.

Check your credit report: 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
PO Box 740241
Atlanta, GA 30374
equifax.com
888-378-4329

Experian
PO Box 2002
Allen, TX 75013
experian.com
888-397-3742

TransUnion
PO Box 1000
Chester, PA 19016
transunion.com
800-888-4213

Place a security freeze: 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 the credit reporting agency with information that identifies you, including your full name, date of birth, Social Security number, all addresses for up to five previous years, 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
P.O. Box 105788
Atlanta, GA 30348
888-298-0045
equifax.com/personal/credit-report-services/credit-freeze/

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
800-916-8800
transunion.com/credit-freeze

Place a fraud alert: 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
P.O. Box 105069
Atlanta, GA 30348
888-836-6351
equifax.com/personal/credit-report-services/credit-fraud-alerts/

Experian
P.O. Box 9554
Allen, TX 75013
888-397-3742
experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19106
800-916-8800
transunion.com/fraud-alerts

Contact additional resources: If you believe you are the victim of identity theft or have reason to believe that your personal information has been misused, you should contact the Federal Trade Commission and/or your state Attorney General. You can obtain information from these sources about additional steps you can take to protect yourself against identity theft and fraud, as well as information on security freezes and fraud alerts. 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). Instances of known or suspected identity theft should be promptly reported to law enforcement and you have the right to file a police report if you ever experience identity theft or fraud. Notice was not delayed as a result of law enforcement.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, oag.state.md.us, or 888-743-0023. Xfinity can be contacted at 1701 John F. Kennedy Blvd., Philadelphia, PA 19103 and 1-800-XFINITY.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information and the consumer reporting agencies may not report outdated negative information. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active-duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

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 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.