WILLKIE FARR & GALLAGHER LLP

1875 K Street, N.W.
Washington, DC 20006-1238

Tel: 202 303 1000
Fax: 202 303 2000

February 20, 2024

BY EMAIL
Consumer Protection & Antitrust Bureau
Office of the Attorney General
1 Granite Place South
Concord, NH 03301
Doj-cpb@doj.nh.gov

Dear Madam or Sir,

We are providing this notification to your office in accordance with N.H. Rev. Stat. § 359-C:20.I(b) on behalf of our client, Xerox Corporation ("Xerox").

In early December 2023, Xerox became aware that an unauthorized third party had gained access to a portion of the network of a Xerox subsidiary, Xerox Business Services ("XBS"). While Xerox personnel promptly detected and contained this unauthorized activity, our investigation has confirmed that on December 10th, 2023 the unauthorized third party was able to acquire a limited amount of information from XBS's systems before the incident was fully contained. The incident otherwise had no impact on Xerox's corporate systems, operations or data, and no effect on XBS operations.

Xerox, with the assistance of third-party cybersecurity experts, has been conducting a thorough investigation into this incident and has taken steps to further secure the XBS IT environment. It is not currently clear how the unauthorized third party initially gained access to the XBS network, but to prevent further unauthorized access Xerox personnel reset all access credentials on the XBS network and is implementing multi-factor authentication to reduce the risk of future such incidents.

On January 30th, Xerox's investigation determined that the of one (1) New Hampshire resident was compromised in this incident. Attached to this letter is a sample of the notification letter that we expect to provide to the affected New Hampshire resident on February 20, 2024.

Xerox values the security of the personal information in its possession and its internal IT team is working diligently to ensure it has addressed any vulnerabilities that may have contributed to this incident. Xerox will continue to assess any obligations in connection with the incident, and will provide supplemental reporting, as appropriate.

If your office has any further questions, please do not hesitate to contact us.

***

Xerox claims confidential treatment for this letter and the information contained herein or attached hereto (together, the "Confidential Material") pursuant to N.H. Rev. Stat. §§ 91-A:5(IV)

and 91-A:5(XI). The Confidential Material contains commercial information that is of a confidential nature. N.H. Rev. Stat. § 91-A:5(IV). The Confidential Material also contains information about the security of an information system. N.H. Rev. Stat. § 91-A:5(XI). Accordingly, Xerox hereby requests, pursuant to N.H. Rev. Stat. § 91-A:5, that the Confidential Material and all other documents and communications provided to your office with regard to this matter be afforded confidential treatment.

In accordance with N.H. Rev. Stat. § 91-A:5 and other laws and regulations, Xerox submits the Confidential Material to your office with the request that it be kept in a non-public file and that only staff of your office have access to it. Should your office receive any request for any of the Confidential Material, pursuant to open records, freedom of information, sunshine, or other public record disclosure laws, subpoena, discovery in a private civil action or admissible evidence in a private civil action, we ask that the information not be disclosed, pursuant to N.H. Rev. Stat. § 91-A:5. Xerox requests that the undersigned be immediately notified of such request, and be furnished a copy of all written materials pertaining to such request (including but not limited to the request and any determination relating thereto), and that Xerox be given an opportunity to object in advance to any such disclosure.

Should your office be inclined to grant such a request, Xerox requests that we be given at least ten (10) business days' advance notice of any such decision to enable us to pursue any remedies that may be available to us. In such event, Xerox requests that you email us rather than rely upon the United States mail for such notice. You may make such notification directly to the undersigned. If your office is not satisfied that the enclosed materials are exempt from disclosure pursuant to N.H. Rev. Stat. § 91-A:5, Xerox stands ready to supply further particulars, and to request a hearing on the claim of exemption.

The Confidential Material and the information contained herein remain the property of Xerox. Accordingly, we request that these items (and all copies thereof) be returned to us after your office has completed its efforts on this matter. Furthermore, the production of the Confidential Material to your office is not intended to, and does not, waive any privilege or protection. The requests set forth in the preceding paragraphs also apply to any memoranda, notes, transcripts or other writings of any sort that are made by, or at the request of, any employee of your office (or any other government agency) and which (1) incorporate, include or relate to any of the Confidential Material; or (2) refer to any conference, meeting or telephone conversation between Xerox's current or former employees, representatives, agents, auditors or counsel on the one hand, and employees of your office (or any other government agency) on the other, relating to the Confidential Material.

The Confidential Material is provided in an effort to facilitate the ongoing discussions between Xerox and your office. Xerox reserves all rights.

Sincerely,

Laura Jehl
Willkie Farr & Gallagher LLP

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

February 20, 2024

K8729-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

NOTICE OF SECURITY INCIDENT

Dear Sample A. Sample:

We are writing to let you know about an incident that affected the security of information maintained by a Xerox subsidiary, Xerox Business Services ("XBS"). The data privacy and protection of our clients, partners, and employees are our highest priority.

WHAT HAPPENED?
In early December 2023, we became aware that an unauthorized third party had gained access to a portion of the XBS network. While Xerox personnel promptly detected and contained this unauthorized activity, our investigation has confirmed that on December 10th, 2023 the unauthorized third party was able to acquire a limited amount of information from XBS's systems before the incident was fully contained.

We are conducting a thorough investigation of the incident. We have notified law enforcement of this incident, but have not delayed this notification as a result of any law enforcement investigation.

WHAT INFORMATION WAS INVOLVED?
Our investigation indicates that your name, contact information and social security number were affected in this incident.

WHAT WE ARE DOING?
Upon learning of this unauthorized activity, we promptly began an investigation and took steps to address this incident, including by taking steps to prevent unauthorized actors from obtaining further personal information such as resetting all access credentials for the XBS network.

We do not have information to suggest that your personal information has been used by any unauthorized third party, but to mitigate the risk to you, we have secured the services of Experian to provide identity and credit monitoring services at no cost to you for . Experian is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Below, please find information on signing up for a complimentary membership to Experian's identity monitoring services:

Additional information describing the services and enrollment instructions are included in Attachment A to this letter.

WHAT YOU CAN DO?
We encourage you to contact Experian and take advantage of the credit monitoring and identity theft protection services we are providing to you free of charge. In addition, remain vigilant and carefully review your accounts for any suspicious activity. This is a best practice for all consumers.

If you detect any suspicious activity on an account, you should change the password and security questions associated with the account, and promptly notify the financial institution or other company with which the account is maintained and any relevant government agency, such as your state's consumer protection agency.

If you would like to take additional steps to protect your personal information, Attachment B to this letter provides helpful resources on how to do so, including recommendations from the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

FOR MORE INFORMATION
We take our responsibility to protect your information extremely seriously, and we sincerely regret any inconvenience that this matter has caused you.

If you have any questions regarding this incident or the services available to you, please call Monday through Friday 8am to 8pm CST (excluding major U.S. holidays). Be prepared to provide your engagement number

Sincerely,

William Eipert
Chief Privacy Officer
Xerox Corporation

Attachment A

EXPERIAN PRODUCT INFORMATION

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for .

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at Monday through Friday 8am to 8pm CST (excluding major U.S. holidays) by . Be prepared to provide engagement number as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*****
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Below are additional helpful tips you may want to consider to protect your personal information.

Review Your Credit Reports and Account Statements; Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by reviewing your credit reports and account statements closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or other company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidents of identity theft to proper law enforcement authorities. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact law enforcement, the Federal Trade Commission ("FTC") and/or the Attorney General's office in your home state. You can also contact these agencies for information on how to prevent or avoid identity theft, and you can contact the FTC at:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
www.ftc.gov/IDTHEFT
1-877-IDTHEFT (438-4338)

Copy of Credit Report

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to the Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print this form at https://www.annualcreditreport.com/manualRequestForm.action. Credit reporting agency contact details are provided below.

Equifax:
equifax.com
equifax.com/personal/credit-report-services
P.O. Box 740241
Atlanta, GA 30374
866-349-5191

Experian:
experian.com
experian.com/help
P.O. Box 2002
Allen, TX 75013
888-397-3742

TransUnion:
transunion.com
transunion.com/credit-help
P.O. Box 1000
Chester, PA 19016
888-909-8872

When you receive your credit reports, review them carefully. Look for accounts or credit inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number, that is inaccurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Fraud Alert

You may want to consider placing a fraud alert on your credit file. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. If you have already been a victim of identity theft, you may have an extended alert placed on your report if you provide the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above.

Security Freeze

You have the right to place a security freeze on your credit file free of charge. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. As a result, using a security freeze may delay your ability to obtain credit. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name; social security number; date of birth; current and previous addresses; a copy of your state-issued identification card; and a recent utility bill, bank statement, or telephone bill.

Federal Fair Credit Reporting Act Rights

The Fair Credit Reporting Act (FCRA) is federal legislation that regulates how consumer reporting agencies use your information. It promotes the accuracy, fairness, and privacy of consumer information in the files of consumer reporting agencies. As a consumer, you have certain rights under the FCRA, which the FTC has summarized as follows: you must be

told if information in your file has been used against you; you have the right to know what is in your file; you have the right to ask for a credit score; you have the right to dispute incomplete or inaccurate information; consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. Identity theft victims and active duty military personnel have additional rights.

For more information about these rights, you may go to www.ftc.gov/credit or write to: Consumer Response Center, Room 13-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

Additional Information

You have the right to obtain any police report filed in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

You may consider starting a file with copies of your credit reports, any police report, any correspondence, and copies of disputed bills. It is also useful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

For Colorado, Delaware, and Illinois residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Maryland residents: You may contact the Office of the Maryland Attorney General, 200 St. Paul Place, Baltimore, MD 21202, http://www.marylandattorneygeneral.gov, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, 9001 Mail Service Center, Raleigh, NC 27699-9001, http://www.ncdoj.gov, 1-877-566-7226. You are also advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, including the Federal Trade Commission and the Oregon Attorney General.

For Georgia, Maryland, New Jersey, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit bureaus directly to obtain such additional report(s).

For New York residents: You may contact the New York Office of the Attorney General at: The Capitol, Albany, NY 12224-0341, http://www.ag.ny.gov/home.html, 1-800-771-7755, and the New York Department of State Division of Consumer Protection at: 99 Washington Avenue, Albany, New York 12231-0001, http://www.dos.ny.gov/consumerprotection, 1-800-697-1220.

For Rhode Island residents: You may obtain information from the Federal Trade Commission and the credit reporting agencies about fraud alerts and security freezes. You may also contact the Rhode Island Office of the Attorney General, 150 South Main Street Providence, Rhode Island 02903, http://www.riag.ri.gov, (401) 274-4400.