

18 1 4601 *****SNGLP

SAMPLE A. SAMPLE - Adult

APT ABC

123 ANY ST

ANYTOWN, US 12345-6789



May 12, 2023

Subject: Notice of Data [Extra1]

Dear Sample A. Sample:

We are writing to inform you about a recent data security incident experienced by Brown & Streza, LLP (“Brown & Streza”) that may have involved your personal information. Please read this letter carefully. It contains important details about the incident and resources you may utilize to help protect your personal information.

What Happened? On January 18, 2023, we noted unusual activity within our computer network. With the assistance of independent cybersecurity experts, we took immediate steps to ensure our network was secure and launched a forensic investigation to determine what happened and whether any sensitive information may have been affected. Based on that investigation, we learned that an unknown actor gained unauthorized access to our network and may have acquired certain files, some of which may have contained individuals’ personal information. We then undertook a comprehensive review of the potentially impacted data to determine precisely whose personal information may have been involved. That process concluded on April 12, 2023 and identified your information as potentially impacted, which is the reason for this notification.

What Information Was Involved? The information that may have been involved in this incident includes your name, as well as your [Extra2].

What Are We Doing? As soon as we discovered this incident, we took the steps described above and reported the incident to law enforcement. We implemented additional security measures to reduce the risk of future incidents. And we are notifying you of the event to advise you about resources we are providing and additional steps you can take to help protect your information.

While we have no evidence that any of your information was misused, out of an abundance of caution we are offering you complimentary identity protection services through Experian IdentityWorks—a data breach and recovery services expert. These services include 12 months of credit¹ and dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services.

¹ To receive credit monitoring services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** August 31, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product or need assistance with enrolling, please contact Experian's customer care team at (855) 896-4446 by August 31, 2023.

You are automatically eligible for Experian identity restoration services for 12 months from the date of this letter (www.ExperianIDWorks.com/restoration). Please be prepared to provide engagement number B090748 as proof of eligibility.

What Can You Do? We recommend that you review the guidance included with this letter about how to protect your information. You can also enroll in the complimentary identity protection services being offered to you through Experian IdentityWorks by using the activation code provided above.

For More Information: Further information about how to help protect your information appears on the following page. If you have questions about this matter or need assistance enrolling in the complimentary services being offered to you, please call Experian at (855) 896-4446 Monday through Friday from 6 am – 8 pm Pacific, or Saturday and Sunday from 8 am – 5 pm Pacific (excluding major U.S. holidays).

We take your trust in us and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,

Richard E. Streza

Richard E. Streza
Managing Partner
Brown & Streza, LLP

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

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 <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. 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. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. 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 potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. 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 insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

California Attorney General

Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, CA 94244-2550
<https://oag.ca.gov/contact>
1-916-210-6276

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH 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.
- Internet Surveillance: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- Identity Restoration: Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- Experian IdentityWorks ExtendCARE™: 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.