



SIDLEY AUSTIN LLP
1501 K STREET, N.W.
WASHINGTON, D.C. 20005
+1 202 736 8000
+1 202 736 8711 FAX

AMERICA • ASIA PACIFIC • EUROPE

+1 202 736 8465
CTBROWN@SIDLEY.COM

VIA EMAIL

Office of the Attorney General
Email: Idtheft@oag.state.md.us

March 27, 2025

Re: **Security Incident Notification**

Dear Attorney General Anthony G. Brown,

We are writing on behalf of the Civic Committee of the Commercial Club of Chicago (the “Civic Committee”) to inform you of a recent data security incident. By providing this notice, Civic Committee does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland breach notification statute, or personal jurisdiction.

Civic Committee took action to investigate the incident, report the incident to law enforcement, and further enhance its security safeguards. On March 21, 2025, Civic Committee identified that 1 Maryland resident’s data was impacted and today began notifying affected individuals of the incident. For your reference, attached to this letter as Appendix A is a sample of the notice being provided to 1 Maryland resident, which includes an offer of free credit monitoring, fraud assistance, and cyber monitoring services via TransUnion for 24 months.

If you have any questions, please do not hesitate to contact me.

Sincerely,

A handwritten signature in cursive script that reads "Colleen Theresa Brown".

Colleen Theresa Brown
Partner

APPENDIX A

Civic Committee
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

 190 S LaSalle St, 39th Floor
Chicago, IL 60603
Phone: (312) 853-1200
Fax: (312) 853-1209
Email: civiccommittee@civicc.com

JOHN DOE
<<Address>>
<<City>>, <<State>> <<Zip>>



March 27, 2025

Dear John Doe,

We are writing to let you know about a data security incident that may have affected certain information in our possession. We take the security of your information very seriously and are contacting you directly to explain the circumstances as we understand them, the steps we have taken in response to the incident, and the resources we are making available to you.

What Happened?

We recently discovered that a third party gained unauthorized access to part of our IT systems. Upon discovery, we took immediate action to investigate the incident and report the incident to law enforcement. We conducted a detailed review of impacted data and are reaching out to you to let you know that the incident involved some of your personal information.

What Information May Have Been Involved?

The personal information included your <<PII elements>>. We are not aware of any misuse of your personal information at this time.

What We Are Doing

The privacy and security of your personal information is of utmost importance to us. In addition to the actions above, we continue to monitor our systems and identify improvements to our overall security. We have introduced additional measures to further enhance our security defenses. Finally, to support your needs, we are offering free credit monitoring services and fraud assistance to impacted individuals.

What You Can Do

We recommend that you remain vigilant by reviewing your personal records and monitor free credit reports. The free credit monitoring services we are offering provides you with access to **Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Non-Credit Public Records monitoring/Cyber Monitoring** services at no charge. These services provide you with alerts for twenty-four months from the date of enrollment when changes occur to any of one of your Experian, Equifax, or TransUnion credit files. When using this credit monitoring system, notifications will be sent to you the same day that any change or update takes place with any of the three bureaus. In addition to credit-related data, the services will also monitor any changes to your non-credit public records including: Change of Address, Court Records, and Social Security number trace. Cyber monitoring will look out for your personal data on the dark web and alert you if your personal identifiable information is found online.

000010103G0500

P

Finally, we also are providing you with proactive fraud assistance to help with any questions that you might have or in the event you become a victim of identity theft. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services and Fraud Assistance services, at no charge, please log on to <https://bfs.cyberscout.com/activate> and follow the instructions provided. When prompted, please provide the following unique code to receive services: <<**Unique Code**>>. In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and is not available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

For More Information

Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-800-405-6108 and supply the fraud specialist with your unique code listed above.

Please also refer to the enclosure entitled “Additional Ways to Protect Your Identity” for additional actions you should consider taking to protect yourself against fraud and identity theft.

Sincerely,

Suzanne Fisher
Vice President, Finance & Administration

Additional Ways to Protect Your Identity: Important Identity Theft Information

You may wish to take additional steps to protect your identity. Here are some steps we suggest you consider:

Reviewing Your Accounts and Credit Reports

Federal regulators recommend that you be especially vigilant for the next 12 to 24 months. As part of staying vigilant, you should regularly review your account statements and periodically obtain your credit report from one or more of the three national credit reporting companies. Those companies are:

Equifax 1-800-525-6285 Equifax.com	Experian 1-888-397-3742 Experian.com	TransUnion 1-800-680-7289 Transunion.com
---	---	---

You can obtain your credit report from each of those companies for free once every 12 months. Free reports are available online at www.annualcreditreport.com. You may also obtain a free report by calling toll free 1-877-322-8228, or by mailing 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. If you do not have any free credit reports left, you can still purchase a copy of your credit report by contacting one or more of the three credit reporting companies listed above.

Placing a Fraud Alert

A fraud alert tells lenders that they should verify your identification before they extend credit in your name. Each of the three nationwide credit reporting companies can place a fraud alert on your credit report.

If you wish to place a fraud alert, contact any one of the three credit reporting companies listed above. As soon as one company confirms your fraud alert, the others are notified to place fraud alerts as well.

Requesting a Security Freeze on Your Credit Report

A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Placing, lifting, or removing a security freeze is free of charge.

If you wish to place a security freeze on your credit report, you must do so separately at each credit reporting company. The credit reporting companies do not notify each other about security freezes.

Please be aware that while a security freeze is in effect, it may delay, interfere with, or prevent the timely approval of any request you make for new credit, loans, mortgages, employment, housing, or other services that require a credit check. If you want to allow a credit check for those or other purposes, you will have to lift the security freeze by contacting each credit reporting company. Each credit reporting agency will provide you a PIN number or a password when you place a security freeze. You will need that PIN or password to lift the freeze and should be careful to record it somewhere secure.

Suggestions if You Are a Victim of Identity Theft

If you find suspicious activity on your accounts or credit reports, or have other reason to believe your information is being misused, you should take the following steps:



File a Police Report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.

Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. If you file an identity theft complaint with the FTC, your case will be added to that database. You can find more information and file a complaint online at www.IdentityTheft.gov. You can also file a complaint by calling the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338), or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580. You may also wish to obtain a copy of *Identity Theft: A Recovery Plan*, a guide from the FTC to help you guard against and deal with identity theft. It is available online at: https://www.bulkorder.ftc.gov/system/files/publications/501a_idt_a_recovery_plan_508.pdf.

Exercise Your Rights Under the Fair Credit Reporting Act (FCRA). You have certain legal rights under the FCRA. These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have credit reporting companies correct or delete inaccurate, incomplete, or unverifiable information. You can find more information about your rights under the FCRA online at <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf>. The laws of your state may provide you with additional rights. Your state's attorney general or consumer protection department may be able to give you more information about your rights under state law.

Keep a record of your contacts. Start a file with copies of your credit reports, police reports, any correspondence, and copies of disputed bills. Keep a log of your conversations with creditors, law enforcement officials, credit reporting companies, and other relevant parties.

Special Information for Residents of the District of Columbia, Iowa, Maryland, Massachusetts, New York, North Carolina, Rhode Island, and Vermont.

District of Columbia residents can learn more about preventing identity theft from the District of Columbia Office of the Attorney General, by visiting their website at <https://oag.dc.gov/>, calling (202) 727-3400, or requesting more information via email oag@dc.gov or mail 400 6th Street NW, Washington DC 20001.

Iowa residents may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft. This office can be reached by visiting the website at www.iowaattorneygeneral.gov, calling (515) 281-5164 or requesting more information from the Office of the Attorney General, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at <http://www.oag.state.md.us/idtheft/index.htm>, calling the Identity Theft Unit at 1.410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. There is no charge to place a security freeze on your account; however, you may be required to provide the credit reporting agency with certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to its honoring your request.

New York residents may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; <https://ag.ny.gov/consumer-frauds-bureau/identity-theft>; Telephone: 800-771-7755.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at <https://ncdoj.gov/protecting-consumers/protecting-your-identity/>, calling 1.919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Rhode Island residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. Residents can learn more by contacting the Rhode Island Office of the Attorney General by phone at 1.410.274.4400 or by mail at 150 South Main Street, Providence, Rhode Island 02903.

Vermont residents may learn helpful information about fighting identity theft, placing a security freeze, and obtaining a free copy of your credit report on the Vermont Attorney General's website at <http://www.atg.state.vt.us>.



00001030300000

P

