

Eckell, Sparks, Levy, Auerbach, Monte, Sloane, Matthews & Auslander, P.C.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998



August 19, 2024

Notice of Data Incident

Dear [REDACTED]:

This letter is to inform you that Eckell, Sparks, Levy, Auerbach, Monte, Sloane, Matthews & Auslander, P.C (“Eckell Sparks”) experienced a data security incident which may have affected some of your personal information, including some privileged and confidential legal information. At present, there is no evidence that any of your personal information has been misused; however, out of an abundance of caution, we are notifying you of this incident and offering you the resources discussed below so that you can take precautionary steps to protect yourself, should you wish to do so.

Eckell Sparks is a law firm and, in that capacity, we receive information from our clients. We take the protection and proper use of your information seriously and sincerely apologize for any inconvenience this incident may cause.

What Happened?

On or about November 21, 2023, Eckell Sparks experienced a ransomware incident, despite our robust multi-factor authentication and other security measures and safeguards. We promptly launched an investigation, engaged a national cybersecurity firm to assist in assessing the scope of the incident, and took steps to mitigate the potential impact to our community. Unfortunately, these types of incidents are becoming increasingly common and organizations with some of the most sophisticated IT infrastructure available continue to be affected.

What Information Was Involved?

The types of information that may have been compromised was different for each individual but may have included your: Date of Birth and Social Security Number. In addition, some privileged and confidential communications may have been compromised. Please note that there is no evidence at this time that any Eckell, Sparks client privileged and confidential legal information has been misused as a result of the incident.

What Are We Doing?

We take the security of information that our clients entrust in us very seriously. Upon discovery, we immediately secured the environment in question and took steps to prevent further unauthorized access. We also engaged a third-party digital forensics investigator to conduct an exhaustive investigation of this matter and filed a report with the FBI. As part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and security measures to enhance the privacy and security of information in our systems. In addition to providing this notice to you, we are providing notice to privacy regulators and other parties as required.

We want to make sure you have the information you need so that you can take steps to help protect yourself from identity theft. We encourage you to remain vigilant and to regularly review and monitor relevant account statements and credit reports and report suspected incidents of identity theft to local law enforcement, your state's Attorney General, or the Federal Trade Commission (the "FTC"). We have included more information on these steps in this letter.

What Can You Do?

Complimentary Identity Protection and Credit Monitoring Services

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. 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 at no charge, please log on to **<https://www.mytrueidentity.com>** and follow the instructions provided. When prompted please provide the following unique code to receive services:

██████████.

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 may not be 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.

What Else Can You Do?

In addition to enrolling in the complimentary identity theft protection services being offered, we encourage you to review the enclosed *Steps You Can Take to Protect Your Information* for additional information on how to protect against identify theft and fraud.

For More Information

On behalf of Eckell Sparks, please accept my sincere apology for this isolated incident and any inconvenience it may cause you. Eckell Sparks values its relationship with its clients and others who provide us with information.

I can assure you that we are taking steps intended to prevent an incident like this from reoccurring and protect you and your information, now and in the future. If you have questions about this notice or this incident, or require further assistance, please do not hesitate to call 1-833-531-2225, Monday - Friday, excluding holidays, 8am - 8pm, and supply the fraud specialist with your unique code listed above

Sincerely,

Leonard A. Sloane, Esquire
Eckell Sparks Law Firm

Additional Important Information

For residents of Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia:

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Vermont: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-828-3171 (800-649-2424 toll free in Vermont only).

For residents of New Mexico: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For Residents of Washington, D.C.: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202
1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903
1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224
1-800-771-7755 <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts and Rhode Island: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.



PKHXKZ0010000100001020280000

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788

Atlanta, GA 30348

equifax.com/personal/credit-report-services/

1-888-Equifax (1-888-378-4329)

Experian Security Freeze

P.O. Box 9554

Allen, TX 75013

experian.com/freeze/center.html

1-888-397-3742

TransUnion Security Freeze

P.O. Box 160

Woodlyn, PA 19094

transunion.com/credit-freeze

1-833-395-6938

More information can also be obtained by contacting the Federal Trade Commission listed above.