

Kennedys

570 Lexington Ave.
8th Floor
New York, NY 10022

kennedyslaw.com

t +1 646 625 4030

Daniel.marvin@kennedyslaw.com

January 28, 2025

By Email

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

Dear Attorney General Brown:

Our office writes on behalf of our client, Steven Miller & Co. LLC ("Steven Miller & Co."), to provide notice for a data breach impacting the personally identifiable information of five (5) Maryland residents.

On or about July 8, 2024, Steven Miller & Co. learned that an unauthorized actor gained access to a web-based accounting platform as a result of a phishing scam. Upon learning about the incident, Steven Miller & Co. initiated an investigation with the assistance of our firm and third-party IT specialists (at our direction). After a thorough investigation, Steven Miller & Co. learned that the unauthorized actor acquired certain personal information. The identity of those individuals was learned by Steven Miller & Co. on November 22, 2024, at the conclusion of a forensic investigation and data review.

Steven Miller & Co. notified those individuals on January 21, 2025, and offered the opportunity to enroll of 12 months of complimentary credit monitoring for those persons whose Social Security Number was involved. In addition, a dedicated call center of trained professionals has been made available to provide support services and address inquiries concerning the incident, credit monitoring, identity protection services, and proactive fraud assistance to help with any questions individuals may have. These services are also being provided by Cyberscout, a TransUnion company.

In addition, Steven Miller & Co. implemented multi-factor authentication for all end-users, initiated a mandatory password reset, implemented security tools, and revised its information security policies and procedures.

Kennedys is a trading name of Kennedys CMK LLP. Kennedys Law LLP, a UK Limited Liability Partnership, is a partner of Kennedys CMK LLP

Kennedys offices, associations and cooperations: Argentina, Australia, Belgium, Bermuda, Brazil, Canada, Chile, China, Colombia, Denmark, Dominican Republic, England and Wales, France, Guatemala, Hong Kong, India, Ireland, Israel, Italy, Mexico, New Zealand, Northern Ireland, Norway, Oman, Pakistan, Panama, Peru, Poland, Portugal, Puerto Rico, Russian Federation, Scotland, Singapore, Spain, Sweden, Thailand, United Arab Emirates, United States of America.

Attorney General Anthony Brown
Office of the Attorney General

Should you have any further questions, please do not hesitate to contact me. Thank you.

Very truly yours,

/s/Daniel S. Marvin

Daniel S. Marvin

Partner
for Kennedys



Steven Miller & Co, LLC
 c/o Cyberscout
 555 Monster Rd SW
 Renton, WA 98057
 USBFS68



**STEVEN
 MILLER & CO.**
 A LIMITED LIABILITY COMPANY
 — CPA'S & ADVISORS —
 LOOKING BEYOND TODAY

Stefan Thonnard
 118 Granville Ave
 Annapolis MD 21401-3519



January 21, 2025

Notice of Data Breach

Dear Stefan Thonnard:

We are writing to inform you of a data security incident experienced by our company that involved your information as described below. We take privacy and security very seriously and are providing notice about the incident and steps you can take to help protect your information.

What Happened: On or about July 8, 2024, we learned that an unauthorized actor gained access to a web-based accounting platform as a result of a phishing scam. Upon learning about the incident, we immediately began an investigation with the assistance of cyber counsel and third-party IT specialists (at the direction of counsel). After a thorough investigation, we learned that the unauthorized actor acquired certain personal information. We do not have any evidence of misuse of your data. Nor are we aware of any reports of misuse of your data.

What Information Was Involved: The information involved includes your first and last name, in combination with the following data element(s): Social Security number and driver's license.

What We Are Doing: We also are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no cost to you. These services provide you with alerts for twelve 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. Instructions about how to enroll in these services and additional resources available to you are included in the enclosed “*Steps You Can Take to Help Protect Your Information.*”

What You Can Do: To date, we are not aware of any reports of identify fraud as a result of this incident. As a general matter, it is always prudent to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact the financial institution or company. We have provided additional information below, which contains more information about steps you can take to help protect yourself against fraud and identity theft, as well as credit monitoring enrollment instructions.

For More Information: Should you have any questions or concerns, please contact our dedicated assistance line with TransUnion at 1-800-405-6108, Monday through Friday, excluding major U.S. holidays, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time. Please know that the security of information is of the utmost importance to us. We stay committed to protecting your trust in us and continue to be thankful for your support during this time.

Sincerely,

Steven Miller
Partner

Faby Law
Partner

Enclosure: *Steps You Can Take to Help Protect Your Information*

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Enrollment in Credit Monitoring Services

To enroll in Credit Monitoring 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: **1DDFCCFE608F**.

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.

Monitor Your Accounts and Credit Reports

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements and explanation of benefits forms for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit www.annualcreditreport.com or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you should provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

TransUnion 1-800-680-7289 www.transunion.com TransUnion Fraud Alert P.O. Box 2000 Chester, PA 19016-2000 TransUnion Credit Freeze P.O. Box 160 Woodlyn, PA 19094	Experian 1-888-397-3742 www.experian.com Experian Fraud Alert P.O. Box 9554 Allen, TX 75013 Experian Credit Freeze P.O. Box 9554 Allen, TX 75013	Equifax 1-888-298-0045 www.equifax.com Equifax Fraud Alert P.O. Box 105069 Atlanta, GA 30348-5069 Equifax Credit Freeze P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--



Additional Information

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

For D.C. residents, the District of Columbia Attorney General may be contacted at 441 4th Street NW #1100, Washington, D.C. 20001; 202-727-3400, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202; 1-888-743-0023; or www.marylandattorneygeneral.gov.

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: (i) the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (ii) the consumer reporting agencies may not report outdated negative information; (iii) access to your file is limited; (iv) you must give consent for credit reports to be provided to employers; (v) you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; (vi) and you may seek damages from violators. 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 https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, FTC, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov>.

For North Carolina residents, the North Carolina Attorney General may be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Oregon residents, the Oregon Attorney General may be contacted at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096; 1-877-877-9392; and <https://doj.state.or.us/consumer-protection/>.

For Rhode Island residents, the Rhode Island Attorney General may be contacted at 150 South Main Street, Providence, RI 02903; 1-401-274-4400; and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are 0 Rhode Island residents impacted by this incident.