

CIPRIANI & WERNER

A PROFESSIONAL CORPORATION

ATTORNEYS AT LAW

Amanda Ruggieri
ARuggieri@c-wlaw.com

450 Sentry Parkway, Suite 200
Blue Bell, PA 19422

A Mid-Atlantic Litigation Firm

Visit us online at
www.C-WLAW.com

Jonathan Quagliarello
JQuagliarello@c-wlaw.com

Phone: (610) 567-0700

Fax: (610) 567-0712

www.C-WLAW.com

May 1, 2024

Via E-Mail (IDTheft@oag.state.md.us)

Office of the Attorney General
200 St. Paul Place
Baltimore, Maryland 21202

RE: Data Incident Notification

To Whom It May Concern:

We serve as counsel for Symphony Financial located at 441 A Carlisle Dr. Ste A, Herndon, VA 20170 and write to inform you of a data security incident. By providing this notice, Symphony Financial does not waive any rights or defenses under Maryland law, including the data breach notification statute.

On or around January 5, 2024, Symphony Financial became aware of potential unauthorized access to an employee email account. Upon discovery, Symphony Financial immediately took steps to secure the affected account and engaged a third-party team of forensic experts to determine the full nature and scope of the incident. Following a full and thorough investigation, Symphony Financial confirmed that a limited amount of personal information may have been accessed by an unauthorized third-party in connection with this incident. On March 27, 2024, after a thorough review, Symphony Financial confirmed that information related to forty-one (41) Maryland residents may have been accessed by an unauthorized party in connection with this incident. The impacted information was limited to first and last name in combination with payment card information.

On May 1, 2024, Symphony Financial sent written notice of this incident to the potentially impacted Maryland residents pursuant to Maryland state law. The notice letter included an offer of complimentary credit monitoring and identity protection services for twelve (12) months. The notice letter sent to the individual is substantially similar to the letter attached hereto as Exhibit "A."

If you have any questions, please contact me.

Very truly yours,



Amanda Ruggieri, Esquire
CIPRIANI & WERNER, P.C.

Exhibit A

Symphony Financial
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08824



May 1, 2024

RE: *Important Security Notification. Please read this entire letter.*

Dear [REDACTED]

Symphony Financial ("Symphony") writes to notify you of an incident that may have impacted some of your personal information described below.

Symphony takes the privacy and security of information in our care very seriously. At this time, there is no evidence to suggest that any information was actually viewed or misused. Out of an abundance of caution, we are providing you information about this incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

What Happened:

On January 5, 2024, Symphony became aware of potential unauthorized access to an employee email account. Upon discovery, we immediately performed a password reset for the affected account and engaged a third-party team of forensic investigators in order to determine the full nature and scope of the incident. Following a full and thorough investigation, it was confirmed that five (5) employee email accounts were subject to unauthorized access during this incident. Upon confirmation of unauthorized access to the employee email accounts, Symphony immediately investigated whether the affected accounts contained sensitive information pertaining to individuals. On March 27, 2024, following a thorough review, Symphony confirmed that a limited amount of information may have been accessed by an unauthorized third party in connection with this incident.

At this time, there is no indication that any information has been actually viewed or misused. However, we are providing this notification to you out of an abundance of caution and so that you may take steps to safeguard your information if you feel it is necessary to do so.

What Information Was Involved:

The potentially accessed information may have included your first name or initial and last name, in combination with your [REDACTED]

What Are We Doing:

Symphony has taken steps to address the incident and is committed to protecting personal information in its care. Upon learning of this incident, we immediately took steps to secure our email tenant and undertook a thorough investigation.

Credit Monitoring:

As an additional safeguard, 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 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.

What You Can Do:

In addition to enrolling in the complimentary credit monitoring service detailed within, we recommend that you remain vigilant in regularly reviewing and monitoring all of your account statements and credit history to guard against any unauthorized transactions or activity. If you discover any suspicious or unusual activity on any of your accounts, please promptly change your password, notify your financial institution or company if applicable, and take any additional steps needed to protect your account. Additionally, please report any suspicious incidents to local law enforcement and/or your state Attorney General. Please review the enclosed "Steps You Can Take to Help Protect Your Information" for additional resources.

For More Information:

Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center between the hours of 8:00 am to 8:00 pm Eastern time, Monday through Friday, excluding holidays at 1-800-405-6108. You can also write us at 441 A Carlisle Dr. Ste A, Herndon, VA 20170 or feel free to reach out to your advisor by email or telephone.

Symphony takes the security of information entrusted to our care very seriously. While it is regrettable this potential exposure occurred, please be assured that we are taking appropriate actions to rectify the situation and prevent such incidents in the future.

Sincerely,

Symphony Financial

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Activate Identity 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: **263D829DECA1**. 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

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 will need to 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 District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th St. NW Washington, D.C. 20001; 202-442-9828, and <https://oag.dc.gov/consumer-protection>.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-528-8662 or 1-888-743-0023; and <https://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, the consumer reporting bureaus 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 credit 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 violator. 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 www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

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.