



MULLEN
COUGHLIN^{LLC}
ATTORNEYS AT LAW

M. Alexandra Belton
Office: (267) 930-4773
Fax: (267) 930-4771
Email: abelton@mullen.law

426 W. Lancaster Avenue, Suite 200
Devon, PA 19333

July 3, 2024

VIA E-MAIL

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

Re: Notice of Data Event

To Whom It May Concern:

We represent Norshield Security Products, LLC (“Norshield”), located at 3232 Mobile Highway, Montgomery, AL 36108, and write to notify your office of a data event that may impact three (3) Maryland residents. By providing this notice, Norshield does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On February 19, 2024, Norshield became aware of suspicious activity occurring within certain systems on its network. In response, Norshield promptly took steps to secure its network environment and began a comprehensive investigation to determine what happened and what information may have been affected. Through its investigation, Norshield learned that an unauthorized actor likely copied certain files from its network on or around February 16, 2024. Working with a third-party data review team, Norshield subsequently began an extensive review of the relevant files to identify and catalogue what information was present and to whom that information related. The third-party data review was completed on May 23, 2024. Norshield then worked to review and reconcile the relevant data against its internal records to identify contact information in furtherance of providing individuals with notice. The types of personal information, as defined by Maryland law, that may be affected by this incident include names and Social Security number.

Notice to Maryland Residents

On July 5, 2024, Norshield is providing written notice of this incident to potentially affected individuals, including three (3) Maryland residents. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

In response to this event, Norshield acted promptly to conduct a diligent investigation and determine what information may be affected. Further, Norshield notified federal law enforcement regarding the event. Norshield also worked to review and enhance its existing security measures following the event. Norshield previously provided its current and former employees access to credit monitoring services and is now again providing access to credit monitoring services for 12 months, through Experian, to Maryland residents whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, Norshield is providing impacted individuals with guidance on how to better protect against identity theft and fraud. Norshield is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4773.

Very truly yours,



M. Alexandra Belton of
MULLEN COUGHLIN LLC

MABB/cml

Enclosure

EXHIBIT A



Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

July 5, 2024

L5654-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



NOTICE OF [Extra1]

Dear Sample A. Sample:

Norshield Security Products, LLC (“Norshield”) is writing [Extra2]. This notice provides you with details about the event, our response, and resources available to you to help protect your personal information, should you feel it is appropriate to do so.

What Happened? We became aware of suspicious activity occurring within certain systems on our network. We promptly took steps to secure our network environment and began a comprehensive investigation to determine what happened and what information may have been affected. Through our investigation, we learned that an unauthorized actor likely copied certain files from our network on or around February 16, 2024. We subsequently began an extensive review of the affected files to identify and catalogue what information was present and to whom that information related. Through that review, we determined that your information was present in the relevant files.

What Information Was Involved? The investigation determined that your name and the following types of information relating to you were present in files at issue: [Extra3].

What We Are Doing. We take this event and the security of the information in our care very seriously. Upon becoming aware of the unauthorized access, we quickly responded by isolating the impacted systems, ensuring the security of our wider network environment, and beginning a comprehensive investigation into the nature and scope of the event. We also proactively notified federal law enforcement of the event. We further reviewed our existing policies and procedures and implemented additional security measures and technical safeguards. As an added precaution, we are offering you access to credit monitoring services for [Extra4] months at no cost to you. Information about these services and instructions on how to activate them may be found in the attached Steps You Can Take to Help Protect Personal Information section of this notice. Please note, due to privacy restrictions, we are unable to enroll you in these services on your behalf.

What You Can Do. We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements and monitoring your free credit reports for suspicious activity and to detect any errors. We also encourage you to review the attached *Steps You Can Take to Help Protect Personal Information* and enroll in the credit monitoring services we are offering.

0000001



ENGAGE#

L5654-L01

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call 866-530-9923 toll-free Monday through Friday from 8am to 8pm Central Time (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Norshield Security Products, LLC

STEPS YOU CAN TAKE TO PROTECT PERSONAL INFORMATION

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for [Extra4] months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for [Extra4] months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary [Extra4]-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** October 31, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/3bplus>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 866-530-9923 by October 31, 2024. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR [Extra4]-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, Equifax and Transunion files 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 ExtendCARETM:** 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.

ENGAGE#

0000001



L5654-L01

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should consumers wish to place a fraud alert, please contact any of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers 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 the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer’s name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

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

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

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

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

to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and the relevant state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and <https://www.marylandattorneygeneral.gov/>.



