



Seyfarth Shaw LLP

1075 Peachtree Street, N.E.

Suite 2500

Atlanta, Georgia 30309-3958

T (404) 885-1500

F (404) 892-7056

jpriebe@seyfarth.com

T (404) 885-6773

www.seyfarth.com

November 8, 2024

VIA EMAIL: Idtheft@oag.state.md.us

Dear Sir or Madam:

We are writing to notify you, on behalf of Seyfarth Shaw LLP (“Seyfarth”), of a data security incident that has affected the personal information of a resident of Maryland. This notice may be supplemented upon further investigation. By providing this notice, Seyfarth does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the relevant state statute, or personal jurisdiction.

Background: Seyfarth first became aware of a potential security incident on November 4, 2024, involving unauthorized access to one of its employee accounts. During this incident, a threat actor conducted a social engineering attack, successfully impersonating a Seyfarth employee to manipulate the Seyfarth Service Desk staff. The Service Desk staff, believing the request was legitimate, modified the Multi-Factor Authentication (MFA) settings for the employee’s account, replacing the registered phone number with an unauthorized one. This modification enabled the threat actor to obtain unauthorized remote access to a single employee’s payroll application where they changed direct deposit payroll information to their own account.

Upon investigation, we discovered that the incident began during the evening of September 20, 2024. The unauthorized activity ceased in the early hours of September 21, 2024, and the unauthorized phone number was removed from the employee’s account on September 24, 2024. However, unauthorized paycheck redirections associated with the incident were not discovered and interrupted until November 3, 2024.

The personal information that may have been impacted for the Maryland resident includes full name and financial information, specifically payroll and compensation details stored within the individual’s personnel account. There was no compromise of the greater personnel or payroll systems and Seyfarth has no indication that this information has been further disclosed or misused.

Upon discovering the unauthorized access, Seyfarth took swift action to secure its systems and prevent further unauthorized activity. The unauthorized multi-factor settings were promptly corrected, and Seyfarth’s IT team began a comprehensive investigation to assess the extent of the incident. Seyfarth has implemented additional safeguards to prevent similar incidents in the future, including enhanced personnel training, improved multi-factor authentication protocols, and tighter controls on access permissions within the remote access environment. Additionally, Seyfarth has conducted a thorough review of the affected employee account and alerted other employees to be vigilant against potential impersonation tactics.

As part of our response, we also filed a report with the Internet Crime Complaint Center (IC3) to engage law enforcement in addressing this incident and to support further investigation into the threat actor's activities.

Notice to Maryland Residents: We have determined that the number of Maryland residents potentially affected by this security incident is one (1). Seyfarth mailed notice to the impacted individual on November 8, 2024. Written notice to individual was provided in substantially the same form as the letter attached to this email submission.

Other Steps Taken and To Be Taken: Seyfarth is taking action to provide assistance to the affected individual. Seyfarth is providing the individual whose personal information was affected by this incident with access to credit monitoring services for 12 months through Experian at no cost to the individual.

Additionally, Seyfarth is providing the impacted individual with guidance on how to guard himself against identity theft and fraud. These measures include advising the individual to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Seyfarth is also providing the individual with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, 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 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 incident, please contact the undersigned at (404) 885-1500 or jpriebe@seyfarth.com.

Very truly yours,

SEYFARTH SHAW LLP

/s/ Jason Priebe

Jason Priebe
Chief Privacy Officer and Associate General Counsel

JP:DR



Seyfarth Shaw LLP
1075 Peachtree Street, N.E.
Suite 2500
Atlanta, Georgia 30309-3958
T (404) 885-1500
F F (404) 892-7056

jpriebe@seyfarth.com
T T (404) 885-6773

www.seyfarth.com

November 8, 2024

[Name]
[Address]

RE: Important Information Regarding Security Event.

Dear [Name]:

We are writing to provide information and notification concerning an incident involving your personal information.

What Happened: On September 20, an unauthorized individual contacted the Seyfarth Service Desk (“service desk”) impersonating you. The caller claimed to have a new phone and, as a result of a temporary lapse in verification protocols, was granted access to the Seyfarth internal employee portal. Once access was gained, the unauthorized individual accessed your payroll information through the ADP system and successfully rerouted compensation bank account information.

After Seyfarth became aware of the incident, the Technology Service Group blocked the unauthorized individual from further access and secured your user account. We have since conducted a full review of our security protocols and implemented additional measures to prevent this from happening in the future. We have notified law enforcement regarding this incident.

What Information Was Involved: We have investigated the incident and have identified the following categories of your personal information that were made visible to the other individual for a brief period of time:

- Full Name
- Financial Account Numbers
- Address
- Date of Birth

We regret that this incident occurred and take the security of our information very seriously. Our service desk team recently conducted a training session across a variety of information security topics, including document delivery validation and verification.

What You Can Do: While we have no reason to believe there will be further attempted improper use or disclosure of your personal information with any bad actors, we encourage you to remain vigilant by reviewing your account statements and monitoring credit report information. You can also obtain

information about fraud alerts and security freezes from the FTC and the credit reporting agencies listed below:

- Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP
- Nationwide Consumer Reporting Companies:
 - Equifax, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
 - Experian, <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
 - TransUnion, <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289
- Maryland Office of the Attorney General (OAG), <https://www.marylandattorneygeneral.gov>, 200 St. Paul Place, Baltimore, MD 21202, Toll-Free: 1-888-743-0023

To the extent you desire to freeze your credit report, you must separately place a credit freeze on your credit file at each of the three credit reporting agencies. There is no charge associated with placing a credit freeze. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

What we are doing to protect your information: To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: [DATE]** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll:
<https://www.experianidworks.com/3bcredit> [[experianidworks.com](https://www.experianidworks.com)]
- Provide your **activation code: ABCDEFGH**

If you have questions about the product, need assistance with identity restoration for your minor that arose as a result of this incident, please contact Experian's customer care team at (833) 931-7577 by **January 31, 2025**. Be prepared to provide engagement number **B098470** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING THE 12-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 for your minor:

- **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 specialist are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (833) 931-7577. 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 (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 this Identity Restoration support is available to you for 12 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. You will also find self-help tips and information about identity protection at this site.

For More Information: Please contact us if you have questions or require additional information about the incident.

Email: dataprotection@seyfarth.com
Phone: (833) 931-7577

Sincerely,

SEYFARTH SHAW LLP

/s/ Jason Priebe

Jason Priebe
Chief Privacy Officer and Associate GC

DER