
Pursuant to MD law, I am providing notice of a security breach potentially affecting Maryland residents:

Brief description of the nature of the security breach:

On or about September 21, 2023, Shift5, Inc. learned that a single O365 account on Shift5's network had been compromised on or around September 11, 2023, through a phishing scheme.

Number of Maryland residents being notified: 14

Sample copy of the notice being sent: Please see attached

Information which may have been compromised: Name and Social Security Number

Steps the business is taking to restore the integrity of the system:

In addition to containing and remediating the intrusion, Shift5 has enhanced its monitoring capabilities to increase the likelihood of promptly detecting similar incidents in the future. Concurrently, we are working on implementing third-party surveillance across all corporate systems in order to obtain correlational analysis and ensure round-the-clock monitoring. Furthermore, a comprehensive audit of recent system accesses has been conducted, enabling the company to ascertain with a high degree of confidence that the cyber-attack in question was an isolated event. There is no evidence to suggest that the same method of unauthorized entry has been employed against additional accounts in conjunction with the issue we are reporting. As an additional measure of protection, we are offering a **complimentary** 24-month membership of Experian's® IdentityWorksSM.

Ellen McDonald

General Counsel

ellen@shift5.io

510-501-9718



CONFIDENTIALITY NOTICE: This e-mail (and any attachments) may be confidential and proprietary. It is for the sole use of the intended recipient(s) and any use or disclosure by others is prohibited. If you are not the intended recipient(s), please notify the sender by return e-mail and delete all copies of this e-mail (and any attachments).

October __, 2023

Dear [NAME],

NOTICE OF DATA BREACH

Shift5, Inc. (“Shift5,” “we” and “us”) is writing to notify you of an issue that involves your personal data. As your employer or former employer, we receive and handle information that may include personal data in certain instances. Although we have no indication of identity theft or fraud in relation to this event, we are providing you with information about the event, our response, and additional measures you can take to help protect your personal information from identity theft, phishing and other potential misuse.

WHAT HAPPENED

On or about September 21, 2023, we learned that a single O365 account on Shift5’s network had been compromised on or around September 11, 2023, through a phishing scheme. Upon becoming aware of the issue, we promptly took steps to secure our systems and launched an investigation.

WHAT INFORMATION WAS INVOLVED

Certain limited files within the O365 environment may have been compromised through this security vulnerability. One of these files contains your personal data. The personal data in the relevant files were your first name or first initial and last name and social security number.

WHAT WE ARE DOING

Shift5 takes this event and the security of information in our care seriously. In addition to containing and remediating the intrusion, Shift5 has enhanced its monitoring capabilities to increase the likelihood of promptly detecting similar incidents in the future. Concurrently, we are working on implementing third-party surveillance across all corporate systems in order to obtain correlational analysis and ensure round-the-clock monitoring. Furthermore, a comprehensive audit of recent system accesses has been conducted, enabling the company to ascertain with a high degree of confidence that the cyber-attack in question was an isolated event. There is no evidence to suggest that the same method of unauthorized entry has been employed against additional accounts in conjunction with the issue we are reporting.

As an additional measure of protection, we are offering a **complimentary** 24-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:** [enrollment end date] (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [URL]
- Provide your **activation code:** [code]

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian’s customer care team at [customer service number] by [enrollment end date]. Be prepared to provide engagement number [engagement #] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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.
- **Identity Restoration:** Identity Restoration specialists 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 [\[customer service number\]](#). 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 24 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.

WHAT YOU CAN DO

Over the next 12 to 24 months, we recommend you remain alert for any unsolicited communications regarding your personal data and review your account statements and credit reports for suspicious activity. You should promptly notify your financial institution of any unauthorized transactions or suspected identity theft. We also recommend that you enroll in the complimentary Credit Monitoring Service offered by Shift5. Finally, please review the “Additional Resources” section included with this letter below. This section describes additional steps you can take to help protect your information, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

MORE INFORMATION

Should you have any questions regarding this incident, please contact Shift5 at 703-810-3320 (ask for the General Counsel) or legal@shift5.io to assist you during this process.

We regret any inconvenience this issue may cause you.

Shift5, Inc.

ADDITIONAL RESOURCES

Order Your Free Credit Report: To order your free annual credit report, visit www.annualcreditreport.com, call toll-free at (877) 322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's (FTC) website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. The three credit bureaus (Equifax, Experian, and TransUnion) provide free annual credit reports only through the website, toll-free number, or request form.

Depending upon your state you may also obtain one or more additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies listed below directly to obtain such additional report(s). You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax www.equifax.com	(800) 685-1111
Experian www.experian.com	(888) 397-3742
TransUnion www.transunion.com	(800) 916-8800

Upon receiving your credit report, review it carefully. Errors may be a warning sign of possible identity theft. Here are a few tips of what to look for:

- Look for accounts you did not open.
- Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case.
- Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security Number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

We encourage you to take advantage of these protections and remain vigilant for incidents of fraud and identity theft, including regularly reviewing and monitoring your credit reports and account statements.

Federal Trade Commission and State Attorneys General Offices: If you detect any unauthorized transactions in any of your financial accounts, promptly notify the appropriate payment card company or financial institution. If you detect any incidence of identity theft or fraud, promptly report the matter to your local law enforcement authorities (from whom you can obtain a police report), state Attorney General, and the Federal Trade Commission (FTC). You can contact the FTC to learn more about how to protect yourself from becoming a victim of identity theft by using the contact information below:

Federal Trade Commission Bureau of Consumer Protection
600 Pennsylvania Avenue NW Washington, DC 20580
(877) IDTHEFT (438-4338)
www.ftc.gov/idtheft and www.identitytheft.gov

For District of Columbia residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; 202-727-3400; and oag.dc.gov.

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 Oregon residents: The Attorney General may be contacted at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; (877) 877-9392; www.doj.state.or.us.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report:

For Massachusetts residents: Under Massachusetts law, you have the right to obtain any police report filed in connection with the incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Placing a Fraud Alert or Security Freeze

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 one-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