



April 26, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Sent via email – ldtheft@oag.state.md.us

**Re: Notification of a Potential Breach of Security Involving Ten (10)
Maryland Residents**

Dear Attorney General Brown,

I am writing on behalf of Massachusetts Mutual Life Insurance Company ("MassMutual") to inform you of a security related matter that may have involved the personal information of ten (10) Maryland residents.

At 11:39 AM EDT on February 2, 2023, MassMutual's Security Operations Center received an internal report that an unknown threat actor had called MassMutual's Information Technology Service Center and impersonated an employee of an independent MassMutual agency (the "agency employee"). This resulted in a successful change of the agency employee's Okta password.

Upon further review, the threat actor called MassMutual's Information Technology Service Center twice on February 1, 2023, impersonating the agency employee and speaking to a different representative on each call. The threat actor had the name and last four digits of the agency employee's Social Security number and requested a password reset. The threat actor also claimed they forgot their username and was provided with the username of the agency employee. On the subsequent call, the threat actor successfully provided the last four digits of the agency employee's social security number and username and requested a reset of the existing multi-factor authentication.

Later the same day, the agency employee contacted MassMutual's Information Technology Service center and reported not being able to log in to their user account. As part of that call, the Okta password and multi-factor authentication method were again reset, and any open Okta sessions were terminated. As a result of this action, the threat actor could no longer use the credentials nor access any MassMutual resources.



The window of exposure was approximately 3 hours and 50 minutes, on February 1, 2023, between 9:54 AM EDT and 1:44 PM EDT.

Upon review of the impacted systems (limited to Microsoft Exchange, OneDrive/SharePoint, and one proprietary system) the company developed a listing of data elements contained in the files.

Ten (10) Maryland residents' information were included in this incident. The information contained in the impacted systems include the Maryland residents' names, account numbers, Social Security Numbers, and Medical Information.

While we have no indication that the information has been or will be subject to misuse or further disclosure, MassMutual is providing the impacted individuals a free, 24-month subscription to IdentityForce. The credit monitoring services offered are consistent with the requirements of Maryland law.

Attached, please find a copy of the redacted notification letter to be provided to the impacted individuals.

MassMutual took several preventative measures to combat future incidents, including clarifying procedures, providing team training on the topic, and implementing a control enhancement regarding performing both a password reset and Okta Multifactor reset within a certain period of time. Further, as the Technology Service Center employee failed to follow established processes, that employee was terminated.

If you have any questions regarding this matter, please do not hesitate to call me at (413) 744-5002.

Sincerely,

A handwritten signature in black ink, appearing to read "LW", with a stylized flourish at the end.

Lisa Walkuski
Compliance Consultant
MassMutual Compliance & Ethics Department

Encl.



April 27, 2023

Re: Notification Regarding Your Personal Information

Dear :

We are notifying you on behalf of Massachusetts Mutual Life Insurance Company ("MassMutual") to let you know of an issue we believe may have involved the exposure of some of your personal information.

What happened: On February 2, 2023 MassMutual was made aware of an incident involving unauthorized access to an independent MassMutual agency employee's online account for a short period of time on February 1, 2023.

MassMutual immediately took steps to secure the agency employee's account and launched an investigation to determine the full nature and scope of the incident. We subsequently performed an assessment of the Microsoft Outlook mailbox and other impacted systems and determined that some of the emails and files contained certain personal information. Although we have no evidence that the threat actor misused your personal information, we are notifying you of this incident out of an abundance of caution.

What information was involved: From the investigation, we have determined that the personal information that may have been affected includes your . Again, at this time, we are not aware of any malicious or fraudulent activity relating to anyone's personal information as a result of this incident.

What we are doing and what you can do: While we have no indication that your information has been or will be subject to misuse, as an added precaution, we have arranged to have IdentityForce protect your identity for 24 months at no cost to you.

IdentityForce's Rapid Response product provides you with identity theft protection and resolution services, including credit report monitoring, identity monitoring, lost wallet coverage, fully managed restoration and recovery services, and identity theft insurance. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you enroll within 90 days of this letter
- Visit the IdentityForce website to enroll: <https://secure.identityforce.com/benefit/massmutual>
- Provide your verification code: 

If you have questions about the product, need assistance with services, or would like an alternative to enrolling online, please contact IdentityForce's Member Services team at 1-877-694-3367.

For more information: Attached to this letter is additional information for your review.

We apologize for any inconvenience that this incident may have caused you. If you have any questions regarding this matter, please contact 1-844-950-4676.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

If you believe you are the victim of identity theft or any of your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps to avoid identity theft and to place fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. You should obtain a copy of the police report in case you are asked to provide it to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW,
Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Credit Freeze: Under the Economic Growth, Regulatory Relief, and Consumer Protection Act of 2018 (Public Law No. 115-174), as of September 21, 2018, you have the right to put a credit freeze on your credit file free of charge. A credit freeze is designed to prevent a credit reporting company from releasing your credit report without your consent. If you place a credit freeze on your credit file, no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate the freeze. In addition, potential creditors and other third parties will not be able to access to your credit report unless you lift the freeze. Therefore, a credit freeze may delay your ability to obtain credit. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting agency. You can obtain more information about fraud alerts and credit freezes by contacting the Federal Trade Commission or one of the national credit reporting agencies listed above.

If you are a resident of Iowa, you are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General. Iowa Office of the Attorney General, Consumer Protection Division, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319, 1-888-777-4590, consumer@ag.iowa.gov.

If you are a resident of Maryland, you may contact the Maryland Attorney General's Office at 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to obtain a copy of any police report. Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19022-2000, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

If you are a resident of North Carolina, you may contact the North Carolina Attorney General's Office at 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-919-716-6400.

If you are a resident of Oregon, you are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Office of the Attorney General: Oregon Office of the Attorney General, Consumer Protection Division, 1162 Court St. NE, Salem, OR 97301-4096, 1-877-877-9392, www.doj.state.or.us.

If you are a resident of Rhode Island, note that pursuant to Rhode Island law, you have the right to file or obtain a police report. If you request a security freeze, as of September 1, 2018, Rhode Island law prohibits consumer reporting agencies from charging a fee for a security freeze service. Please refer to the Credit Freeze section above for directions on requesting a security freeze. You may also obtain information about identity theft prevention from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, (401) 274-4400, consumers@riag.ri.gov.

If you are a resident of West Virginia, you also have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to

obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax, PO Box 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 9554, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-680-7289

As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.ftc.gov/idtheft/.

You may also obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a security freeze on your credit report pursuant to West Virginia law. The security freeze will prohibit a consumer reporting agency from releasing any information in your credit report without your express authorization or approval.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five business days you will be provided a unique personal identification number ("PIN") or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the distribution of your credit report for a period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

- (1) The unique personal identification number ("PIN") or password provided by the consumer reporting agency;
- (2) Proper identification to verify your identity; and
- (3) The period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three business days after receiving the request.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.