



April 26, 2024

VIA EMAIL – ldtheft@oag.state.md.us

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

Re: Notification of a Potential Breach of Security Involving Eighteen (18) Maryland residents

To Whom It May Concern:

Massachusetts Mutual Life Insurance Company ("MassMutual") is informing you of a security related matter that involved the personal information of eighteen (18) Maryland residents.

On February 15, 2024, Enroll Confidently, Inc. ("Enroll Confidently"), a third-party enrollment platform provider, notified MassMutual that it experienced an attempted ransomware attack on February 13, 2024. Enroll Confidently advised MassMutual that at that time there was no evidence of any impact to MassMutual confidential information.

Enroll Confidently maintains a cloud-based benefit administration platform ("the Platform") that permits employers to offer benefits to their employees. MassMutual utilize the Platform to offer its group whole life insurance product to employees of those employers that have selected the MassMutual product as a benefit offering. Employees who seek to obtain the product enroll in the benefit offering via the Platform.

On March 4, 2024, Enroll Confidently informed MassMutual that MassMutual confidential information, including personal information, was present on Enroll Confidently's servers impacted by this event. Enroll Confidently engaged a third-party forensic provider to conduct an analysis and confirmed on April 2, 2024, that certain MassMutual confidential information, to include personal information of those individuals who sought to obtain the MassMutual product offering on the Platform was subject to unauthorized access and acquisition. That forensic provider is continuing to perform data discovery, which is not yet complete. MassMutual was able, however, to use its own data to determine impacted individuals relating to its



business. Accordingly, on April 16, 2024, MassMutual determined that eighteen (18) Maryland residents had been impacted.

The personal information involved in this matter includes the individuals' first and last name, Social Security number, address, date of birth and, in some cases, medical information. At this time, MassMutual does not have evidence of any misuse or subsequent disclosure of MassMutual confidential information because Enroll Confidently indicated that their forensic firm engaged with the threat actor and received assurances that the information acquired would be deleted. Notwithstanding, MassMutual is requiring Enroll to notify all individuals associated with MassMutual whose personal information was impacted by this event.

The notification to all of the impacted individuals associated with MassMutual to be fulfilled by Enroll Confidently will include a free, 24-month subscription to Experian IdentityForce. Attached, please find the template notification letters to be provided to the impacted individuals.

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



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

April 26, 2024

L2322-L01-0000001 T00001 P001 *****SCH 5-DIGIT 12345

SAMPLE A SAMPLE - L01 INDIVIDUAL

APT ABC

123 ANY STREET

ANYTOWN, FC 1A2 B3C

COUNTRY



RE: Notice of Data [Extra1]

Dear Sample A. Sample:

Enroll Confidently is writing to make you aware of a recent incident that may affect your personal information. Enroll Confidently provides a benefits enrollment platform to support employers and benefits providers throughout the employee enrollment process. Employees who seek to obtain an employer-sponsored product enroll in the benefit offering via the Platform. We have your information because we provide these services to Massachusetts Mutual Life Insurance Company (“MassMutual”). MassMutual utilizes the Platform to offer its group whole life insurance product to employees of those employers that have selected the MassMutual product as a benefit offering. This notice includes information about the incident, steps we have taken in response, and resources available to help you protect your information, should you feel it is appropriate to do so.

What Happened? On February 13, 2024, we became aware of unusual system activity within our network. We promptly took steps to secure our systems and began a comprehensive investigation to determine what happened and what information may be affected. Through this investigation, we learned that an unauthorized actor gained access to our network on February 13, 2024, and copied certain files from the system as part of a cybersecurity event. We are undertaking a detailed review of the relevant files to confirm what information is present and to whom it relates. Through that review, we recently determined that your information was present in the relevant files.

What Information Was Involved? Our investigation determined that your [Extra2] were affected by this incident.

What We Are Doing. We take our responsibility to safeguard the data entrusted to us very seriously. We responded promptly to this incident and have been working diligently to conduct a thorough investigation. We are also working to enhance our existing security measures to further protect our systems moving forward. Additionally, we have notified federal law enforcement of this incident.

As an added precaution, we are providing you with access to 24 months of complimentary credit monitoring services through Experian. Information on how to enroll in these services is provided in the attached **More Information On Ways To Protect Yourself**. This section also includes guidance on resources available to you to protect personal information against potential misuse.

0000001



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 errors. We also encourage you to review the attached ***More Information On Ways To Protect Yourself*** and enroll in the credit monitoring services we are offering. Please note, we are not permitted to enroll you in these services and so you will need to follow the instructions included below to enroll.

For More Information. If you have questions that are not addressed by this letter, please contact our dedicated assistance line at 833-931-7500 Monday through Friday from 8am to 8pm Central Time. Be prepared to provide engagement number B121453. You may also write to Enroll Confidently at P.O. Box 25880, Scottsdale, AZ 85255.

Sincerely,

Enroll Confidently

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

Enroll in Monitoring Services

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) 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 twenty-four (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.

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 twenty-four (24)-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** August 30, 2024 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/credit>
- 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 833-931-7500 by August 30, 2024. Be prepared to provide engagement number B121453 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 file for indicators of fraud.
- **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.



Review Your Account Statements: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. 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 the District of Columbia, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, you should immediately contact the District of Columbia Attorney General at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

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, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, you should immediately contact the Maryland Attorney General at Office of Attorney, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

If you are a resident of New Mexico, you have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

If you are a resident of New York, the Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-(800)-771-7755; or www.ag.ny.gov.

If you are a resident of North Carolina, and you either believe you are the victim of identity theft or need to obtain information on the steps to take to avoid identify theft, 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 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.