



March 21, 2024

Attorney General's Office
700 W. Jefferson Street
P. O. Box 83720
Boise, ID 83720-0010

Sent via email – consumer_protection@ag.idaho.gov

Re: Notification of a Potential Breach of Security Involving Thirty-Nine (39) Idaho Residents

To Whom It May Concern:

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 thirty-nine (39) Idaho residents.

Newport Group, Inc. ("Newport") serves as a third-party recordkeeper for non-qualified deferred compensation plans sponsored by MassMutual for its eligible employees, agents, and independent contractors.

On November 6, 2023, Newport Group, Inc. ("Newport") notified MassMutual that their provider, Infosys McCamish Systems ("IMS"), experienced a ransomware event on November 2, 2023. Newport advised MassMutual that at that time there was no evidence of data exfiltration or exposure. Newport provided MassMutual with several updates indicating that the investigation was ongoing and that there was no evidence of data exfiltration or exposure.

On January 12, 2024, Newport advised MassMutual that some Newport-related data was impacted by this incident and that their investigation, including a forensic analysis, was unable to provide with certainty what information may have been accessed or acquired.

Based on the information received, including the results of the forensic analysis, on February 5, 2024, MassMutual determined it was reasonable to conclude that the threat actors obtained unauthorized access to personal information of individuals associated with the plans or their beneficiaries. Upon conducting a review of the data Newport provided IMS, the information associated with the impacted individuals includes, first and last name, Social Security number and in some cases, address, and date of birth. We do not have any evidence at this time of any misuse or subsequent disclosure of MassMutual data.



Newport will notify all impacted individuals associated with these plans, which 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", written in a cursive style.

Lisa Walkuski
Compliance Consultant
MassMutual Compliance & Ethics Department

SAMPLE A. SAMPLE - L28

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789

March 22, 2024

Reference: Security Incident & Complimentary Identity Protection Package

Newport Group, Inc. (“Newport” or “We”) serves as a third-party recordkeeper for non-qualified deferred compensation plans sponsored by Massachusetts Mutual Life Insurance Company (“MassMutual”) for its eligible employees, agents and independent contractors. You are receiving this notice because you are or were eligible to participate in a MassMutual non-qualified retirement plan, or are or were a named beneficiary of a plan participant.

We are writing to notify you of a security incident described in more detail below. As a result of this incident, we are offering you a complimentary two-year identity protection package through Experian, called IdentityWorks. The relevant details of the incident, and how to enroll with IdentityWorks, are summarized below:

<p>What Happened?</p>	<p>On November 2, 2023, Infosys McCamish Systems ("IMS"), a provider that we use to process transactions for your plan, became aware of a ransomware event. Upon learning of the event, IMS engaged a leading third-party security expert, Unit 42, part of Palo Alto Networks, to validate the scope of the incident and handle remediation.</p> <p>IMS subsequently successfully restored and rebuilt its environment. In addition, Unit 42 validated that the IMS environment has been hardened and they have observed no indication of ongoing unauthorized access or activity. After confirming it was safe to do so, we reconnected to the IMS system and resumed normal processing for your plan.</p> <p>IMS engaged a leading e-discovery firm, EY, to determine what data of any of the plans or participants that we service was present on the system at the time of the incident and potentially subject to unauthorized access. IMS informed us that some Newport data was present on their system at the time of the event, however:</p> <ul style="list-style-type: none">• While there was evidence of unauthorized access to IMS systems observed by the third-party security expert, at this time IMS does not have any indication that personal information was subject to misuse or further disclosure.• The review by EY of accounts and systems to identify what personal information was present at the time of the attack is ongoing.
<p>What information was involved?</p>	<p>According to our records, we have provided IMS with names, addresses, dates of birth and Social Security numbers of individuals eligible to participate in the Plans.</p> <p>We have provided IMS with names, Social Security numbers, and in some cases, dates of birth of named beneficiaries under the Plans.</p>

What We Are Doing?	We will continue to be in close contact with IMS and will provide an update if we have additional relevant information. Although there is no evidence that your personal information has been subject to misuse or further disclosure, Newport is offering you a two-year identity protection package from IdentityWorks at no cost to you.
What You Can Do?	<p>IdentityWorks helps detect possible misuse of personal information and provides you with identity protection support focused on immediate identification and resolution of identity theft¹. Please note that this offer is available to you for two years from the date of this letter and requires an action on your part.</p> <p>Additional information, terms of this service, self-help tips, and information about identity protection are located at www.ExperianIDWorks.com/restoration.</p> <ol style="list-style-type: none"> 1. To start monitoring your personal information please follow the steps below: 2. Ensure that you enroll by: June 30, 2024 3. Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit 4. Provide your activation code: ABCDEFGHI <p>If you have questions about Experian or IdentityWorks, or if you would like an alternative to enrolling in IdentityWorks online, please contact Experian’s customer care team at 1-877-890-9332. As proof of eligibility for this service, you will need to provide the engagement number – B118258.</p>
For More Information	If you have any questions about Newport, IMS, or this event, please contact 800-230-3950. We are available to assist you Monday – Friday, 8:00 am - 8:00 pm EST.

We apologize for the inconvenience and any concern this incident may have caused you.

¹ If you are not located in the United States, the terms of this service may be different. You can call the Experian number above for more information.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

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.

Return Mail Processing
PO Box 999
Suwanee, GA 30024

51 1 11904 *****SNGLP

To the Parents/Guardians of
SAMPLE A. SAMPLE - L24
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



March 22, 2024

Reference: Security Incident & Complimentary Identity Protection Package

Newport Group, Inc. (“Newport” or “We”) serves as a third-party recordkeeper for non-qualified deferred compensation plans sponsored by Massachusetts Mutual Life Insurance Company (“MassMutual”) for its eligible employees, agents and independent contractors. You are receiving this notice because you are or were eligible to participate in a MassMutual non-qualified retirement plan, or are or were a named beneficiary of a plan participant.

We are writing to notify you of a security incident described in more detail below. As a result of this incident, we are offering you a complimentary two-year identity protection package through Experian, called IdentityWorks. The relevant details of the incident, and how to enroll with IdentityWorks, are summarized below:

What Happened?	<p>On November 2, 2023, Infosys McCamish Systems ("IMS"), a provider that we use to process transactions for your plan, became aware of a ransomware event. Upon learning of the event, IMS engaged a leading third-party security expert, Unit 42, part of Palo Alto Networks, to validate the scope of the incident and handle remediation.</p> <p>IMS subsequently successfully restored and rebuilt its environment. In addition, Unit 42 validated that the IMS environment has been hardened and they have observed no indication of ongoing unauthorized access or activity. After confirming it was safe to do so, we reconnected to the IMS system and resumed normal processing for your plan.</p> <p>IMS engaged a leading e-discovery firm, EY, to determine what data of any of the plans or participants that we service was present on the system at the time of the incident and potentially subject to unauthorized access. IMS informed us that some Newport data was present on their system at the time of the event, however:</p> <ul style="list-style-type: none">• While there was evidence of unauthorized access to IMS systems observed by the third-party security expert, at this time IMS does not have any indication that personal information was subject to misuse or further disclosure.• The review by EY of accounts and systems to identify what personal information was present at the time of the attack is ongoing.
----------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

What information was involved?	<p>According to our records, we have provided IMS with names, addresses, dates of birth and Social Security numbers of individuals eligible to participate in the Plans.</p> <p>We have provided IMS with names, Social Security numbers, and in some cases, dates of birth of named beneficiaries under the Plans.</p>
What We Are Doing?	<p>We will continue to be in close contact with IMS and will provide an update if we have additional relevant information. Although there is no evidence that your personal information has been subject to misuse or further disclosure, Newport is offering you a two-year identity protection package from IdentityWorks at no cost to you.</p>
What You Can Do?	<p>To help protect your minor dependent’s identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months.</p> <p>If you believe there was fraudulent use of your minor dependent’s 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).</p> <p>Please note that Identity Restoration 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.</p> <p>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 24 month membership. This product provides you with identity detection and resolution of identity theft. To start monitoring your minor dependent’s personal information, please follow the steps below:</p> <ul style="list-style-type: none"> • Ensure that you enroll by: June 30, 2024 • Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/minorplus • Provide your activation code: ABCDEFGHI • Provide your minor’s information when prompted <p>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 1-877-890-9332 by June 30, 2024. Be prepared to provide engagement number B118276 as proof of eligibility for the Identity Restoration services by Experian.</p>
For More Information	<p>If you have any questions about Newport, IMS, or this event, please contact 800-230-3950. We are available to assist you Monday – Friday, 8:00 am - 8:00 pm EST.</p>

We apologize for the inconvenience and any concern this incident may have caused you.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

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.

