NORTON ROSE FULBRIGHT

January 24, 2025

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

Via Email: *idtheft@oag.state.md.us*

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: ***Supplemental Legal Notice of Security Incident***

Dear Sir or Madam:

I am writing on behalf of our client, Stryker Corporation ("Stryker"), to supplement Stryker's data security incident notification submissions to your office on October 30, 2024 and December 4, 2024. As stated in our initial notice, we have finished our review of the data and have reached out to Stryker customers who have data subjects impacted by the incident. This supplemental notice includes additional data subjects from customers who have responded to Stryker and provided addresses and those individuals are Maryland residents.

On January 24, 2025, Stryker sent a notification letter via First Class Mail to the 1 additional Maryland resident whose personal information was involved (for a new total of 41). A copy of the representative example(s) of the individual notice letter is attached. Stryker's review of the exfiltrated data to identify individuals who had personal information in the data set is now substantially complete; however, we are continuing to work with our impacted customers to confirm contact information for their impacted individuals. We may provide supplemental notice if the total number of impacted residents changes.

Stryker is offering 24-months of complimentary credit monitoring and fraud protection services to all Maryland residents receiving notice, regardless of the data elements impacted, and is providing a toll-free hotline for individuals to call with any questions regarding the incident.

We are also writing to provide a list with the customer who has directed Stryker to provide notice to your office on their behalf. A list with the customer who authorized us to provide their name to your office is enclosed at Appendix A.

The information being provided with this submission, and any potential supplemental submissions, constitutes proprietary and confidential information that is exempt from disclosure under the Freedom of Information Act and Maryland's Public Information Act (collectively, "FOIA"). Stryker designates this response and information therein, and any potential supplemental responses and information, as confidential commercial information protected from disclosure by, among other exemptions, the exemptions contained in Maryland's Public Information Act, MD General Provisions Code § 4-335 (2023). In the event that a FOIA request is received pursuant to which this letter could be deemed responsive, we request that we be furnished with a copy of all written materials pertaining to such request and be given a reasonable opportunity to respond prior to any determination that this response and any of the information herein will be produced.

The foregoing request for confidentiality under FOIA is without prejudice to any other rights, objections, or arguments that Stryker may have with respect to the confidential nature, and any production to third parties of this response.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

David Kessler

David Kessler

Appendix A

1	West Virginia University Health System	Tina Williams tina.williams1@wvumedicine.org 844-988-6446

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

December 4, 2024

Via Email: *idtheft@oag.state.md.us*

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Re: ***Supplemental Legal Notice of Security Incident***

Dear Sir or Madam:

I am writing on behalf of our client, Stryker Corporation ("Stryker"), to supplement Stryker's data security incident notification submission to your office on October 30, 2024. As stated in our initial notice, we have finished our review of the data and have reached out to Stryker customers who have data subjects impacted by the incident. This supplemental notice includes additional data subjects from customers who have responded to Stryker and provided addresses and those individuals are Maryland residents.

On November 26, 2024, Stryker sent notification letters via First Class Mail to the additional 28 Maryland residents whose personal information was involved (for a new total of 40). A copy of the representative example(s) of the individual notice letter is attached. Stryker's review of the exfiltrated data to identify individuals who had personal information in the data set is now substantially complete; however, we are continuing to work with our impacted customers to confirm contact information for their impacted individuals. We may provide supplemental notice if the total number of impacted residents changes.

Stryker is offering 24-months of complimentary credit monitoring and fraud protection services to all Maryland residents receiving notice, regardless of the data elements impacted, and is providing a toll-free hotline for individuals to call with any questions regarding the incident.

We are also writing to provide a list with the customer who has directed Stryker to provide notice to your office on their behalf. A list of the customer who authorized us to provide their name to your office is enclosed at Appendix A.

The information being provided with this submission, and any potential supplemental submissions, constitutes proprietary and confidential information that is exempt from disclosure under the Freedom of Information Act and Maryland's Public Information Act (collectively, "FOIA"). Stryker designates this response and information therein, and any potential supplemental responses and information, as confidential commercial information protected from disclosure by, among other exemptions, the exemptions contained in Maryland's Public Information Act, MD General Provisions Code § 4-335 (2023). In the event that a FOIA request is received pursuant to which this letter could be deemed responsive, we request that we be furnished with a copy of all written materials pertaining to such request and be given a reasonable opportunity to respond prior to any determination that this response and any of the information herein will be produced.

The foregoing request for confidentiality under FOIA is without prejudice to any other rights, objections, or arguments that Stryker may have with respect to the confidential nature, and any production to third parties of this response.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

David Kessler

David Kessler

Appendix A

1	LifeBridge Health, Inc.	Darlene A Skinner daskinne@lifebridgehealth.org 401-601-0973
2	University of Utah Health	Jamie Ross, Information Privacy Office privacy@utah.edu 801-587-9241
3	Mercy Health Services	Gregory Lederman glederman@mullen.law 267-930-4637

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

November 26, 2024

M4460-L04-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Security Incident

Dear Sample A. Sample,

Stryker Corporation ("Stryker") is a medical technology company, headquartered in the U.S. and specializing in medical and surgical, neurotechnology, orthopedics and spine products and services. In the course of its work, Stryker is provided access to certain personal information to perform services for its customers in the medical and healthcare industries.

We are writing to inform you that we experienced a cybersecurity incident that involved some of your personal information. Stryker was in possession of this information due to its work with [Extra1]. This notice explains the incident, steps we have taken in response, and additional information on steps you may take to help protect your information.

What happened

On Monday, June 10, 2024, Stryker discovered unauthorized activity in a limited portion of its environment. Stryker immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Stryker also notified law enforcement and swiftly contained the incident.

The investigation determined that the unauthorized third party gained access to certain Stryker internal systems at various times between approximately May 14, 2024, and June 10, 2024, and obtained some data from Stryker systems. A thorough review of the impacted data was conducted to identify what information was involved and identify individuals to whom the data related.

Importantly, this incident was limited to Stryker's corporate environment and did not impact the functioning of any of Stryker's products.

What information was involved

The review determined that the data involved contained some of your personal information, including your name, and one or more of the following: [Extra2].

What we are doing

To help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to enhance the security of our network, internal systems and applications. Stryker will also continue to evaluate additional steps that may be taken to further increase our defenses. In addition, we are continuing to support federal law enforcement's investigation.

stryker

What you can do

While we are not aware of any evidence that your personal information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant of your information and, as a precaution, **Stryker is offering you complimentary access to Experian IdentityWorks^{SM} for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian is completely free to you and enrolling in this program will not hurt your credit score.

For more information on Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary 24-month membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For more information

Stryker takes the security of your personal information seriously, and sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call 833-918-9002, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time. If you have a speech or hearing impairment and use a TTY to call 711.

Sincerely,

Stryker

stryker

Experian IdentityWorks℠ Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 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 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 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** March 31, 2025 (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 833-918-9002 by March 31, 2025 (5:59 UTC). Be prepared to provide engagement number B135707 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 ExtendCARE™:** 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.

stryker

Information About Identity Theft Protection Guide

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: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

> **For New Mexico residents:** You may 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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For New York residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

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.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. Three Rhode Island residents were impacted by this incident.

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

November 26, 2024

M4460-L06-0000003 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L06 ADULT CUSTOMER NAME EXCLUDED
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Security Incident

Dear Sample A. Sample,

Stryker Corporation ("Stryker") is a medical technology company, headquartered in the U.S. and specializing in medical and surgical, neurotechnology, orthopedics and spine products and services. In the course of its work, Stryker is provided access to certain personal information to perform services for its customers in the medical and healthcare industries.

We are writing to inform you that we experienced a cybersecurity incident that involved some of your personal information. Stryker was in possession of this information due to its work related to joint replacement procedures or treatments performed by one of Stryker's healthcare customers. This notice explains the incident, steps we have taken in response, and additional information on steps you may take to help protect your information.

What happened

On Monday, June 10, 2024, Stryker discovered unauthorized activity in a limited portion of its environment. Stryker immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Stryker also notified law enforcement and swiftly contained the incident.

The investigation determined that the unauthorized third party gained access to certain Stryker internal systems at various times between approximately May 14, 2024, and June 10, 2024, and obtained some data from Stryker systems. A thorough review of the impacted data was conducted to identify what information was involved and identify individuals to whom the data related.

Importantly, this incident was limited to Stryker's corporate environment and did not impact the functioning of any of Stryker's products.

What information was involved

The review determined that the data involved contained some of your personal information, including your name, and one or more of the following: [Extra2].

What we are doing

To help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to enhance the security of our network, internal systems and applications. Stryker will also continue to evaluate additional steps that may be taken to further increase our defenses. In addition, we are continuing to support federal law enforcement's investigation.

stryker

What you can do

While we are not aware of any evidence that your personal information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant of your information and, as a precaution, **Stryker is offering you complimentary access to Experian IdentityWorks^{SM} for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian is completely free to you and enrolling in this program will not hurt your credit score.

For more information on Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary 24-month membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For more information

Stryker takes the security of your personal information seriously, and sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call 833-918-9002, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time. If you have a speech or hearing impairment and use a TTY to call 711.

Sincerely,

Stryker

stryker

Experian IdentityWorks℠ Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 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 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 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** March 31, 2025 (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 833-918-9002 by March 31, 2025 (5:59 UTC). Be prepared to provide engagement number B135707 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 ExtendCARE™:** 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.

stryker

Information About Identity Theft Protection Guide

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: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

> **For New Mexico residents:** You may 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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

stryker

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For New York residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

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.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. Three Rhode Island residents were impacted by this incident.

NORTON ROSE FULBRIGHT

October 30, 2024

Via Email: *idtheft@oag.state.md.us*

Office of the Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202

Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3382
david.kessler@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

Re: Legal Notice of Security Incident

Dear Sir or Madam:

I am writing on behalf of our client, Stryker Corporation ("Stryker"), to notify your office of a cybersecurity incident that involved the personal information of 12 Maryland residents.

Stryker is a medical technology company specializing in medical and surgical, neurotechnology, orthopedics and spine products and services. In the course of its work, Stryker is provided access to personal information to perform services for its customers in the medical and healthcare industries.

On Monday, June 10, 2024, Stryker discovered unauthorized activity in a limited portion of its environment. Stryker immediately began an investigation, engaged leading third-party cybersecurity and forensic experts to assist in the investigation, and notified law enforcement.

Stryker's investigation determined that an unauthorized party gained access to certain Stryker internal systems at various times between May 14, 2024 and June 10, 2024, and that the unauthorized party exfiltrated some data from certain Stryker systems during this period ("exfiltrated data"). While Stryker cannot guarantee it, Stryker believes that the data has not been retained by the unauthorized party and has not been disclosed or transferred to any other third parties. Stryker is not aware of any evidence of any fraud or misuse of any personal information as result of this incident and continues to perform dark web monitoring.

A thorough review of the affected data was conducted to identify what personal information it contained and identify individuals to whom the information related. The bulk of the impacted individuals were associated with Stryker customers, including, but not limited to, patients and healthcare providers at hospitals. The investigation revealed the personal information included name, date of birth, and medical information. On September 25, 2024, Stryker substantially completed its review of the exfiltrated data and began notifying customers of any customer-related personal information included in these files.

After obtaining permission from its impacted customers who had patients affected by the incident, on October 31, 2024, Stryker will begin sending notification letters via First Class Mail to the affected individuals whose personal information was involved. A copy of the representative example(s) of the individual notice letter is attached. Stryker is offering 24 months of complimentary credit monitoring and fraud protection services to these individuals through Experian. Stryker is also providing a toll-free hotline for the individuals to call with any questions regarding the incident.

We are also writing to provide a list of customers who have directed Stryker to provide notice to your office on their behalf. A list of the customers who authorized us to provide their names to your office is enclosed at <u>Appendix A</u>.

To help prevent a similar type of incident from occurring in the future, Stryker implemented additional security protocols designed to enhance the security of its network, internal systems and applications. Stryker also continues to evaluate additional steps that may be taken to further increase its defenses.

The information being provided with this submission, and any potential supplemental submissions, constitutes proprietary and confidential information that is exempt from disclosure under the Freedom of Information Act and Maryland’s Public Information Act (collectively, “FOIA”). Stryker designates this response and information therein, and any potential supplemental responses and information, as confidential commercial information protected from disclosure by, among other exemptions, the exemptions contained in Maryland’s Public Information Act, MD General Provisions Code § 4-335 (2023). In the event that a FOIA request is received pursuant to which this letter could be deemed responsive, we request that we be furnished with a copy of all written materials pertaining to such request and be given a reasonable opportunity to respond prior to any determination that this response and any of the information herein will be produced.

The foregoing request for confidentiality under FOIA is without prejudice to any other rights, objections, or arguments that Stryker may have with respect to the confidential nature, and any production to third parties of this response.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Respectfully submitted,

David Kessler

David Kessler

NORTON ROSE FULBRIGHT

Appendix A

1	MedStar Health	Katherine Bornstein katherine.b.bornstein@medstar.net 443-285-2506

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

October 31, 2024

M3270-L04-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L04 ADULT
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Security Incident

Dear Sample A. Sample,

Stryker Corporation ("Stryker") is a medical technology company, headquartered in the U.S. and specializing in medical and surgical, neurotechnology, orthopedics and spine products and services. In the course of its work, Stryker is provided access to certain personal information to perform services for its customers in the medical and healthcare industries.

We are writing to inform you that we experienced a cybersecurity incident that involved some of your personal information. Stryker was in possession of this information due to its work with [Extra1]. This notice explains the incident, steps we have taken in response, and additional information on steps you may take to help protect your information.

What happened

On Monday, June 10, 2024, Stryker discovered unauthorized activity in a limited portion of its environment. Stryker immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Stryker also notified law enforcement and swiftly contained the incident.

The investigation determined that the unauthorized third party gained access to certain Stryker internal systems at various times between approximately May 14, 2024, and June 10, 2024, and obtained some data from Stryker systems. A thorough review of the impacted data was conducted to identify what information was involved and identify individuals to whom the data related.

Importantly, this incident was limited to Stryker's corporate environment and did not impact the functioning of any of Stryker's products.

What information was involved

The review determined that the data involved contained some of your personal information, including your name, and one or more of the following: [Extra2].

What we are doing

To help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to enhance the security of our network, internal systems and applications. Stryker will also continue to evaluate additional steps that may be taken to further increase our defenses. In addition, we are continuing to support federal law enforcement's investigation.

What you can do

While we are not aware of any evidence that your personal information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant of your information and, as a precaution, **Stryker is offering you complimentary access to Experian IdentityWorks^{SM} for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian is completely free to you and enrolling in this program will not hurt your credit score.

For more information on Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary 24-month membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For more information

Stryker takes the security of your personal information seriously, and sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call 833-918-9002, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time. If you have a speech or hearing impairment and use a TTY to call 711.

Sincerely,

Stryker

stryker

Experian IdentityWorks℠ Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 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 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 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** February 28, 2025 (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 833-918-9002 by February 28, 2025 (5:59 UTC). Be prepared to provide engagement number B134006 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 ExtendCARE™:** 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.

0000001

stryker

Information About Identity Theft Protection Guide

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: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

> **For New Mexico residents:** You may 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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

stryker

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For New York residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

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.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. One Rhode Island resident was impacted by this incident.

stryker

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

October 31, 2024

M3270-L06-0000003 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L06 ADULT CUSTOMER NAME EXCLUDED
APT ABC
123 ANY STREET
ANYTOWN, ST 12345-6789

Re: Notice of Data Security Incident

Dear Sample A. Sample,

Stryker Corporation ("Stryker") is a medical technology company, headquartered in the U.S. and specializing in medical and surgical, neurotechnology, orthopedics and spine products and services. In the course of its work, Stryker is provided access to certain personal information to perform services for its customers in the medical and healthcare industries.

We are writing to inform you that we experienced a cybersecurity incident that involved some of your personal information. Stryker was in possession of this information due to its work related to joint replacement procedures or treatments performed by one of Stryker's healthcare customers. This notice explains the incident, steps we have taken in response, and additional information on steps you may take to help protect your information.

What happened

On Monday, June 10, 2024, Stryker discovered unauthorized activity in a limited portion of its environment. Stryker immediately began an investigation and engaged leading third-party cybersecurity and forensic experts to assist. Stryker also notified law enforcement and swiftly contained the incident.

The investigation determined that the unauthorized third party gained access to certain Stryker internal systems at various times between approximately May 14, 2024, and June 10, 2024, and obtained some data from Stryker systems. A thorough review of the impacted data was conducted to identify what information was involved and identify individuals to whom the data related.

Importantly, this incident was limited to Stryker's corporate environment and did not impact the functioning of any of Stryker's products.

What information was involved

The review determined that the data involved contained some of your personal information, including your name, and one or more of the following: [Extra2].

What we are doing

To help prevent a similar type of incident from occurring in the future, we implemented additional security protocols designed to enhance the security of our network, internal systems and applications. Stryker will also continue to evaluate additional steps that may be taken to further increase our defenses. In addition, we are continuing to support federal law enforcement's investigation.

stryker

What you can do

While we are not aware of any evidence that your personal information has been misused, we wanted to make you aware of the incident and provide you with additional information on steps you may consider taking. We encourage you to remain vigilant of your information and, as a precaution, **Stryker is offering you complimentary access to Experian IdentityWorks^{SM} for 24 months**. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. Experian is completely free to you and enrolling in this program will not hurt your credit score.

For more information on Experian IdentityWorks^{SM}, including instructions on how to activate your complimentary 24-month membership, as well as additional steps you may take to help protect your information, please see the additional information provided in the following pages.

For more information

Stryker takes the security of your personal information seriously, and sincerely regrets that this incident occurred. For more information, or if you have any questions or need additional information, please call 833-918-9002, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time. If you have a speech or hearing impairment and use a TTY to call 711.

Sincerely,

Stryker

stryker

Experian IdentityWorks℠ Enrollment Information

To help protect your identity, we are offering complimentary access to Experian IdentityWorks℠ for 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 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 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** February 28, 2025 (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 833-918-9002 by February 28, 2025 (5:59 UTC). Be prepared to provide engagement number B134006 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 ExtendCARE™:** 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.

stryker

Information About Identity Theft Protection Guide

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: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. 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, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

> **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement.

It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

> **For New Mexico residents:** You may 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 may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, https://oag.dc.gov, 202-442-9828.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743- 0023.

For New York residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697- 1220, http://www.dos.ny.gov/consumerprotection; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

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.

For Rhode Island residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, http://www.riag.ri.gov, 401-274-4400.

Reporting of Identity Theft and Obtaining a Police Report. You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. One Rhode Island resident was impacted by this incident.