

September 4, 2020

Eric Benson
914.872.7328 (direct)
Eric.Benson@wilsonelser.com

VIA EMAIL:

DOJ-CPB@doj.nh.gov; Attorneygeneral@doj.nh.gov

Attorney General Gordon McDonald
Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

To Whom it May Concern:

Wilson Elser Moskowitz Edelman and Dicker LLP (“Wilson Elser”) represents Starling Physicians, PC (“Starling Physicians”) with respect to a recent data security incident (hereinafter, the “Incident”) described in more detail below. Starling Physicians takes the security and privacy of the information in its control seriously, and has taken steps to prevent a similar incident from occurring in the future.

1. Nature of the security Incident.

On or about July 7, 2020 Starling Physicians discovered that a recent data security incident involving Starling Physicians’ business email environment resulted in the exposure of personal information of current and past Starling Physicians’ patients to an unknown individual who was not authorized to view it. Starling Physicians has since worked diligently to determine exactly what happened and what information was involved as a result of this Incident.

Based on the results of an investigation conducted by a third-party electronic discovery vendor, Starling Physicians determined that the following elements of personal information may have been accessed and/or acquired by an unauthorized individual: names, dates of birth, social security numbers, and medical information including medical record and/or patient account numbers, Medicare and/or Medicaid ID numbers, diagnostic information, healthcare provider information, prescription and/or treatment information, and health insurance information. The exact elements of personal information that were exposed as a result of this incident varied per individual.

Starling Physicians does not have any evidence that any personal information belonging to its patients has been or will be misused or further disclosed as a result of this incident.

1133 Westchester Avenue • White Plains, NY 10604 • p 914.323.7000 • f 914.323.7001

Albany • Austin • Baltimore • Beaumont • Boston • Chicago • Dallas • Denver • Edwardsville • Garden City • Hartford • Houston • Kentucky • Las Vegas • London
Los Angeles • Miami • Michigan • Milwaukee • New Jersey • New Orleans • New York • Orlando • Philadelphia • San Diego • San Francisco • Stamford • Virginia
Washington, DC • West Palm Beach • White Plains

wilsonelser.com

2. Number of New Hampshire residents affected.

On or about August 25, 2020, Starling Physicians finished identifying a population of thirteen (13) current and one (1) former (residents have been identified as deceased) New Hampshire residents that were potentially affected by this Incident.

In accordance with the Health Insurance Portability and Accountability Act (HIPAA) “Breach Notification Rule,” 45 CFR §§ 164.400-414, incident notification letters addressed to these individuals or their representatives will be mailed on September 4, 2020, via First Class Mail. Sample copies of the Incident notification letters being mailed to potentially affected residents of New Hampshire are attached as Exhibit A – Exhibit C.

3. Steps taken.

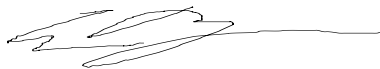
Starling Physicians has gone to great lengths to identify and notify any individuals who were potentially impacted as result of this Incident with the assistance of third-party vendors. Additionally, Starling Physicians has arranged for any potentially affected residents of New Hampshire to receive complimentary credit monitoring and identify theft protection services for twenty-four (24) months.

Starling Physicians is committed to ensuring the security of all information in its control, and is taking steps to prevent a similar event from occurring in the future. This includes strengthening its cybersecurity posture. Specifically, Starling Physicians is performing additional hardening of its network, platforms, and software to prevent the future occurrence of any similar data security incidents.

4. Contact information.

Starling Physicians remains dedicated to protecting the sensitive information within its control. If you have any questions or need additional information, please do not hesitate to contact me at Eric.Benson@wilsonelser.com or (914) 872-7328.

Very truly yours,



Eric Benson

WILSON ELSE MOSKOWITZ EDELMAN AND DICKER LLP

EXHIBIT A



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Heading>>

Dear <<Name 1>>,

Starling Physicians, PC (“Starling Physicians”) recently experienced a data security incident which may have affected your personal information. Starling Physicians takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident and steps we are taking to protect your personal information.

What Happened

On or about July 7, 2020 Starling Physicians discovered that a recent data security incident involving Starling Physicians’ business email environment resulted in the exposure of personal information of current and past Starling Physicians’ patients to an unknown individual who was not authorized to view it. Starling Physicians has since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

Based on the results of an investigation conducted by a third-party electronic discovery vendor, Starling Physicians determined that the following elements of your personal information may have been accessed and/or acquired by an unauthorized individual: <<Breached Elements>>.

Starling Physicians does not have any evidence that your home address, your Social Security number, your payment card information or your bank account information were disclosed during this incident. Additionally, Starling Physicians does not have any evidence that any personal information belonging to you has been or will be misused or further disclosed as a result of this incident. Nevertheless, Starling Physicians decided to notify you out of an abundance of caution so you may take steps to protect your information as recommended below.

What We Are Doing

Starling Physicians is committed to ensuring the security of all information in our control, and we are taking steps to prevent a similar event from occurring in the future. This includes strengthening our cybersecurity posture. Specifically, Starling Physicians is performing additional hardening of our network, platforms, and software to prevent the future occurrence of any similar data security incidents.

As a safeguard, we have arranged for you to enroll in a complementary, online credit monitoring service (*myTrueIdentity*) for twenty-four (24) months provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

Starling Physicians, PC | 2110 Silas Deane Highway, Rocky Hill, CT 06067 | (860) 258-3470

What You Can Do

To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive the credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two (2) years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (888) 490-0254, Monday – Friday, 9:00am to 9:00pm Eastern Standard Time.

Sincerely,



Michael Posner, MD, MBA, FACS
Chief Executive Officer and Chief Medical Officer
Starling Physicians, PC

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

EXHIBIT B



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

<<Variable Heading>>

Dear <<Name 1>>,

Starling Physicians, PC (“Starling Physicians”) recently experienced a data security incident which may have affected your personal information. Starling Physicians takes the security of your personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident and steps we are taking to protect your personal information.

What Happened

On or about July 7, 2020 Starling Physicians discovered that a recent data security incident involving Starling Physicians’ business email environment resulted in the exposure of personal information of current and past Starling Physicians’ patients to an unknown individual who was not authorized to view it. Starling Physicians has since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

Based on the results of an investigation conducted by a third-party electronic discovery vendor, Starling Physicians determined that the following elements of your personal information may have been accessed and/or acquired by an unauthorized individual: <<Breached Elements>>.

Starling Physicians **does not** have any evidence that your name, your home address, your Social Security number, your payment card information, or your bank account information were disclosed during this incident. **Additionally, at this time, Starling Physicians does not** have any evidence that any personal information belonging to you has been or will be misused or further disclosed as a result of this incident. Nevertheless, Starling decided to notify you out of an abundance of caution so you may take steps to protect your information as recommended below.

What We Are Doing

Starling Physicians is committed to ensuring the security of all information in our control, and we are taking steps to prevent a similar event from occurring in the future. This includes strengthening our cybersecurity posture. Specifically, Starling Physicians is performing additional hardening of our network, platforms, and software to prevent the future occurrence of any similar data security incidents.

As a safeguard, we have arranged for you to enroll in a complementary, online credit monitoring service (*myTrueIdentity*) for twenty-four (24) months provided by TransUnion Interactive, a subsidiary of TransUnion,[®] one of the three nationwide credit reporting companies.

Starling Physicians, PC | 2110 Silas Deane Highway, Rocky Hill, CT 06067 | (860) 258-3470

What You Can Do

To enroll in this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as “Enter Activation Code,” enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive the credit monitoring service online within minutes. If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

Once you are enrolled, you will be able to obtain two (2) years of unlimited access to your TransUnion credit report and credit score. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more. The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (888) 490-0254, Monday – Friday, 9:00am to 9:00pm Eastern Standard Time.

Sincerely,



Michael Posner, MD, MBA, FACS
Chief Executive Officer and Chief Medical Officer
Starling Physicians, PC

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.

EXHIBIT C



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>

Representative of the Estate of

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

<<City>><<State>><<Zip>>

<<Country>>

<<Date>>

<<Variable Heading>>

Dear Representative of the Estate of <<Name 1>>,

Starling Physicians, PC (“Starling Physicians”) recently experienced a data security incident which may have affected the personal information of your relative. Starling Physicians takes the security of all personal information very seriously, and we sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident and steps we are taking to protect your relative’s personal information.

What Happened

On or about July 7, 2020 Starling Physicians discovered that a recent data security incident involving Starling Physicians’ business email environment resulted in the exposure of personal information of current and past Starling Physicians’ patients to an unknown individual who was not authorized to view it. Starling Physicians has since worked diligently to determine exactly what happened and what information was involved as a result of this incident.

What Information Was Involved

Based on the results of an investigation conducted by a third-party electronic discovery vendor, Starling Physicians determined that the following elements of your relative’s personal information may have been accessed and/or acquired by an unauthorized individual: <<Breached Elements>>.

Starling Physicians does not have any evidence that your relative’s payment card information or bank account information were disclosed during this incident. Additionally, Starling Physicians does not have any evidence that any personal information belonging to your relative has been or will be misused or further disclosed as a result of this incident. Nevertheless, Starling Physicians decided to notify you out of an abundance of caution so you may take steps to protect your relative’s information as recommended below.

What We Are Doing

Starling Physicians is committed to ensuring the security of all information in our control, and we are taking steps to prevent a similar event from occurring in the future. This includes strengthening our cybersecurity posture. Specifically, Starling Physicians is performing additional hardening of our network, platforms, and software to prevent the future occurrence of any similar data security incidents.

Starling Physicians, PC | 2110 Silas Deane Highway, Rocky Hill, CT 06067 | (860) 258-3470

What You Can Do

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your relative's account statements, and to monitor his or her credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your relative's free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228.

You may also contact the three major credit bureaus directly to request a free copy of your relative's credit report. We recommend contacting the three credit reporting agencies listed below to discuss your particular situation and obtain specific guidance. Once you establish a relationship with the credit reporting agency and verify your authorization to make a request on behalf of your loved one, you can request a copy of your loved one's credit report. A review of the credit report will let you know of any active credit accounts that still need to be closed or any pending collection notices. Be sure to ask for all contact information on accounts currently open in your loved one's name (credit granters, collection agencies, etc.) so that you can follow through with these entities.

You may also request, in writing, that the credit report list the following alert:

"Deceased. Do not issue credit. If an application is made for credit, notify the following person(s) immediately: (list yourself, and/or another authorized relative, and/or executor/trustee of the estate – noting the relationship of any individual listed to your family members – and/or a law enforcement agency)."

In most cases, this flag will prevent the opening of new credit accounts in your relative's name. Contact information for the three major credit bureaus is as follows:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion

P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

Additionally, you can report a death by calling the Social Security Administration's toll-free number, 1-800-772-1213, between the hours of 6 AM – 6 PM CST, Monday through Friday. When you call, be sure to have the decedent's social security number available.

Although we are unaware of any misuse of your or anyone's information, to help relieve concerns and restore confidence following this incident, we have arranged for you to enroll in a complementary, online credit monitoring service (*myTrueIdentity*) for twenty-four (24) months provided by TransUnion Interactive, a subsidiary of TransUnion, one of the three nationwide credit reporting companies.

To activate this service, go to the *myTrueIdentity* website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code <<Insert Unique 12-letter Activation Code>> and follow the three steps to receive the credit monitoring service online within minutes. If you do not have access to the Internet and wish to use a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at 1-855-288-5422. When prompted, enter the six-digit telephone passcode <<Insert static 6-digit Telephone Pass Code>> and follow the steps to use the offline credit monitoring service.

You can sign up for the online or offline credit monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly.

For More Information

Please know that the protection of personal information is a top priority, and we sincerely regret any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call (888) 490-0254, Monday – Friday, 9:00am to 9:00pm Eastern Standard Time.

Sincerely,



Michael Posner, MD, MBA, FACS
Chief Executive Officer and Chief Medical Officer
Starling Physicians, PC

Additional Important Information

For residents of Hawaii, Michigan, Missouri, Virginia, Vermont, and North Carolina: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at <https://www.consumer.ftc.gov/articles/0155-free-credit-reports>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of Iowa: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina:

You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

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

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

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

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

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224, 1-800-771-7755, <https://ag.ny.gov/consumer-frauds/identity-theft>

For residents of Massachusetts: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (<https://www.transunion.com/fraud-alerts>); or Experian (<https://www.experian.com/fraud/center.html>). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348
<https://www.equifax.com/personal/credit-report-services/credit-freeze/>
800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013
www.experian.com/freeze
888-397-3742

TransUnion (FVAD)

P.O. Box 2000
Chester, PA 19022
freeze.transunion.com
800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.