MULLEN COUGHLIN LLC
ATTORNEYS AT LAW

Ryan C. Loughlin
Office: (267) 930-4786
Fax: (267) 930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

May 6, 2020

INTENDED FOR ADDRESSEE(S) ONLY

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Sir or Madam:

We represent Doctors Community Medical Center ("DCMC") at 8118 Good Luck Road, Lanham, Maryland 20706, and are writing to notify your office of an incident that may affect the security of personal information relating to three (3) New Hampshire residents. This notice may be supplemented if any new significant facts are learned subsequent to its submission. By providing this notice, DCMC does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

In January 2020, DCMC noticed suspicious activity within its payroll system. Upon investigation, hospital officials determined that a small number of employees had fallen victim to a phishing attack. By obtaining employees' credentials in the phishing attack, the unauthorized third party was able to access employees' payroll information and their email accounts. The investigation determined on or around February 13, 2020 that certain DCMC employee accounts were accessed by an unknown actor for various periods of time between November 6, 2019 and January 30, 2020.

The investigation was unable to determine with forensic certainty what emails were accessed by the unauthorized actor. In an abundance of caution, DCMC worked with third-party specialists to perform a comprehensive review of all information stored in the email accounts at the time of incident to confirm the identities of the individuals whose information may have been accessible to the unauthorized actor. On March 17, 2020, DCMC received the results of the third-party audit. DCMC immediately began reviewing the results of the audit to determine the identities and contact information for potentially impacted individuals.

The personal information potentially accessible within the email accounts may include the following information: name, financial account number, Social Security number, and driver's license number. The investigation was unable to specifically determine if this information was viewed.

Notice to New Hampshire Residents

On April 13, 2020, DCMC began providing notification of this event to potentially affected individuals via notice on its website in substantially the same form as the notice attached here as ***Exhibit A***. On May 6, 2020, DCMC began providing written notice of this incident to affected individuals, which includes three (3) New Hampshire residents. Written notice was provided to affected individuals in substantially the same form as the letters attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

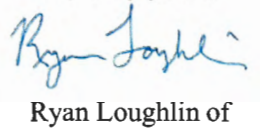
Upon discovering the potential unauthorized access to its email accounts, DCMC moved quickly to identify those that may be affected, put in place resources to assist them, and provide them with notice of this incident. DCMC is also working to implement additional safeguards to protect the security of information in its systems.

DCMC is providing written notice to those individuals who may be affected by this incident, in addition to notice via its website. This notice includes an offer of complimentary access to credit monitoring and identity restoration services through Experian, and the contact information for a dedicated call center for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, DCMC is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. DCMC is providing written notice of this incident to other regulators, as necessary. DCMC also provided notice of this event to federal law enforcement.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4786.

Very truly yours,



Ryan Loughlin of
MULLEN COUGHLIN LLC

RCL: szs
Enclosure

EXHIBIT A

Doctors Community Medical Center Provides Notice of a Phishing Event

Monday, April 13, 2020

(Lanham, MD) April 13, 2020 — In January 2020, DCMC noticed suspicious activity within its payroll system. Upon investigation, hospital officials determined that a small number of employees had fallen victim to a phishing attack. By obtaining employees' credentials in the phishing attack, the unauthorized third party was able to access employees' payroll information and their email accounts.

The investigation determined on or around Feb. 13, 2020 that certain DCMC employee accounts were accessed by an unknown actor for various periods of time between Nov. 6, 2019 and Jan. 30, 2020. As part of the investigation, officials determined that some of the email accounts contained data sheets with patient demographic information. While not the same for all impacted patients, the patient information contained in the emails included: name, address, date of birth, Social Security Number, driver's license, military identification number, financial account information, treatment information/diagnosis, prescription information, provider name, medical record number/patient ID, Medicare/Medicaid number, health insurance information, treatment cost information, and access credentials.

"Upon learning of the potential exposure of personal information, DCMC immediately launched an investigation to determine the nature and scope of this event," said Dave Lehr, chief information officer. "This included working with computer forensic investigators to determine the exact information impacted and identities of the individuals contained in the email accounts. We do not have any evidence that the particular emails with patient information were accessed, copied or re-disclosed. However, out of an abundance of caution, DCMC is providing written notice to all patients impacted by this incident."

"We take this incident and the security of personal information seriously," Lehr continued. "As part of our ongoing commitment to the privacy of personal information in our care, we are reviewing our existing policies and procedures and implementing

additional safeguards to further secure the information in our systems. As an added precaution, we are also offering complimentary credit monitoring and identity restoration services to those affected. We encourage potentially affected individuals to remain vigilant against incidents of identity theft by reviewing account statements and explanations of benefits for unusual activity and report any suspicious activity immediately to your insurance company, health care provider, or financial institution."

DCMC has notified federal law enforcement and is continuing to notify those who may be affected by this event as the investigation continues.

DCMC has established a dedicated assistance line for those seeking additional information regarding this incident. The toll-free assistance line at 833-943-1369 is available Monday through Friday (excluding U.S. holidays), during the hours of 9 am to 6:30 pm, Eastern Time. Those affected may also write to DCMC at 8118 Good Luck Road, Lanham, MD, 20706. Additional information will come via a mailed letter to patients impacted by this incident.

###

About Doctors Community Medical Center

Doctors Community Medical Center, now a part of Luminis Health, is a network of medical and surgical services provided throughout Prince George's County and Anne Arundel County. To complement the hospital's high quality and comprehensive services, the DCMC has more than a dozen centers of care in Bowie, Camp Springs, Crofton, District Heights, Hyattsville, Lanham, Largo, Laurel, Riverdale and Temple Hills. In addition to being recognized by U.S. News & World Report as a high-performing hospital in colon cancer surgery and heart failure, it is the only hospital in Prince George's County on Forbes' list of best midsize employers. Also, it earned Hospital Compare's four-star quality rating – the highest in Prince George's County. For more information, visit DCHweb.org or call 301-DCH-4YOU (301-324-4968).

">

8118 Good Luck Road
Lanham, Maryland 20706

301-552-8118

EXHIBIT B

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Doctors Community Medical Center ("DCMC"), writes to inform you of a recent event that may impact the security of some of your personal information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? In January 2020, DCMC noticed suspicious activity within its payroll system. Upon investigation, hospital officials determined that a small number of employees had fallen victim to a phishing attack. By obtaining employees' credentials in the phishing attack, the unauthorized third party was able to access employees' payroll information and their email accounts. The investigation determined on or around February 13, 2020 that certain DCMC employee accounts were accessed by an unknown actor for various periods of time between November 6, 2019 and January 30, 2020.

What Information Was Involved? As part of our investigation, we determined that some of the email accounts contained certain personal information and may have included your <<b2b_text_3(ImpactedData)>>. We do not have any evidence that any specific emails with personal information were accessed, copied or redisclosed. However, out of an abundance of caution, DCMC is providing written notice to all individuals impacted by this incident.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to secure our email accounts. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state and federal regulators, as well as federal law enforcement. We are also offering you access to 12 months of complimentary of credit monitoring and identity restoration services through Experian.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information*. We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits and to monitor your credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-833-943-1369, Monday through Friday, during the hours of 9:00 a.m. to 6:30 p.m., Eastern Time (excluding U.S. holidays). You may also write to Doctors Community Medical Center at 8118 Good Luck Road, Lanham, Maryland 20706.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Michael Widerman

Michael Widerman
Chief Information Security Officer
Doctors Community Medical Center

ELN-xxxx-xxxx

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enrollment Instructions

If you enrolled in credit monitoring using the instructions previously provided, you need not enroll again.

To help protect your identity, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<b2b_text_1(EnrollmentDeadline)>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code:** <<Member ID>>

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number <<b2b_text_2(Engagement Number)>> as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of 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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your 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 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 credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file

a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [x] Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/."

DOCTORS COMMUNITY HEALTH SYSTEM

<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

Doctors Community Medical Center ("DCMC"), writes to inform you of a recent event that may impact the security of some of your personal information. We are providing you with information about the event, our response, and steps you may take to better protect against the possibility of identity theft and fraud, should you feel it is necessary to do so.

What Happened? In January 2020, DCMC noticed suspicious activity within its payroll system. Upon investigation, hospital officials determined that a small number of employees had fallen victim to a phishing attack. By obtaining employees' credentials in the phishing attack, the unauthorized third party was able to access employees' payroll information and their email accounts. The investigation determined on or around February 13, 2020 that certain DCMC employee accounts were accessed by an unknown actor for various periods of time between November 6, 2019 and January 30, 2020.

What Information Was Involved? As part of our investigation, we determined that some of the email accounts contained data sheets with patient demographic information. While not the same for all impacted patients, the patient information contained in the emails included Name, Address, Date of Birth, Social Security Number, Driver's License, Military Identification Number, Financial Account Information, Treatment Information/Diagnosis, Prescription Information, Provider Name, MRN/Patient ID, Medicare/Medicaid Number, Health Insurance Information, Treatment Cost Information, and Access Credentials. We do not have any evidence that the particular emails with patient information were accessed, copied or redisclosed. However, out of an abundance of caution, DCMC is providing written notice to all patients impacted by this incident.

What We Are Doing. We take this incident and the security of your personal information seriously. Upon learning of this incident, we immediately took steps to secure our email accounts. As part of our ongoing commitment to the privacy of personal information in our care, we are working to review our existing policies and procedures and to implement additional safeguards to further secure the information in our systems. We also notified state and federal regulators, as well as federal law enforcement. We are also offering you access to 12 months of complimentary of credit monitoring and identity restoration services through Experian.

What You Can Do. You can find out more about how to protect against potential identity theft and fraud in the enclosed *Steps You Can Take to Protect Your Information.* We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, explanation of benefits and to monitor your credit reports for suspicious activity. You may also enroll in the complimentary credit monitoring services described above. Enrollment instructions are attached to this letter.

For More Information. If you have additional questions, please call our dedicated assistance line at 1-833-943-1369, Monday through Friday, during the hours of 9:00 a.m. to 6:30 p.m., Eastern Time (excluding U.S. holidays). You may also write to Doctors Community Medical Center at 8118 Good Luck Road, Lanham, Maryland 20706.

We sincerely regret any inconvenience or concern this incident may cause.

Sincerely,

Michael Widerman

Michael Widerman
Chief Information Security Officer
Doctors Community Medical Center

ELN-xxxx-xxxx

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enrollment Instructions

If you enrolled in credit monitoring using the Instructions previously provided, you need not enroll again.

To help protect your identity, we are offering a complimentary one-year membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **<<b2b_text_1(EnrollmentDeadline)>>** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: <<Member ID>>**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057. Be prepared to provide engagement number **<<b2b_text_2(Engagement Number)>>** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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, Equifax and Transunion files for indicators of 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.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call 877-288-8057 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at 877-288-8057.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Monitor Your Accounts

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your 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 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 credit report.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 160	PO Box 105788
Allen, TX 75013	Woodlyn, PA 19094	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	www.equifax.com/personal/credit-report-services

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file

a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For Maryland residents: The Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662, www.oag.state.md.us.

For North Carolina residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For New Mexico residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For Rhode Island residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov, 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [x] Rhode Island residents impacted by this incident.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/."