BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

MONARCH PLAZA
SUITE 1500
3414 PEACHTREE ROAD N.E.
ATLANTA, GEORGIA 30326

PHONE: 404.577.6000
FAX: 404.221.6501

www.bakerdonelson.com

ALEXANDER F. KOSKEY, III, CIPP/US, CIPP/E, PCIP
Direct Dial: 404.443.6734
Email: akoskey@bakerdonelson.com

June 6, 2022

VIA U.S. MAIL

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

Re: *Lincare Holdings Inc. – Supplemental Notice of Data Incident*

Dear Attorney General Landry:

We continue to represent Lincare Holdings Inc. ("Lincare"). We are writing to supplement the notice provided to your Office on February 9, 2022.

Lincare has continued its comprehensive review of the potentially impacted data to identify individuals who may have been affected by the incident. This review required customized protocols and programming in order to analyze the data and identify key information. On or about June 3, 2022, Lincare provided written notice via U.S. Mail to an additional 5,591 New Hampshire residents. The personal information that was potentially involved primarily included the individual's name, health insurance information, and/or medical information. In limited circumstances, Social Security numbers or driver's license numbers were potentially impacted. Lincare is not aware of any misuse of information as a result of this incident. A sample notification letter sent to the New Hampshire residents recently notified is enclosed for your reference and includes:

- A description of the security incident;
- Steps taken to investigate the incident;
- Steps taken to mitigate any potential harm to individuals;
- Instructions for activation of 1 years of free credit monitoring and identity theft protection services where appropriate;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this incident.

Lincare also posted notice of this incident on its website and issued notices to the media in all 50 states. Although Lincare had strong security measures in place prior to the incident, it has implemented and is continuing to implement additional technological safeguards, upgrades, and security measures to further enhance security within its IT environment. These measures include, but are not limited to, upgrading its endpoint monitoring system, modifying firewall geo-blocking rules to restrict IP addresses that are permitted to access its network, and enhanced vulnerability scans and penetration testing.

Please contact me if you have any questions.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

Alexander F. Koskey, III

Exhibit A: Sample Notification Letter
Exhibit B: February 9, 2022 Notice

LINCARE
A Linde company

Exhibit A

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

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

RE: <<b2b_text_1(Notice of Security Incident / Notice of Data Breach>>

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

Lincare Holdings Inc. and its subsidiary companies (collectively, "Lincare") value and respect the privacy and security of personal information, which is why we are notifying you of a security incident that may have involved the disclosure of some of your personal information. This letter contains information regarding the incident, the measures Lincare has taken since the incident, and steps you can take to further protect your information, should you feel it appropriate to do so.

What Happened? On September 26, 2021, Lincare identified unusual activity on certain systems within its network. Lincare took immediate action after learning of the incident to secure its network and launched an investigation, including working with outside cybersecurity experts to determine the source of the activity and potential impact on Lincare's network. The investigation confirmed that certain systems may have first been accessed on September 10, 2021. The unauthorized access was blocked by September 29, 2021. Lincare promptly began a comprehensive review of all potentially impacted data to identify individuals who may have been affected by the incident. This review required customized protocols and programming in order to analyze the data and identify key information. This process, which also included a manual review of the data, was time intensive but necessary in order to ensure that appropriate notification occurred. On April 20, 2022, it was confirmed that your information was involved and an up-to-date mailing address was identified in order to provide you with notification of this incident.

What Information Was Involved? The investigation determined that the following types of information relating to you were involved in this incident: <<b2b_text_2(name, data elements)>><<b2b_text_3(data elements cont.)>>. We are also not aware of any misuse of your information as a result of this incident.

What We Are Doing. We are committed to protecting your information. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary identity and credit monitoring through Kroll. These services will be available to you for one year at no cost to you in order to give you peace of mind. This letter contains additional information regarding these services and instructions on how you may activate. You must complete the activation steps listed in this letter.

We take the protection and proper use of personal information very seriously. We took steps to launch an investigation immediately after identifying the incident, enlisted outside cybersecurity experts to assist in the investigation, and notified law enforcement of the incident. We also promptly reset all user passwords to block any unauthorized access and are implementing additional technological safeguards on our systems that contain personal information to minimize the possibility of an incident like this from occurring in the future. This letter also includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

What You Can Do. We recommend that you activate your complimentary credit monitoring services with Kroll. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review all claims information from your health insurance provider, and to monitor your credit reports and financial statements for suspicious activity. You can also report any suspicious activity to the credit bureaus at the numbers listed below in this letter. We also recommend that you review the information we are enclosing in this letter about steps you can take to help protect your personal information as you deem appropriate.

For more information or if you have additional questions regarding the information contained in this letter, please call our toll-free assistance line at 855-912-1262, Monday through Friday, 9:00 am to 6:30 pm Eastern Time (excluding major US holidays). Lincare regrets any inconvenience that this incident may have caused you.

Sincerely,

Lincare Holdings Inc.

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1]Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Below are additional actions you may take, if you feel it is necessary.

- **FREEZE YOUR CREDIT FILE.** You have a 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES		
Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following:

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, 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.); and
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.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.
- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD**. As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, carefully reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/ credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)
- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report from each of the three major credit reporting bureaus annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

- **FILE OR OBTAIN A POLICE REPORT.** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report incidents of identity theft to local law enforcement or to the Attorney General.
- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1-877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information.
- **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.
- **For residents of North Carolina:** The North Carolina Office of the General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.
- **For residents of Maryland**: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.
- **For residents of New Mexico:** 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. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, 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 violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific 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 residents of New York**: The Attorney General may be contacted at: Office of Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
- **For residents of Rhode Island**: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400, and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident.
- **For residents of the District of Columbia.**: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, by phone at (202) 727-3400; and, https://oag.dc.gov/. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

MONARCH PLAZA
SUITE 1500
3414 PEACHTREE ROAD N.E.
ATLANTA, GEORGIA 30326

PHONE: 404.577.6000
FAX: 404.221.6501

www.bakerdonelson.com

ALEXANDER F. KOSKEY, III, CIPP/US, CIPP/E, PCIP
Direct Dial: 404.443.6734
Email: akoskey@bakerdonelson.com

Exhibit B

February 9, 2022

VIA U.S. MAIL

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

Re: *Lincare Holdings Inc. – Notice of Data Incident*

To Whom It May Concern:

We represent Lincare Holdings Inc. ("Lincare"), whose principal place of business is located at 19387 U.S. 19 North, Clearwater, Florida 33764. Lincare is a HIPAA-regulated entity that, by and through its subsidiaries, supplies in-home respiratory therapy and other related products and services.

This correspondence is to notify you that Lincare was the victim of a recent security incident that may affect the security of some personal information relating to New Hampshire residents.[1] On or about September 26, 2021, Lincare identified unusual activity on certain systems within its network. Lincare took immediate action to secure its network and launched an investigation, including working with outside experts to determine the source of the activity and potential impact on Lincare's network.[2] It has been determined that certain systems may have been first accessed on September 10, 2021. The unauthorized access was blocked by September 29, 2021. A review of the potentially impacted data was commenced to identify the scope of the incident and to identify individuals whose information may have been involved in the incident. The review of potentially impacted data remains ongoing. However, on December 15, 2021, Lincare learned that information of New Hampshire residents may have been involved in the incident and worked diligently to identify an up-to-date mailing address for those individuals.

Due to the risk that personal information may have been accessed or acquired during the incident, in an abundance of caution, notification letters are being sent via U.S. Mail to 5 residents

[1] By providing this notice, Lincare does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data incident notification statute, or personal jurisdiction.
[2] Lincare has notified law enforcement of this incident.

of your state on or about February 9, 2022. The notification letters include instructions for activating one (1) year of credit monitoring services at no cost to the residents. The personal information that was potentially at risk included the individual's name, Social Security number, financial account number, and/or health information. A sample notification letter is enclosed for your reference and includes:

- A description of the security incident;
- Steps taken to investigate the incident;
- Steps taken to mitigate any potential harm to individuals;
- Instructions for activation of 1 year of free credit monitoring and identity theft protection services;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this incident.

Lincare is fully committed to protecting the privacy and confidentiality of personal information. As the investigation continues, we will follow up this correspondence with additional information if necessary.[3] Please contact me if you require any additional information regarding this incident in the meantime.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC

Alexander F. Koskey, III

Exhibit A: Sample notification letter to 5 residents

[3] Lincare also published substitute notice on its website on November 24, 2021.

LINCARE
A Linde company

EXHIBIT A

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

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

<<b2b_text_1(RE: Notice of Security Incident / Notice of Data Breach>>

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

Lincare Holdings Inc. and its subsidiary companies (collectively, "Lincare") value and respect the privacy and security of personal information, which is why we are notifying you of a recent security incident that may have involved the disclosure of some of your personal information. This letter contains information regarding the incident, the measures Lincare has taken since the incident, and steps you can take to further protect your information, should you feel it appropriate to do so.

What Happened? On September 26, 2021, Lincare identified unusual activity on certain systems within its network. Lincare took immediate action after learning of the incident to secure its network and launched an investigation, including working with outside cybersecurity experts to determine the source of the activity and potential impact on Lincare's network. The investigation confirmed that certain systems may have first been accessed on September 10, 2021. The unauthorized access was blocked by September 29, 2021. Lincare promptly began a comprehensive review of all potentially impacted data to identify individuals whose information may have been exposed during the period of unauthorized access. This review, which included a manual review of the data, was necessary in order to identify any individuals whose information may have been involved in the incident. On December 15, 2021, we learned that some of your personal information may have been involved in the incident. We then worked diligently to identify an up-to-date mailing address and provide you with notification of this incident.

What Information Was Involved? The investigation determined that the following types of information relating to you were involved in this incident: <<b2b_text_2(name, data elements)>><<b2b_text_3(data elements cont.)>>. We are also not aware of any misuse of your information as a result of this incident.

What We Are Doing. We are committed to protecting your information. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary credit monitoring through Kroll. These services will be available to you for one year at no cost to you in order to give you peace of mind. This letter contains additional information regarding these services and instructions on how you may activate. You must complete the activation steps listed in this letter.

We take the protection and proper use of personal information very seriously. We took steps to launch an investigation immediately after identifying the incident, enlisted outside cybersecurity experts to assist in the investigation, and notified law enforcement of the incident. We also promptly reset all user passwords to block any unauthorized access and are implementing additional technological safeguards on our systems that contain personal information to minimize the possibility of an incident like this from occurring in the future. This letter also includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so.

What You Can Do. We recommend that you activate your complimentary credit monitoring services with Kroll. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review all claims information from your health insurance provider, and to monitor your credit reports and financial statements for suspicious activity. You can also report any suspicious activity to the credit bureaus at the numbers listed below in this letter. We also recommend that you review the information we are enclosing in this letter about steps you can take to help protect your personal information as you deem appropriate.

For more information or if you have additional questions regarding the information contained in this letter, please call our toll-free assistance line at 855-912-1262, Monday through Friday, 9:00 am to 6:30 pm Eastern Time (excluding major US holidays). Lincare regrets any inconvenience that this incident may have caused you.

Sincerely,

Lincare Holdings Inc.

KROLL

We have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate Your Identity Monitoring Services

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

Take Advantage of Your Identity Monitoring Services

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1]Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Below are additional actions you may take, if you feel it is necessary.

- **FREEZE YOUR CREDIT FILE.** You have a 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. Note that a security freeze generally does not apply to existing account relationships and when a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control or similar activities. There is no charge to place or lift a security freeze.

To place a security freeze on your credit report, contact each of the three major consumer reporting agencies using the contact information listed below:

3 MAJOR CREDIT BUREAUS / CONSUMER REPORTING AGENCIES

Equifax	**Experian**	**TransUnion**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348	Allen, TX 75013	Woodlyn, PA 19094
1-800-685-1111	1-888-397-3742	1-888-909-8872
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following:

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, 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.); and
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.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

- **PLACE FRAUD ALERTS ON YOUR CREDIT FILE.** As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit 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 an alert lasting 7 years. Contact the credit reporting agencies listed above to activate an alert.

- **REMAIN VIGILANT: REVIEW YOUR ACCOUNT STATEMENTS, & REPORT FRAUD.** As a precautionary measure, we recommend that you remain vigilant to protect against potential fraud and/or identity theft by, among other things, carefully reviewing your credit reports, debit/credit card, insurance policy, bank account and other account statements. Activate alerts on your bank accounts to notify you of suspicious activity. Report suspicious or fraudulent charges to your insurance statements, credit report, credit card or bank accounts to your insurance company, bank/ credit card vendor and law enforcement. (For Oregon & Iowa residents: Report any suspected identity theft to law enforcement, Federal Trade Commission, and your State Attorney General.)

- **ORDER YOUR FREE ANNUAL CREDIT REPORTS.** Visit www.annualcreditreport.com or call 877-322-8228 to obtain one free copy of your credit report from each of the three major credit reporting bureaus annually. Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three credit reporting agencies directly to obtain such additional reports.)

- **FILE OR OBTAIN A POLICE REPORT.** You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report incidents of identity theft to local law enforcement or to the Attorney General.

- **OBTAIN INFORMATION ABOUT PREVENTING IDENTITY THEFT FROM FTC / STATE ATTORNEY GENERAL.** Go to http://www.experian.com/credit-advice/topic-fraud-and-identity-theft.html. The Federal Trade Commission also provides information at www.ftc.gov/idtheft. The FTC can be reached by phone: 1-877-438-4338; TTY: 1-866-653-4261 or by writing: 600 Pennsylvania Ave., NW, Washington, D.C. 20580. Your State Attorney General also may provide information.

- **FAIR CREDIT REPORTING ACT:** You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. The FTC has published a list of the primary rights created by the FCRA (https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), and that article refers individuals seeking more information to visit www.ftc.gov/credit. The FTC's list includes the following FCRA rights: (1) To receive a copy of your credit report, which must contain all the information in your file at the time of your request; (2) To receive a free copy of your credit report, at your request, once every 12 months from each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion; (3) To receive a free credit report if a company takes adverse action against you (e.g. denying your application for credit, insurance, or employment), and you ask for your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the credit reporting company. You are also entitled to one free report a year if you are unemployed and plan to look for a job within 60 days; if you are on welfare; or if your report is inaccurate because of fraud, including identity theft; (4) To ask for a credit score; (5) To dispute incomplete or inaccurate information; (6) To obtain corrections to your report or delete inaccurate, incomplete, or unverifiable information; (7) Consumer reporting agencies may not report outdated negative information; (8) To restrict access to your file and to require consent from you for reports to be provided to employer; (9) To limit "prescreened" offers of credit and insurance you receive based on information in your credit report; and (10) To seek damages from violators. Please note that identity theft victims and active duty military personnel may have additional rights under the FCRA.
- **For residents of North Carolina:** The North Carolina Office of the General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.
- **For residents of Maryland**: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.
- **For residents of New Mexico:** 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. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, 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 violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific 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 residents of New York**: The Attorney General may be contacted at: Office of Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.
- **For residents of Rhode Island**: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400, and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident.
- **For residents of the District of Columbia.**: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, by phone at (202) 727-3400; and, https://oag.dc.gov/. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.