



20 Church Street
20th Floor
Hartford, CT 06103
Telephone: 860-525-5065
Fax: 860-955-1145
www.lockelord.com

Theodore P. Augustinos
Direct Telephone: 860-541-7710
Direct Fax: 888-325-9082
ted.augustinos@lockelord.com

July 1, 2022

By E-mail (ldtheft@oag.state.md.us)

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Lightfoot, Franklin & White, LLC
Notice pursuant to MD Code, Commercial Law, §14-3504

To the Office of the Attorney General:

We represent Lightfoot, Franklin & White, LLC ("Lightfoot"), a law firm based in Birmingham, Alabama that handles commercial litigation and other legal matters. On behalf of Lightfoot, we hereby provide notice pursuant to MD Code, Commercial Law, §14-3504 of a security incident involving disclosure of the personal information of 18 Maryland residents, based on our investigation to date. We will supplement this letter if any additional Maryland residents are discovered to be impacted by this incident.

What Happened

On March 4, 2022, Lightfoot discovered that certain client files had been compromised in an apparent ransomware attack. Lightfoot took immediate steps to contain the incident, engaged outside consultants to conduct an investigation, and notified law enforcement. Lightfoot engaged our law firm, and we engaged experienced outside forensics investigators to determine the scope and nature of the attack, as well as the extent to which the security of personal and corporate information may have been compromised.

What Information Was Involved

Based on Lightfoot's investigation, which is ongoing, it appears that the personal information exposed in this incident included affected individuals' names, Social Security numbers and other government-issued identification numbers, and certain health and medical information. Not all affected individuals had the same types of information compromised.

What Lightfoot Is Doing

As noted above, immediately upon the discovery of the attack, Lightfoot took steps to contain the incident and prevent any further unauthorized access. As required by MD Code, Commercial Law, §14-3504, Lightfoot is providing notice of this incident to the affected individuals by mail on or about July 1, 2022. A template for the notification letter is attached. The notification letter describes Lightfoot's offer of credit monitoring services for 12 months at no cost to the affected individuals, and provides additional guidance for affected individuals to protect themselves. Lightfoot is also reviewing and enhancing its safeguards to mitigate the risk of further or future compromises of personal information.

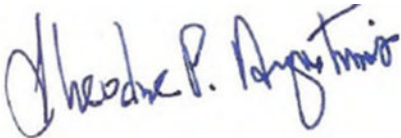
On behalf of Lightfoot, we are notifying state agencies as required in jurisdictions where affected individuals reside.

Please note that the investigation is ongoing and Lightfoot expects to notify additional populations as to other types of data upon completion of the data review process. At that time, if appropriate, we expect to supplement this notification.

* * * * *

Please do not hesitate to contact me with any questions related to this matter.

Sincerely,

A handwritten signature in blue ink that reads "Theodore P. Augustinos". The signature is written in a cursive, flowing style.

Theodore P. Augustinos

Enclosure

[Return Address]
[Return Address]

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Notice of Data Breach
Please read this entire letter.

Dear [Insert name]:

Lightfoot, Franklin & White, LLC is a law firm based in Birmingham, Alabama that handles commercial litigation, product liability, professional liability, white-collar criminal, and other legal matters. We are notifying you about [a security][a ransomware] incident that resulted in unlawful access to a file which contained personal information relating to you. As a result, we are notifying you of this incident to inform you of the immediate steps we have taken and to provide you with tools to help you protect yourself

What Happened?

On March 4, 2022, we learned of and stopped [a security][a ransomware] incident that resulted in unlawful access by an unauthorized third party to certain client files. Some of those files contained personal information for individuals related to certain cases, including plaintiffs, defendants, witnesses, and other non-parties. Your information was contained in the files. [Based upon our analysis to date, the incident impacted the personal information of approximately [insert number] residents of Texas.]

What Information Was Involved?

Your personal information that was potentially exposed may have included your name, date of birth, health information, account information, and government-issued identification numbers such as your Driver's License or Social Security number. **Currently, we have no indication that any of your personal information has been or will be misused in connection with this incident.**

What We Are Doing

Upon discovering this incident, we took immediate steps to contain the incident, engaged outside consultants to conduct an investigation, and notified law enforcement. To take all possible steps to protect your personal information against disclosure or misuse by the unauthorized third party, we reached a resolution and have received confirmation from the third party that the compromised information was destroyed. We have engaged in an extensive review to identify the individuals whose personal information was compromised, and we are notifying those individuals or their families on behalf of clients.

We also continue to enhance the security of our systems and the data entrusted to us. These steps include further segregating and restricting access to client confidential information; enhancing our cyber security team; deploying

additional technical safeguards; and working with outside consultants to further review and enhance our security policies and procedures. We have also engaged a service provider to conduct both public and dark web monitoring for any posting or exchange of personal information related to this incident. While we have no indication that any of your personal information has been or will be misused in connection with this incident, we nevertheless have arranged for services and provided the advice described below to help you protect yourself against potential risk and to alleviate any concern related to this incident.

What You Can Do

We recommend that you remain vigilant by reviewing your account statements and credit reports regularly, as well as reporting any suspicious transactions to your financial services provider. To help you protect yourself against risks related to this incident, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. Enclosed with this letter is information regarding these services and instructions for enrollment, along with additional information regarding steps you can take to protect yourself against identity theft and fraud.

For More Information

To enroll in the credit services we are offering at no cost to you, please follow the instructions enclosed with this letter. While there is no evidence that your personal information has been misused, we encourage you to take full advantage of the information being provided in the enclosure.

Unfortunately, these incidents are a consistent threat to successful businesses across the country, and countless sophisticated organizations have had to deal with this reality. We sincerely apologize for any inconvenience or concern this situation may cause. If you have questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center, toll free, at (877) 770-3331.

Sincerely,

Melody H. Eagan
Managing Partner

Enclosure

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM. 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:

To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: September 30, 2022**. (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/plus>
- Provide your **activation code**: _____

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) 770-3331 by **September 30, 2022**. Be prepared to provide engagement number B055112 as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

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

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at (877) 770-3331. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

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

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax

P.O. Box 740241

Atlanta, Georgia 30374

www.equifax.com

1-800-685-1111 Credit Reports

1-888-766-0008 Fraud Alert

1-800-685-1111 Security Freeze

Experian

P.O. Box 2002

Allen, TX 75013

www.experian.com

1-888-397-3742 Credit Reports

1-888-397-3742 Fraud Alert

1-888-397-3742 Security Freeze

TransUnion (FVAD)

P.O. Box 105281

Atlanta, GA 30348-5281

www.transunion.com

1-800-888-4213 Credit Reports

1-800-680-7289 Fraud Alert

1-800-680-7289 Security Freeze

Federal Trade Commission (FTC) and State Resources: General guidance on protecting yourself from identity theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at <http://www.ftc.gov/bcp/edu/microsites/idtheft>. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may require fees to be paid, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

Additional Information: You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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.

D.C.: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the D.C. Attorney General at (202) 442-9828 or consumer.protection@dc.gov.

Iowa: You should report suspected incidents of identity theft to your local law enforcement or the Iowa Attorney General.

Maryland: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the Maryland Attorney General at 1-888-743-0023, Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, and <https://www.marylandattorneygeneral.gov>.

New Mexico: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You should review your personal account statements and credit reports, as applicable, to detect any errors that may or may not be a result of a security incident.

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

North Carolina: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

Rhode Island: You can also contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.

[Return Address]
[Return Address]

[Date]

[Insert Recipient's Name]
[Insert Address]
[Insert City, State, Zip]

RE: Notice of Data Breach
Please read this entire letter.

Dear Family of [Insert name]:

Lightfoot, Franklin & White, LLC is a law firm based in Birmingham, Alabama that handles commercial litigation, product liability, professional liability, white-collar criminal, and other legal matters. We are notifying you about a ransomware incident that resulted in unlawful access to a file which contained personal information relating to your family member. As a result, we are notifying you of this incident to inform you of the immediate steps we have taken and to provide you with tools to help you protect your family member.

What Happened?

On March 4, 2022, we learned of and stopped a ransomware incident that resulted in unlawful access by an unauthorized third party to certain files related to Lightfoot or its legal representation of certain clients. Your family member's information was contained in the files. [Based upon our analysis to date, the incident impacted the personal information of approximately [insert number] residents of Texas.]

What Information Was Involved?

Your family member's personal information that was potentially exposed may have included your family member's name, date of birth, health information, account information, and government-issued identification numbers such as your family member's Driver's License or Social Security number. **Currently, we have no indication that any of your family member's personal information has been or will be misused in connection with this incident.**

What We Are Doing

Upon discovering this incident, we took immediate steps to contain the incident, engaged outside consultants to conduct an investigation, and notified law enforcement. To take all possible steps to protect your family member's information against disclosure or misuse by the unauthorized third party, we reached a resolution and have received confirmation from the third party that the compromised information was destroyed. We have engaged in an extensive review to identify the individuals whose personal information was compromised, and we are notifying those individuals or their families.

We also continue to enhance the security of our systems and the data entrusted to us. These steps include further segregating and restricting access to client confidential information; enhancing our cyber security team; deploying

additional technical safeguards; and working with outside consultants to further review and enhance our security policies and procedures. We also continue to monitor both the public and dark web for any posting or exchange of personal information related to this incident, and we have found no such indication.

What You Can Do

While we have no indication that any of your family member's personal information has been or will be misused in connection with this incident, we nevertheless have provided the advice described in the enclosure, to help you protect your family member's identity against potential risk and to alleviate any concern related to this incident.

For More Information

Unfortunately, these incidents are a consistent threat to successful businesses across the country, and countless sophisticated organizations have had to deal with this reality. We sincerely apologize for the inconvenience or concern this situation may cause. While there is no evidence that your family member's information has been misused, we encourage you to take full advantage of the information being provided in the enclosure.

If you have questions regarding this incident, please feel free to contact our dedicated call center, toll free, at (877) 770-3331.

Sincerely,

Melody H. Eagan
Managing Partner

Enclosure

Protecting Your Family Member

Below is information on steps you can take when a deceased or incapacitated loved one is affected by a data compromise incident.

Deceased

Decrease the risk of their identity theft regardless of age by following these steps:

1. Obtain at least 12 copies of the official death certificate when it becomes available. In some cases you will be able to use a photocopy, but some businesses will request an original death certificate. Since many death records are public, a business may require more than just a death certificate as proof.
2. If there is a surviving spouse or other joint account holders, make sure to immediately notify relevant credit card companies, banks, stock brokers, loan/lien holders, and mortgage companies of the death. They may require a copy of the death certificate to do this, as well as permission from the survivor, or other authorized account holders.
3. The executor or surviving spouse will need to discuss all outstanding debts and how they will be dealt with. You will need to transfer the account to another person or close the account. If you close the account, ask them to list it as: "Closed. Account holder is deceased."
4. Contact all CRAs (**see contact information below**), credit issuers, collection agencies, and any other financial institution that need to know of the death using the required procedures for each one. The following are general tips:
 - a. Include the following information in all letters:
 - i. Name and SSN of deceased
 - ii. Last known address
 - iii. Last 5 years of addresses
 - iv. Date of birth
 - v. Date of death
 - vi. To speed up processing, include all requested documentation specific to that agency in the first letter
 - b. Send the appropriate Court signed Executive papers.
 - c. Send all mail certified, return receipt requested.
 - d. Keep copies of all correspondence, noting date sent and any response(s) you receive.
 - e. Request a copy of the decedent's credit report – See sample template below. A review of each 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 the name of the deceased (credit granters, collection agencies, etc.) so that you can follow through with those entities.
 - f. Request that the report is flagged with the following alert: "Deceased. **Do not** issue credit. If an application is made for credit, notify the following person(s) immediately: (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Note: Friends, neighbors, or distant relatives do not have the same rights as a spouse or executor of the estate. They are classified as a third party and a CRA may not mail out a credit report or change data on a consumer file upon their request. If you fall into this classification and are dealing with a very unique situation, you may write to the CRA and explain the situation. They are handled on a case-by-case basis. You may also apply to the courts to be named as an executor of the estate.

Other groups to notify:

- Social Security Administration
- Insurance companies - auto, health, life, etc.
- Veteran's Administration - if the person was a former member of the military
- Immigration Services - if the decedent is not a U.S. citizen

- Department of Motor Vehicles if the person had a driver's license or state ID card. Also make sure that any vehicle registration papers are transferred to the new owners.
- Agencies that may be involved due to professional licenses - bar association, medical licenses, cosmetician, etc.
- Any membership programs - video rental, public library, fitness club, etc.

Specific Credit Reporting Agencies (CRAs) information for ordering a credit report or place a deceased flag:

Experian P.O. Box. 9701 Allen, TX 75013	
<u>To Order a Credit Report:</u> A spouse can obtain a credit report by simply making the request through the regular channels - mail, phone, and Internet. The spouse is legally entitled to the report. The executor of the estate can obtain a credit report but must write Experian with a specific request, a copy of the executor paperwork and the death certificate.	<u>For Requests or Changes:</u> A spouse or executor may change the file to show the person as deceased via written request. A copy of the death certificate and in the case of the executor, the executor's paperwork must be included with the request. After any changes, Experian will send an updated credit report to the spouse or executor for confirmation that a deceased statement has been added to the credit report. This is important as executors and spouse can request other types of "changes" that we may not be able to honor. If identity theft is a stated concern, Experian will add a security alert after the file has been changed to reflect the person as deceased. If there are additional concerns, Experian will add a general statement to the file at the direction of the spouse/executor. The spouse/executor must state specifically what they want the general statement to say, such as "Do not issue credit."
Equifax Information Services LLC Office of Consumer Affairs P.O. Box 105139 Atlanta, GA 30348	
<u>To Order a Credit Report:</u> Equifax requests that the spouse, attorney or executor of the estate submit a written request to receive a copy of the deceased consumer's' file. The request should include the following: A copy of a notarized document stating that the requestor is authorized to handle the deceased consumer's affairs (i.e.: Order from a Probate Court or Letter of Testamentary)	<u>For Requests or Changes:</u> Equifax requests that a spouse, attorney or executor of the estate submit a written request if they would like to place a deceased indicator on the deceased consumer's file. The written request should include a copy of the consumer's death certificate. The request should be sent to the address listed above. Upon receipt of the death certificate, Equifax will attempt to locate a file for the deceased consumer and place a death notice on the consumer's file. In addition, Equifax will place a seven

	year promotional block on the deceased consumer's file. Once Equifax's research is complete, they will send a response back to the spouse, attorney, or executor of the estate.
TransUnion P.O. Box 6790 Fullerton, CA 92834	
<u>To Order a Credit Report:</u> TransUnion requires proof of a power of attorney, executor of estate, conservatorship or other legal document giving the requestor the legal right to obtain a copy of the decedent's credit file. If the requestor was married to the deceased and the address for which the credit file is being mailed to is contained on the decedent's credit file, then TransUnion will mail a credit file to the surviving spouse. If the deceased is a minor child of the requestor, TransUnion will mail a credit file to the parent upon receipt of a copy of the birth certificate or death certificate naming the parent as requestor.	<u>For Requests or Changes:</u> Placing a "decease alert" on reports: TransUnion will accept a request to place a temporary alert on the credit file of a deceased individual from any consumer who makes such a request and identifies themselves as having a right to do so. The requestor's phone number is added to the temporary, three month alert. Upon receipt of a verifiable death certificate, TransUnion will entirely suppress the decedent's credit file and so note it as a deceased consumer. TransUnion will not mail out a copy of its contents without the requirements mentioned above. If you suspect fraud, TransUnion suggests a call to their fraud unit at 800-680-7289. It will place the temporary alert over the phone and advise the requestor of what needs to be sent to suppress the credit file and to disclose a copy of its contents. Requests can also be emailed to fvad@transunion.com .

Legal Notice

The information you obtain herein is not, nor intended to be, legal advice. We try to provide quality information but make no claims, promises or guarantees about the accuracy, completeness or adequacy of the information contained. As legal advice must be tailored to the specific circumstances of each case and laws are constantly changing, nothing provided herein should be used as a substitute for the advice of competent legal counsel.

Credit Report Request for the Deceased

Sent credit report request via (include all that apply):

☐ e-mail ☐ fax ☐ mail (certified return receipt requested no.) _____

To (Name of Company): _____

Address: _____

Other Contact Info: _____

Date of Request: _____

Your name: _____

Address: _____

Phone Number (daytime/evening/cell): _____

As the _____ (relationship to deceased), I am notifying you that the following person died.

- Name of deceased: _____
- Date of death: _____
- Date of birth: _____
- Location of birth: _____
- Social Security number of deceased: _____
- Five year address history (most current one first): _____

I would like to make the following requests:

____ I request a current copy of (name of deceased)'s credit report be mailed to me at my address listed above.

____ I request that the following notice be placed on (name of deceased)'s credit report:

"Deceased - Do not issue credit."

____ I request that the following notice also be added to this alert: "If an application is made for credit, notify the following person(s) immediately: _____

____ (list the next surviving relative, executor/trustee of the estate and/or local law enforcement agency- noting the relationship)."

Signed:

Additional Information and U.S. State Notification Requirements

There are a number of steps you should consider to guard against identity theft.

Review Your Account Statements and Credit Report: It is recommended that you remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your credit reports. Report any fraudulent transactions to the creditor or credit reporting agency from whom you received the statement or report. You may obtain a free copy of your credit report from each credit reporting agency once every 12 months, whether or not you suspect any unauthorized activity on your account, by visiting <https://www.annualcreditreport.com>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form available at that website and mailing it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You may also purchase a copy of your credit report at any time by contacting any one or more of the national credit reporting agencies listed below.

Equifax

P.O. Box 740241
Atlanta, Georgia 30374
www.equifax.com
1-800-685-1111 Credit Reports
1-888-766-0008 Fraud Alert
1-800-685-1111 Security Freeze

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
1-888-397-3742 Credit Reports
1-888-397-3742 Fraud Alert
1-888-397-3742 Security Freeze

TransUnion (FVAD)

P.O. Box 105281
Atlanta, GA 30348-5281
www.transunion.com
1-800-888-4213 Credit Reports
1-800-680-7289 Fraud Alert
1-800-680-7289 Security Freeze

Federal Trade Commission (FTC) and State Resources: General guidance on protecting yourself from identity theft is available from the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Ave. NW, Washington D.C. 20580, by phone at 877-ID-THEFT (438-4338), and/or from the FTC website at <http://www.ftc.gov/bcp/edu/microsites/idtheft>. In many states, additional information is also available from your state's Attorney General's Office.

Fraud Alerts and Security Freezes: You may obtain information about fraud alerts and security freezes (also referred to as credit freezes), including how to place a fraud alert or security freeze, from the Federal Trade Commission or credit reporting agencies at the contact information provided above. However, be aware that a fraud alert or security freeze may require fees to be paid, may interfere with or delay legitimate requests for credit approval. You'll need to supply your name, address, date of birth, Social Security number and other personal information in order to place a security freeze on your credit.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

D.C.: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the D.C. Attorney General at (202) 442-9828 or consumer.protection@dc.gov.

Iowa: You should report suspected incidents of identity theft to your local law enforcement or the Iowa Attorney General.

Maryland: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the Maryland Attorney General at 1-888-743-0023, Office of the Attorney General, 200 St. Paul Place, Baltimore, MD 21202, and <https://www.marylandattorneygeneral.gov>.

New Mexico: You have the right to place a fraud alert or security freeze. For more information on how to place a fraud alert or security freeze, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You should review your personal account statements and credit reports, as applicable, to detect any errors that may or may not be a result of a security incident.

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

North Carolina: For more information on steps you can take to prevent identity theft, you can contact the Federal Trade Commission or any of the consumer reporting bureaus as described above. You can also contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

Rhode Island: You can also contact the Rhode Island Attorney General at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.