

VITAS[®] Healthcare

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line

<<Full Name>>
<<Address 3>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

NOTICE OF DATA BREACH

<<Date>>

Dear <<Full Name>>,

VITAS Hospice Services, LLC (“VITAS”) is writing to inform you of a data security incident involving some of your personal information. This letter provides you with details about the incident, steps we are taking in response, and resources available to help you protect against potential misuse of your information.

What Happened? On October 24, 2025, VITAS discovered that an unauthorized party had compromised the account of one of our vendors and used that account to gain access to some of our systems. Upon discovering this incident, VITAS promptly took action to secure our systems, launched an internal investigation, and engaged outside experts to assist with our investigation and response. The investigation determined that the unauthorized party accessed certain VITAS systems between approximately September 21 and October 27, 2025. In the course of that activity, the unauthorized party was able to access and download personal information about some of our patients and former patients, including certain personal information about you.

What Information Was Involved? The affected data varies by individual and may include your: <<Breached Elements>><<Variable Data 1>>.

What We Are Doing. We take this matter very seriously and have taken additional steps to reduce the risk of a similar incident occurring in the future. We are working with a leading cybersecurity firm to assist with our investigation and analysis, and we are reviewing and strengthening our vendor oversight and data protection protocols. We also notified law enforcement of this incident. Our notification to you has not been delayed due to a law enforcement investigation.

As of the date of this letter, we are unaware of any misuse of your personal information as a result of this incident. Nevertheless, as a precaution to help you protect your identity, we have arranged for complimentary credit monitoring and identity protection services for 24 months through Epiq. These services begin on the date of this notice and are available to you at no cost. Instructions on how to enroll in these services are enclosed.



What You Can Do. Please review the “Further Steps You Can Take to Protect Your Information” enclosed with this letter for additional actions you can take to protect your information. We also encourage you to enroll in the complimentary Epiq services described in this letter.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 855-403-1586, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding U.S. holidays.

At VITAS, we are deeply committed to protecting your privacy and supporting you and your family with the same compassion and care that defines everything we do.

Thank you for your understanding. Please note that we will not send any electronic communications regarding this incident and ask that you do not share personal information electronically.

Sincerely,

VITAS Hospice Services



<<Full Name>>

Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Coverage Length: 24 Months

Epiq - Privacy Solutions ID

1B Credit Monitoring + Medical Monitoring

How To Enroll:

- 1) Visit www.privacysolutionsid.com and click "Activate Account"
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Enter your log-in credentials
- 6) You will be directed to your dashboard and activation is complete!

Product Features:

1-Bureau Credit Monitoring with Alerts

Monitors your credit file(s) for key changes, with alerts such as credit inquiries, new accounts, and public records.

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Detect and prevent common identity theft events outside of what is on your credit report. Real-time monitoring of SSNs across situations like loan applications, employment and healthcare records, tax filings, online document signings and payment platforms, with alerts.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Change of Address Monitoring

Monitors the National Change of Address (NCOA) database and the U.S. Postal Service records to catch unauthorized changes to users' current or past addresses.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

Up to \$1M Identity Theft Insurance¹

Provides up to \$1,000,000 (\$0 deductible) Identity Theft Event Expense Reimbursement Insurance on a discovery basis. This insurance aids in the recovery of a stolen identity by helping to cover expenses normally associated with identity theft.

Unauthorized Electronic Funds Transfer- UEFT¹

Provides up to \$1,000,000 (\$0 deductible) Unauthorized Electronic Funds Transfer Reimbursement. This aids in the recovery of stolen funds resulting from fraudulent activity (occurrence based).

Healthcare Insurance Plan ID Monitoring & Medicare Beneficiary Identifier ID Monitoring

Monitors the dark web for exposed registered healthcare, dental, vision, and prescription plan IDs. Monitors the dark web for exposed Medicare Beneficiary Identifier ID numbers.

Medical Record Number Monitoring

Alerts when a Medical Record Number has been detected on the dark web, which could potentially expose permanent medical and health records from providers, hospitals, and urgent care centers.

International Classification of Disease Monitoring

Monitors the dark web for exposed medical information - and notifies users if their PII is exposed along with ICD (disease) codes.

National Provider Identifier Monitoring

Monitor NPI numbers (for healthcare professionals) on the dark web to detect unauthorized usage or exposures.

Health Savings Account Monitoring

Monitors the dark web for exposed HSA account information.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID 1B Credit Monitoring + Medical Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

¹ Identity Theft Insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. or American Bankers Insurance Company of Florida, an Assurant company. 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.

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact each one of the three national credit reporting agencies (contact information below).

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: A security freeze will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (<https://www.identitytheft.gov/>) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. You may be able to locate contact information for your state attorney general here: <https://www.naag.org/find-my-ag/>.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Oregon Attorney General

100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
<https://www.doj.state.or.us/consumer-protection/>
1-877-877-9392

Office of the Attorney General for the District of Columbia

400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
<https://oag.dc.gov>

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Contact Information for Credit Reporting Agencies:

	Equifax	Experian	TransUnion
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert

VITAS[®] Healthcare

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
Family Member of
<<Full Name>>
<<Address 3>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

NOTICE OF DATA BREACH

<<Date>>

Dear Family Member of <<Full Name>>,

VITAS Hospice Services, LLC (“VITAS”) is writing to inform you of a data security incident involving some personal information about your family member listed above. This letter provides you with details about the incident, steps we are taking in response, and resources available to help you protect your family member’s information against potential misuse.

What Happened? On October 24, 2025, VITAS discovered that an unauthorized party had compromised the account of one of our vendors and used that account to gain access to some of our systems. Upon discovering this incident, VITAS promptly took action to secure our systems, launched an internal investigation, and engaged outside experts to assist with our investigation and response. The investigation determined that the unauthorized party accessed certain VITAS systems between approximately September 21 and October 27, 2025. In the course of that activity, the unauthorized party was able to access and download personal information about some of our patients and former patients, including certain personal information about your family member.

What Information Was Involved? The affected data varies by individual and may include your family member’s: <<Breached Elements>><<Variable Data 1>>.

What We Are Doing. We take this matter very seriously and have taken additional steps to reduce the risk of a similar incident occurring in the future. We are working with a leading cybersecurity firm to assist with our investigation and analysis, and we are reviewing and strengthening our vendor oversight and data protection protocols. We also notified law enforcement of this incident. Our notification to you has not been delayed due to a law enforcement investigation.

As of the date of this letter, we are unaware of any misuse of your family member’s personal information as a result of this incident. Nevertheless, as a precaution to help you protect your family member’s identity, we have arranged for complimentary credit monitoring and identity protection services for 24 months through Epiq. These services begin on the date of this notice and are available to you at no cost. Instructions on how to enroll in these services are enclosed.



What You Can Do. Please review the “Further Steps You Can Take to Protect Your Family Member’s Information” enclosed with this letter for additional actions you can take to protect your family member’s information. We also encourage you to enroll in the complimentary Epiq services described in this letter.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 855-403-1586, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding U.S. holidays.

At VITAS, we are deeply committed to protecting your family member’s privacy and supporting you and your family with the same compassion and care that defines everything we do.

Thank you for your understanding. Please note that we will not send any electronic communications regarding this incident and ask that you do not share personal information electronically.

Sincerely,

VITAS Hospice Services



<<Full Name>>
Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>
Coverage Length: 24 Months

Epiq - Privacy Solutions ID Minor Monitoring

Important Enrollment Instructions for Parents and Guardians

A parent/guardian must establish an Epiq Privacy Solutions ID account on behalf of the minor(s) being monitored. The parent/guardian will need an email address and provide additional information on the enrollment form and answers to the verification questions. Once the enrollment is complete, the parent/guardian will be able to add up to 10 minors' information to be monitored.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID Minor Monitoring, please call directly at **866.675.2006**.

How To Enroll:

- 1) Parent/Guardian visit www.privacysolutionsid.com and click “Activate Account”
- 2) Enter the following activation code, <<Activation Code>> and complete the enrollment form
- 3) Parent/Guardian complete the identity verification process
- 4) You will receive a separate email from noreply@privacysolutions.com confirming your account has been set up successfully and will include an Access Your Account link in the body of the email that will direct you to the log-in page
- 5) Parent/Guardian enter your log-in credentials
- 6) Parent/Guardian select “Monitored Information” on the Dashboard
- 7) Parent/Guardian add the minor(s) information (i.e. SSN, Passport ID, Bank Account Numbers, Debit Card Numbers, Driver's License Number, Email, Medical ID, Phone Number)
- 8) Activation is complete!

Product Features:

SSN Monitoring (High Risk Transaction Monitoring, Real-Time Authentication Alerts, Real-Time Inquiry Alerts)

Monitors for the minor's SSN being used in combination with a credit file to fraudulently complete loan applications, open/enroll in new financial accounts, or engage in other high-risk transactions.

Dark Web Monitoring

Scans millions of servers, online chat rooms, message boards, and websites across all sides of the web to detect fraudulent use of your personal information, with alerts.

Credit Protection

3-Bureau credit security freeze assistance with blocking access to the credit file for the purposes of extending credit (with certain exceptions).

Identity Restoration & Lost Wallet Assistance

Dedicated ID restoration specialists who assist with ID theft recovery and assist with canceling and reissuing credit and ID cards.

If you need assistance with the enrollment process or have questions regarding Epiq – Privacy Solutions ID Minor Monitoring, please call directly at **866.675.2006**, Monday-Friday 9:00 a.m. to 5:30 p.m., ET.

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR FAMILY MEMBER'S INFORMATION

Review Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your family member's account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your family member's credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact each one of the three national credit reporting agencies (contact information below).

Fraud Alert: You may want to consider placing a fraud alert on your family member's credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your family member's name. To place a fraud alert on a credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: A security freeze will prevent new credit from being opened in your family member's name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your family member's credit report without consent. As a result, using a security freeze may interfere with or delay the ability to obtain credit. You must separately place a security freeze on your family member's credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies your family member, including full name, Social Security number, date of birth, current and previous addresses, a copy of a state-issued identification card, and a recent utility bill, bank statement or insurance statement. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (<https://www.identitytheft.gov/>) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. You may be able to locate contact information for your state attorney general here: <https://www.naag.org/find-my-ag/>.

Federal Trade Commission
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

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

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Oregon Attorney General
100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
<https://www.doj.state.or.us/consumer-protection/>
1-877-877-9392

Office of the Attorney General for the District of Columbia
400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
<https://oag.dc.gov>

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Contact Information for Credit Reporting Agencies:

	Equifax	Experian	TransUnion
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert

VITAS[®] Healthcare

Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

Postal Endorsement Line
Family Member of
<<Full Name>>
<<Business or Representative Name>>
<<Address 3>>
<<Address 1>>
<<Address 2>>
<<City>>, <<State>> <<Zip>>
<<Country>>
***Postal IMB Barcode

NOTICE OF DATA BREACH

<<Date>>

Dear Family Member of <<Full Name>>,

VITAS Hospice Services, LLC (“VITAS”) is writing to inform you of a data security incident involving some personal information about your family member listed above. This letter provides you with details about the incident, steps we are taking in response, and resources available to help you protect your family member’s information against potential misuse.

What Happened? On October 24, 2025, VITAS discovered that an unauthorized party had compromised the account of one of our vendors and used that account to gain access to some of our systems. Upon discovering this incident, VITAS promptly took action to secure our systems, launched an internal investigation, and engaged outside experts to assist with our investigation and response. The investigation determined that the unauthorized party accessed certain VITAS systems between approximately September 21 and October 27, 2025. In the course of that activity, the unauthorized party was able to access and download personal information about some of our patients and former patients, including certain personal information about your family member.

What Information Was Involved? The affected data varies by individual and may include your family member’s: <<Breached Elements>><<Variable Data 1>>.

What We Are Doing. We take this matter very seriously and have taken additional steps to reduce the risk of a similar incident occurring in the future. We are working with a leading cybersecurity firm to assist with our investigation and analysis, and we are reviewing and strengthening our vendor oversight and data protection protocols. We also notified law enforcement of this incident. Our notification to you has not been delayed due to a law enforcement investigation.

What You Can Do. You can place a deceased alert at one of the three major credit bureaus to help prevent misuse of your family member’s personal information. A deceased alert tells creditors to follow certain procedures, including contacting you. It is necessary to contact only one bureau to provide notification. As soon as one of the three bureaus confirms your deceased alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail. You also may inform the Social Security Administration of your family member’s passing by calling 800.772.1213 or visiting ssa.gov.

VITAS[®]

Healthcare

Please review the “Further Steps You Can Take to Protect Your Family Member’s Information” enclosed with this letter for additional actions you can take to protect your family member’s information and for contact information for the major credit bureaus. As of the date of this letter, we are unaware of any misuse of your family member’s personal information as a result of this incident.

For More Information: Should you have additional questions or concerns regarding this matter, please do not hesitate to contact our dedicated call center agents at 855-403-1586, Monday through Friday, between 9:00 a.m. and 9:00 p.m. Eastern Time, excluding U.S. holidays.

At VITAS, we are deeply committed to protecting your family member’s privacy and supporting you and your family with the same compassion and care that defines everything we do.

Thank you for your understanding. Please note that we will not send any electronic communications regarding this incident and ask that you do not share personal information electronically.

Sincerely,

VITAS Hospice Services

FURTHER STEPS YOU CAN TAKE TO PROTECT YOUR FAMILY MEMBER'S INFORMATION

Review Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your family member's account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may be able to obtain a free copy of your family member's credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>. You also can contact each one of the three national credit reporting agencies (contact information below).

Fraud Alert: You may want to consider placing a fraud alert on your family member's credit report. An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your family member's name. To place a fraud alert on a credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: A security freeze will prevent new credit from being opened in your family member's name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your family member's credit report without consent. As a result, using a security freeze may interfere with or delay the ability to obtain credit. You must separately place a security freeze on your family member's credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies your family member, including full name, Social Security number, date of birth, current and previous addresses, a copy of a state-issued identification card, and a recent utility bill, bank statement or insurance statement. Under federal law, you may not be charged to place or remove a credit freeze.

Police Report: If you file a police report, you have the right to obtain a copy of it.

Additional Free Resources on Identity Theft: You can obtain information from the consumer reporting agencies, FTC (<https://www.identitytheft.gov/>) or from your respective state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the Federal Trade Commission or to the Attorney General in your state. You may want to contact your state Attorney General to obtain further information. You may be able to locate contact information for your state attorney general here: <https://www.naag.org/find-my-ag/>.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

New York Attorney General

Office of the Attorney General
The Capitol
Albany, NY 12224-0341
<https://ag.ny.gov/>
1-800-771-7755

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Oregon Attorney General

100 SW Market Street
First Floor
Tilikum Room
Portland, OR 97201
<https://www.doj.state.or.us/consumer-protection/>
1-877-877-9392

Office of the Attorney General for the District of Columbia

400 6th Street NW
Washington, D.C. 20001
oag@dc.gov
<https://oag.dc.gov>

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
Main number: 410-576-6300
Toll-free: 1-888-743-0023
Consumer Hotline: 410-528-8662

Contact Information for Credit Reporting Agencies:

	Equifax	Experian	TransUnion
To obtain a copy of your credit report	P.O. Box 740241 Atlanta, GA 30374 (866) 349-5191 www.equifax.com	P.O. Box 4500 Allen, TX 75013 (888) 397-3742 www.experian.com	P.O. Box 1000 Chester, PA 19016 (800) 888-4213 www.transunion.com
To obtain a security freeze	PO Box 105788 Atlanta, GA 30348 (800) 685-1111 www.equifax.com/personal/credit-report-services	PO Box 9554 Allen, TX 75013 (888) 397-3742 www.experian.com/freeze/center.html	P.O. Box 2000 Chester, PA 19016 (888) 909-8872 www.transunion.com/credit-freeze
To place a fraud alert	P.O. Box 105069 Atlanta, GA 30348 (888) 766-0008 www.equifax.com/personal/credit-report-services	P.O. Box 2002 Allen, TX 75013 (888) 397-3742 www.experian.com/fraud/center.html	P.O. Box 2000 Chester, PA 19016 (800) 680-7289 www.transunion.com/fraud-victim-resource/place-fraud-alert