

**BakerHostetler**

**Baker&Hostetler LLP**

999 Third Avenue  
Suite 3600  
Seattle, WA 98104-4040

T 206.332.1380  
F 206.624.7317  
www.bakerlaw.com

Randal L. Gainer  
direct dial: 206.332.1381  
rgainer@bakerlaw.com

**RECEIVED**

**SEP 19 2017**

**CONSUMER PROTECTION**

September 18, 2017

**Via Overnight Mail**

Joseph Foster  
Office of the Attorney General  
33 Capitol Street  
Concord, New Hampshire 03301

*Re: Incident Notification*

Dear Attorney General Foster:

I am writing on behalf of our client, TRUEbenefits LLC, to notify you of a security incident involving New Hampshire residents. TRUEbenefits is an insurance brokerage company that provides employee benefit insurance procurement, consultation, and support services for its client employers and health plans.

On May 19, 2017, a phishing email was sent from the email account of an employee of TRUEbenefits without the employee's knowledge. When TRUEbenefits determined that the email was sent illegitimately to perpetuate the phishing scheme, the company immediately secured the employee's email account, began an investigation, and engaged a leading forensic firm. After conducting a thorough review of the employee's email account, TRUEbenefits determined on June 26, 2017, that an unauthorized person had access to the employee's email account and that some of the emails accessible through the account contained the names of clients' employees and/or plan members, together with the Social Security numbers of some employees and/or plan members, as well as member support services information for some employees and/or plan members. The membership support services information that was potentially accessible included health insurance numbers, claims information, dates of service, provider names, diagnoses or treatment information, explanation of benefits forms, invoice amounts, or invoice statements.

On June 30, 2017, TRUEbenefits began notifying certain clients of the incident pursuant to contractual obligations with those clients. TRUEbenefits initially notified the clients by phone and later in writing. TRUEbenefits also engaged a forensic firm to perform the time-consuming process of identifying all potentially affected individuals and their corresponding employers. TRUEbenefits provided written notification to all of its clients with potentially affected

Atlanta Chicago Cincinnati Cleveland Columbus Costa Mesa Denver  
Houston Los Angeles New York Orlando Philadelphia Seattle Washington, DC

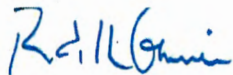
employees by August 14, 2017. For each client, TRUEbenefits offered to provide notifications to the potentially affected employees, as well as complimentary credit monitoring services, call center services, and required regulator notifications.

On August 14, 2017, TRUEbenefits began mailing written notifications to individuals whose employers had responded affirmatively to TRUEbenefits' offer. However, none of the notified individuals were New Hampshire residents until the final set of mailings were sent on September 13th-18th. There are a total of ten (10) New Hampshire residents who were notified of the incident in writing in accordance with N.H. Rev. Stat. Ann. § 359-C:20 in substantially the same form as the enclosed letters.<sup>1</sup> TRUEbenefits is offering the potentially affected individuals a complimentary two-year membership in credit monitoring and identity theft protection services from Experian. TRUEbenefits has also provided a telephone number for potentially affected individuals to call with any questions they may have. TRUEbenefits provided notice to the individuals as soon as possible and without unreasonable delay after TRUEbenefits received affirmative responses from the individuals' employers to TRUEbenefits' offer to send notifications to the individuals.

To help prevent something like this from happening in the future, TRUEbenefits has conducted additional training and education for its employees regarding phishing emails, enhanced email security, and amended email retention policies.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Randal L. Gainer  
Partner

Enclosures

---

<sup>1</sup> This report is not, and does not constitute, a waiver of TRUEbenefits' objection that New Hampshire lacks personal jurisdiction regarding the company related to this matter.



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

<<MailID>>  
 <<Name 1>>  
 <<Name 2>>  
 <<Address 1>>  
 <<Address 2>>  
 <<Address 3>>  
 <<Address 4>>  
 <<Address 5>>  
 <<City>><<State>><<Zip>>  
 <<Country>> <<Date>>

Dear <<Name 1>>:

TRUEbenefits LLC is an insurance brokerage company that provides employee benefit insurance procurement, consultation, and support services for its client employers and health plans. TRUEbenefits understands the importance of protecting personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your personal information, which was provided to TRUEbenefits for services that we provided to <<Client>>. <<Rhode Island>>This notice explains the incident, measures we have taken, and some steps you can take in response.

A phishing email was sent from the email account of an employee of TRUEbenefits on May 19, 2017, without the employee's knowledge. When we determined that the email was sent illegitimately to perpetuate the phishing scheme, we immediately secured the employee's email account, began an investigation, and engaged a leading forensic firm. We conducted a thorough review of the employee's email account and determined on June 26, 2017, that an unauthorized person had access to the employee's email account and some of the emails may have contained your name<<Variable Data 1 and Social Security number.>><<Variable Data 2 , Social Security number, and member support services information, which may have included a health insurance number, claims information, date of service, provider name, diagnoses or treatment information, explanation of benefits, invoice amount, or invoice statement. >><<Variable Data 3 and member support services information, which may have included a health insurance number, claims information, date of service, provider name, diagnoses or treatment information, explanation of benefits, invoice amount, or invoice statement. A Social Security number and financial information were not included with the information.>>

We have no indication that the information in the emails was actually viewed or has been used in any way. However, out of an abundance of caution, we are offering a complimentary two-year membership of Experian's® IdentityWorks<sup>SM</sup> Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks Credit 3B is completely free to you and enrolling in this program will not hurt your credit score. For more information on identity theft prevention and IdentityWorks Credit 3B, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter. We recommend that you regularly review the explanation of benefits received from your health insurer. If you see services that you did not receive, please contact the insurer immediately.

We sincerely regret that this incident occurred and apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have conducted additional training and education for our employees regarding phishing emails, enhanced email security, and amended email retention policies. If you have any questions or want clarification on what information may have been accessible, please call 1-888-457-2326, Monday through Friday between 6 a.m. and 6 p.m. Pacific Time.

Sincerely,

A handwritten signature in black ink, appearing to read 'Grant McDonald', with a stylized flourish at the end.

Grant McDonald  
Privacy Officer & Managing Principal

## Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: [www.experianidworks.com/3bcredit2](http://www.experianidworks.com/3bcredit2)
3. PROVIDE the **Activation Code**: <<Enrollment 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 877-288-8057. Be prepared to provide engagement number <<Engagement Number>> as proof of eligibility for the identity restoration services by Experian.

### ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

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

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

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

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.\*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your membership today at [www.experianidworks.com/3bcredit2](http://www.experianidworks.com/3bcredit2)  
or call 877-288-8057 to register with the activation code above.**

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

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

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

## **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 (toll free when calling within Maryland) (410) 576-6300 (for calls originating outside Maryland)

*Office of the Attorney General*, One Ashburton Place, Boston, MA 02108, 1-508-990-9700, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400

*Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 401-274-4400

**If you are a resident of Massachusetts or Rhode Island**, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of any police report.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)

**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)

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

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

The credit reporting agencies 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 in order 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 identity 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 your 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 your request to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, 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](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like 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're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

**TRUEbenefits** LLC

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

<<MailID>>

The Parent or Guardian of

<<Name 1>>

<<Name 2>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<Address 4>>

<<Address 5>>

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

<<Country>>

<<Date>>

Dear Parent or Guardian of <<Name 1>>:

TRUEbenefits LLC is an insurance brokerage company that provides employee benefit insurance procurement, consultation, and support services for its client employers and health plans. TRUEbenefits understands the importance of protecting personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your child's personal information, which was provided to TRUEbenefits for services that we provided to <<client>>. <<Rhode Island>>This notice explains the incident, measures we have taken, and some steps you can take in response.

A phishing email was sent from the email account of an employee of TRUEbenefits on May 19, 2017, without the employee's knowledge. When we determined that the email was sent illegitimately to perpetuate the phishing scheme, we immediately secured the employee's email account, began an investigation, and engaged a leading forensic firm. We conducted a thorough review of the employee's email account and determined on June 26, 2017, that an unauthorized person had access to the employee's email account and some of the emails may have contained your child's name<<Variable Data 1 and Social Security number.>><<Variable Data 2 , Social Security number, and member support services information, which may have included a health insurance number, claims information, date of service, provider name, diagnoses or treatment information, explanation of benefits, invoice amount, or invoice statement. >><<Variable Data 3 and member support services information, which may have included a health insurance number, claims information, date of service, provider name, diagnoses or treatment information, explanation of benefits, invoice amount, or invoice statement. A Social Security number and financial information were not included with the information.>>

Out of an abundance of caution, we are offering a complimentary two-year membership of Experian IdentityWorks<sup>SM</sup> Minor Plus. This product provides you with internet surveillance of your minor's personal information. In addition, IdentityWorks Minor Plus will tell you if your child has a credit report, a potential sign that his or her identity has been stolen. For more information on identity theft prevention and IdentityWorks Minor Plus, including instructions on how to activate your complimentary two-year membership, please see the additional information provided in this letter. We recommend that you regularly review the explanation of benefits received from your child's health insurer. If you see services that your child did not receive, please contact the insurer immediately.

We sincerely regret that this incident occurred and apologize for any inconvenience or concern this may cause you. To help prevent something like this from happening in the future, we have conducted additional training and education for our employees regarding phishing emails, enhanced email security, and amended email retention policies. If you have any questions or want clarification on what information may have been accessible, please call 1-888-457-2326, Monday through Friday between 6 a.m. and 6 p.m. Pacific Time.

Sincerely,



Grant McDonald  
Privacy Officer & Managing Principal



## Activate Experian IdentityWorks Minor Plus Now in Four Easy Steps

1. ENROLL by: <<Enrollment Deadline>> (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks** website to enroll: [www.experianidworks.com/minorplus2](http://www.experianidworks.com/minorplus2)
3. PROVIDE the **Activation Code**: <<Enrollment Code>> and the parent's/guardian's information
4. PROVIDE your minor's information when prompted

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

### **ADDITIONAL DETAILS REGARDING THE 24-MONTH EXPERIAN IDENTITYWORKS MINOR PLUS MEMBERSHIP:**

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

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

Once you enroll your minor in Experian IdentityWorks, you can access the following additional features:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of the minor's personal information on the Dark Web.
- **Experian IdentityWorks ExtendCARE™:** Receive the same high-level of Identity Restoration support even after the Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**Activate your minor's membership today at [www.experianidworks.com/minorplus2](http://www.experianidworks.com/minorplus2) or call 877-288-8057 to register with the activation code above.**

**What you can do to protect your minor's information:** There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your minor's account(s). Please refer to [www.ExperianIDWorks.com/restoration](http://www.ExperianIDWorks.com/restoration) for this information.

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

## **MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

Even if you choose not to take advantage of this free credit monitoring, we recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

*Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

*Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

*TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

*Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

**If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island**, you may contact and obtain information from your state attorney general at:

*Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, [www.ct.gov/ag](http://www.ct.gov/ag)

*Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023 (toll free when calling within Maryland)  
(410) 576-6300 (for calls originating outside Maryland)

*Office of the Attorney General*, One Ashburton Place, Boston, MA 02108, 1-508-990-9700, [www.mass.gov/ago/contact-us.html](http://www.mass.gov/ago/contact-us.html)

*North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400

*Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 401-274-4400

**If you are a resident of Massachusetts or Rhode Island**, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of any police report.

**Fraud Alerts:** There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

**Credit Freezes:** You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally \$5 to \$20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

**Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)  
**Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)  
**TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)

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

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

The credit reporting agencies 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 in order 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 identity 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 your 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 your request to remove the security freeze.

**Fair Credit Reporting Act:** You also have rights under the federal Fair Credit Reporting Act, 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](http://www.ftc.gov/credit). The FTC's list of FCRA rights includes:

- You have the right to receive a copy of your credit report. The copy of your report must contain all the information in your file at the time of your request.
- Each of the nationwide credit reporting companies – Equifax, Experian, and TransUnion – is required to provide you with a free copy of your credit report, at your request, once every 12 months.
- You are also entitled to a free report if a company takes adverse action against you, like 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're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; if you're on welfare; or if your report is inaccurate because of fraud, including identity theft.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited. And you must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.