353 N. CLARK STREET CHICAGO, IL 60654-3456

JENNER&BLOCK LLP

August 20, 2019

David Saunders
Tel +1 312 923 8388
DSaunders@jenner.com

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Courtesy Data Issue Notification

Dear Attorney General MacDonald:

I am writing on behalf of Alight Solutions LLC ("Alight" or the "Company"), as third-party provider to each of the Federal Reserve Banks[1] (the "Federal Reserve"), to provide you with a courtesy notification of an inadvertent disclosure involving the personal information of 46 New Hampshire residents. By providing this notice, the Company does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Alight is an Illinois-based company, headquartered at 4 Overlook Point, Lincolnshire, IL 60069, that provides certain benefits administration and cloud-based HR services to the Federal Reserve. In that role, the Company collects certain information from the Federal Reserve and their benefit plan participants (the "Participants") in order to deliver these services.

On May 20, 2019, in connection with a routine Federal Reserve security review, Alight became aware of two issues involving the inadvertent use of Participants' personal information. First, the Company became aware that starting on September 22, 2014, system-generated emails from its SmartBenefits website were sent to individual Participants confirming changes they made to their online benefits account. System-generated emails were also sent to some individual Participants to follow up on open cases with the Federal Reserve Benefits Center, which is a customer service center operated by Alight. In both situations, those communications inadvertently included unencrypted, individual Participants' personal data in the properties of the email. Specifically, these system-generated emails included Participants' Social Security Numbers within the e-mail properties amidst a longer string of numbers. These numbers were not visible in the subject or body of the email. The Participants' personal information was included in the e-mail properties for purposes of tracking and recording communications with the Participant. Additionally, based on our investigation to date, the Company has determined the system-generated emails were sent to the correct Participant. The Company has no indication

[1]The Federal Reserve has asked us to convey that: Federal Reserve Banks are federal instrumentalities chartered by the U.S. Congress under the Federal Reserve Act of 1913 (12 U.S.C. § 221 et. seq.). As federal instrumentalities engaged in federal activities, they are not subject to state regulation unless Congress has explicitly authorized that regulation.

that any Participant personal information has been misused by any unauthorized individuals as a result of this issue.

Second, in that same review, the Company became aware that, as an unintended result of a system modification, from October 1, 2016 to February 22, 2019, URLs linking the SmartBenefits website – via encrypted transmission – to two (2) trusted third-party websites, also providing benefits services to Participants, included individual Participants' Social Security Numbers and date of birth. While the URL was sent encrypted, this information may have been inadvertently stored in an un-encrypted form on a device used by a Participant to access the SmartBenefits website; for example, if the information were saved in the Participant's web browser's cache.

Upon learning of these situations, Alight promptly initiated an investigation and addressed these issues by encrypting Social Security Numbers in the email properties of both forms of system-generated emails and removing personal information from the URLs linking SmartBenefits to the trusted third-parties. Both of these actions were completed by June 29, 2019.

Out of an abundance of caution, the Company is informing you and the affected Participants of these issues. Commencing on or about August 26, 2019, the Company is providing the affected Participants with a written notification of these issues in substantially the same form as the attached letters. Also out of an abundance of caution, the notified Participants will receive two years of complimentary identity theft protection services through InfoArmor; information on the process for placing a fraud alert and/or security freeze on their credit files at no cost to the participant; obtaining free credit reports; and the contact information for the consumer reporting agencies and the Federal Trade Commission. Notification to you and the notified Participants was delayed as the Company worked with the Federal Reserve to determine the scope of these inadvertent disclosures.

Protecting the privacy of personal information is a top priority for Alight. Alight is committed to maintaining the privacy of personal information in its possession and has taken many precautions to safeguard it. Alight continually evaluates and modifies its practices and internal controls to enhance the security and privacy of personal information.

Alight regrets this issue, and is committed to ensuring that personal information remains protected. If you have any questions, please contact me at 312 923-8388 or dsaunders@jenner.com.

Sincerely,

David Saunders

Enclosures

ENCLOSURE 1

Template letter to Participants subject to e-mail issue only

alight

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice Regarding Your Online Benefits Account

Dear <<First Name>>,

We are contacting you with important information regarding your Federal Reserve benefits account. Alight Solutions LLC ("Alight" or "we"), which administers the Federal Reserve Benefits Center, SmartBenefits website and your SmartBenefits online account on behalf of the Federal Reserve, recently discovered and addressed an incident involving your personal information. There is no indication that your personal information has been misused by any unauthorized parties, and we believe the risk of harm to you or your information is minimal. However, in an abundance of caution, we are writing to keep you fully informed.

This letter contains information about the personal information that was involved, how it has been used, the services that are being made available to you, and what you can do; please read it carefully.

What Happened?

On May 20, 2019, in connection with a routine Federal Reserve security review, we became aware of an issue involving your personal information.

Starting on September 22, 2014, system-generated emails from the SmartBenefits website were sent to individual participants confirming changes they made to their SmartBenefits online account. Federal Reserve Benefits Center system-generated emails were also sent to some individual participants to follow up on open cases with the Federal Reserve Benefits Center. Those communications inadvertently included your Social Security Number in the properties of the email. This information, which was used as an internal identifier for account tracking and customer service, was not included in the subject line or body of any email, and only included information pertinent to the recipient. You may have received at least one such email, sent via an unencrypted transmission, during the period from September 22, 2014 through June 29, 2019.

What Information Was Involved?

The system-generated emails described above included your Social Security Number within the properties of the email. This information, which was used as an internal identifier for account tracking and customer service, was not included in the email subject line or body and was only sent to you.

What Are We Doing?

Upon learning of the situation, Alight initiated an investigation and promptly addressed the issue by encrypting Social Security Numbers in the email properties of both forms of system-generated emails. Encryption of emails was completed in June 2019.

Further, in an abundance of caution, and at no cost to you, we are offering you two years of identity theft protection through InfoArmor, a leading provider of employer-sponsored identity theft protection. Please review the Other Important Information attached to this letter for instructions on how to enroll with

InfoArmor's PrivacyArmor service, which includes identity theft protection, continuous identity monitoring and credit monitoring. If you wish to continue receiving the service after expiration, you will be responsible for payment at a rate negotiated by the Federal Reserve.

What Can You Do?

Based on our investigation, there is no indication that your personal information has been misused by any unauthorized parties, and we believe the risk of harm to you is minimal. However, we recommend you take the following steps:

- Delete any automated confirmation or open case follow-up emails you received from SmartBenefits and/or the Federal Reserve Benefits Center prior to June 29, 2019 from your inbox, archives or sent folders. If you would like to retain a record of these emails, you should consider printing the emails.

- Activate identity theft protection services, at no cost to you, by contacting InfoArmor. For more information on these services, review the attached information or go to www.infoarmor.com/IDProtect or call 1-866-724-5798.

The attachment to this letter also describes other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, at no cost to you, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We regret any inconvenience that this may cause you. We are committed to maintaining the privacy and security of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Need More Information?

If you have more questions, please call 1-866-279-8289, 8 a.m. – 6 p.m. Eastern time, Monday through Friday, to speak with a dedicated benefits specialist specifically trained on this issue. For your state's TTY/TDD number for the hearing impaired, dial 711. If you are calling from an international location, the phone number for the Benefits Center is +1-704-646-8917.

– OTHER IMPORTANT INFORMATION –

1. **Activate your ID Theft Protection with Credit Monitoring at No Cost to You:**

   Activate Now in Three Easy Steps

   1. VISIT www.infoarmor.com/IDprotect or call 1-866-724-5798 and provide the activation code to InfoArmor's Privacy Advocate.
   2. CLICK on the Enroll Now button online.
   3. ENTER the **Activation Code**: **<<Code>>**

   If you currently are paying for InfoArmor's PrivacyArmor services and want to consider taking advantage of the 24-month membership at no cost, contact a Privacy Advocate at 1-866-724-5798 to explain the differences in coverage and to assist you in transitioning to the no-cost option. Coverage will end on September 1, 2021.

   ADDITIONAL DETAILS REGARDING YOUR PRIVACYARMOR MEMBERSHIP:

   A credit card is **not** required for activation, however additional information, such as: name, address, date of birth, Social Security Number and contact information are required to activate your account and begin proactive identity theft and credit monitoring. Activating this membership will help to uncover and resolve misuse of personal information early.

   Once you activate your PrivacyArmor coverage, you will have access to the following additional features and more:

   - **Identity and Credit Monitoring** – Actively monitors for the most damaging types of fraud.
   - **Credit Alerts and Scores** - Alerts on transactions like new inquiries, accounts in collections, new accounts and bankruptcy filings. Alerts and scores are provided by TransUnion.
   - **Dark Web Monitoring** – Artificial Intelligence bots and human intelligence operatives scan closed hacker forums for compromised credentials and IP addresses.
   - **Financial Activity Monitoring** - Alerts are triggered from sources such as bank accounts, credit and debit cards, 401(k)s, and other investment accounts.
   - **Digital Exposure Reports** - Enables members to see what personal information is publicly available on the internet.
   - **Full-service and Pre-existing Condition Remediation** – Trained advocates can help restore a member's identity regardless of when or how the damage occurred, including pre-existing fraudulent activity.
   - **$1 Million Identity Theft Insurance** – Reimburses members' out-of-pocket costs in the event they are a victim of fraud.

   Activate your membership at any time at www.infoarmor.com/IDprotect or call 1-866-724-5798 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.infoarmor.com/IDprotect for more information. If you have any questions about your PrivacyArmor coverage or suspect that an item on your credit report may be fraudulent, please contact InfoArmor's Privacy Advocates at 1-866-724-5798.

2. **As Always, Keep Your SmartBenefits Account and Information Safe By:**

   - Updating security software on each device you use to access your accounts.
   - Using a private device and a protected wireless connection (for example, connecting through a VPN or using password-protected Wi-Fi) when accessing your benefits information.

- Using a strong, unique password for your SmartBenefits account that you don't use for any other account or website.
- Not saving your logon information on any device.
- Not sharing your account access or logon information with anyone, including friends and family.
- Updating your contact information by calling the Benefits Center or by logging on to the SmartBenefits website. Then, make sure to sign up online for mobile text alerts.
- Visiting Alight's new Security Center, accessible as a footnote at the bottom of the SmartBenefits website, to find the latest industry guidance on what you should do to keep your data secure. You can also learn about the Alight Protection Program and what you need to do to be covered.

3. **Placing a Fraud Alert on Your Credit File:**

Whether or not you choose to activate this 24-month service, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

4. **Consider Placing a Security Freeze on Your Credit File:**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit-reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit-reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security Number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze ***prior*** to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

5. **Obtaining a Free Credit Report:**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

6. **Additional Helpful Resources:**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 1-515-281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 1-877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903; 1-401-274-4400; http://www.riag.ri.gov.

ENCLOSURE 2

Template letter to Participants subject to e-mail and URL issues

alight

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Notice Regarding Your Online Benefits Account

Dear <<First Name>>,

We are contacting you with important information regarding your Federal Reserve benefits account. Alight Solutions LLC ("Alight" or "we"), which administers the Federal Reserve Benefits Center, SmartBenefits website and your SmartBenefits online account on behalf of the Federal Reserve, recently discovered and addressed two incidents involving your personal information. There is no indication that your personal information has been misused by any unauthorized parties, and we believe the risk of harm to you or your information is minimal. However, in an abundance of caution, we are writing to keep you fully informed.

This letter contains information about the personal information that was involved, how it has been used, the services that are being made available to you, and what you can do; please read it carefully.

What Happened?

On May 20, 2019, in connection with a routine Federal Reserve security review, we became aware of two issues involving your personal information.

Starting on September 22, 2014, system-generated emails from the SmartBenefits website were sent to individual participants confirming changes they made to their SmartBenefits online account. Federal Reserve Benefits Center system-generated emails were also sent to some individual participants to follow up on open cases with the Federal Reserve Benefits Center. Those communications inadvertently included your Social Security Number in the properties of the email. This information, which was used as an internal identifier for account tracking and customer service, was not included in the subject line or body of any email, and only included information pertinent to the recipient. You may have received at least one such email, sent via an unencrypted transmission, during the period from September 22, 2014 through June 29, 2019.

In that same review, and as part of a system modification, we also learned that from October 1, 2016 to February 22, 2019, URLs linking the SmartBenefits website – via encrypted transmission – to two (2) trusted third-party websites, also providing benefits services, included individual participants' Social Security Numbers and date of birth. While the URL was sent encrypted, this information may have been inadvertently stored in an un-encrypted form on a device used to access the SmartBenefits website. By URL, we mean the address of a specific webpage or website on the Internet. URLs can contain information that may not be fully visible to a user. While we are unable to confirm the existence of this URL on your particular device, we are informing you of this matter in the event you may have clicked on one or more of the links from the SmartBenefits website during this time.

What Information Was Involved?

The system-generated emails described above included your Social Security Number within the properties of the email. This information, which was used as an internal identifier for account tracking and customer service, was not included in the email subject line or body and was only sent to you.

With respect to the website URL issue discussed above, your Social Security Number and date of birth were included in the encrypted URLs sent from the SmartBenefits website – via encrypted transmission -- to two (2) third-party benefit providers. They were not labeled in any way.

What Are We Doing?

Upon learning of the situation, Alight initiated an investigation and promptly addressed these issues by encrypting Social Security Numbers in the email properties of both forms of system-generated emails and removing personal information from the URLs linking SmartBenefits to the trusted third-party websites.

Further, in an abundance of caution, and at no cost to you, we are offering you two years of identity theft protection through InfoArmor, a leading provider of employer-sponsored identity theft protection. Please review the Other Important Information attached to this letter for instructions on how to enroll with InfoArmor's PrivacyArmor service, which includes identity theft protection, continuous identity monitoring and credit monitoring. If you wish to continue receiving the service after expiration, you will be responsible for payment at a rate negotiated by the Federal Reserve.

What Can You Do?

Based on our investigation, there is no indication that your personal information has been misused by any unauthorized parties, and we believe the risk of harm to you is minimal. However, we recommend you take the following steps:

- Delete any automated confirmation or open case follow-up emails you received from SmartBenefits and/or the Federal Reserve Benefits Center prior to June 29, 2019 from your inbox, archives or sent folders. If you would like to retain a record of these emails, you should consider printing the emails.
- Clear your browsing history and/or your cache if you have not done so recently, especially if you know you have accessed the SmartBenefits website since October 1, 2016. If you do not know how to do this, consult the "help" section of your web browser(s).
- Activate identity theft protection services, at no cost to you, by contacting InfoArmor. For more information on these services, review the attached information or go to www.infoarmor.com/IDProtect or call 1-866-724-5798.

The attachment to this letter also describes other precautionary measures you can take to protect your personal information, including placing a fraud alert and security freeze on your credit files, at no cost to you, and obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

We regret any inconvenience that this may cause you. We are committed to maintaining the privacy and security of personal information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of your personal information.

Need More Information?

If you have more questions, please call 1-866-279-8289, 8 a.m. – 6 p.m. Eastern time, Monday through Friday, to speak with a dedicated benefits specialist specifically trained on this issue. For your state's TTY/TDD number for the hearing impaired, dial 711. If you are calling from an international location, the phone number for the Benefits Center is +1-704-646-8917.

– OTHER IMPORTANT INFORMATION –

1. **Activate your ID Theft Protection with Credit Monitoring at No Cost to You:**

   Activate Now in Three Easy Steps

   1. VISIT www.infoarmor.com/IDprotect or call 1-866-724-5798 and provide the activation code to InfoArmor's Privacy Advocate.
   2. CLICK on the Enroll Now button online.
   3. ENTER the **Activation Code**: **<<Code>>**

   If you currently are paying for InfoArmor's PrivacyArmor services and want to consider taking advantage of the 24-month membership at no cost, contact a Privacy Advocate at 1-866-724-5798 to explain the differences in coverage and to assist you in transitioning to the no-cost option. Coverage will end on September 1, 2021.

   ADDITIONAL DETAILS REGARDING YOUR PRIVACYARMOR MEMBERSHIP:

   A credit card is **not** required for activation, however additional information, such as: name, address, date of birth, Social Security Number and contact information are required to activate your account and begin proactive identity theft and credit monitoring. Activating this membership will help to uncover and resolve misuse of personal information early.

   Once you activate your PrivacyArmor coverage, you will have access to the following additional features and more:

   - **Identity and Credit Monitoring** – Actively monitors for the most damaging types of fraud.
   - **Credit Alerts and Scores** - Alerts on transactions like new inquiries, accounts in collections, new accounts and bankruptcy filings. Alerts and scores are provided by TransUnion.
   - **Dark Web Monitoring** – Artificial Intelligence bots and human intelligence operatives scan closed hacker forums for compromised credentials and IP addresses.
   - **Financial Activity Monitoring** - Alerts are triggered from sources such as bank accounts, credit and debit cards, 401(k)s, and other investment accounts.
   - **Digital Exposure Reports** - Enables members to see what personal information is publicly available on the internet.
   - **Full-service and Pre-existing Condition Remediation** – Trained advocates can help restore a member's identity regardless of when or how the damage occurred, including pre-existing fraudulent activity.
   - **$1 Million Identity Theft Insurance** – Reimburses members' out-of-pocket costs in the event they are a victim of fraud.

   Activate your membership at any time at www.infoarmor.com/IDprotect or call 1-866-724-5798 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.infoarmor.com/IDprotect for more information. If you have any questions about your PrivacyArmor coverage or suspect that an item on your credit report may be fraudulent, please contact InfoArmor's Privacy Advocates at 1-866-724-5798.

2. **As Always, Keep Your SmartBenefits Account and Information Safe By:**

   - Updating security software on each device you use to access your accounts.
   - Using a private device and a protected wireless connection (for example, connecting through a VPN or using password-protected Wi-Fi) when accessing your benefits information.
   - Using a strong, unique password for your SmartBenefits account that you don't use for any other account or website.

- Not saving your logon information on any device.
- Not sharing your account access or logon information with anyone, including friends and family.
- Updating your contact information by calling the Benefits Center or by logging on to the SmartBenefits website. Then, make sure to sign up online for mobile text alerts.
- Visiting Alight's new Security Center, accessible as a footnote at the bottom of the SmartBenefits website, to find the latest industry guidance on what you should do to keep your data secure. You can also learn about the Alight Protection Program and what you need to do to be covered.

3. **Placing a Fraud Alert on Your Credit File:**

Whether or not you choose to activate this 24-month service, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax	**Experian**	**TransUnion LLC**
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

4. **Consider Placing a Security Freeze on Your Credit File:**

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit-reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit-reporting companies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
PO Box 105788	PO Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19016
https://www.freeze.equifax.com	http://experian.com/freeze	http://www.transunion.com/securityfreeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

In order to place the security freeze, you will need to supply your name, address, date of birth, Social Security Number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

If you do place a security freeze ***prior*** to enrolling in the credit monitoring service as described above, you will need to remove the freeze in order to sign up for the credit monitoring service. After you sign up for the credit monitoring service, you may refreeze your credit file.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

5. **Obtaining a Free Credit Report:**

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them

for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

6. **Additional Helpful Resources:**

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission ("FTC") recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 1-515-281-5164

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Department of Justice, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 1-877-566-7226.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392.

Rhode Island Residents: You may obtain information about preventing identity theft from the Rhode Island Attorney General's Office: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903; 1-401-274-4400; http://www.riag.ri.gov.