

# KING & SPALDING

King & Spalding LLP  
1700 Pennsylvania Ave, NW  
Suite 200  
Washington, D.C. 20006-4707  
Tel: +1 202 737 0500  
www.kslaw.com

Nicholas A. Oldham  
Direct Dial: +1 202 626 3740  
noldham@kslaw.com

July 21, 2017

**VIA EMAIL:** [attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)

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

Dear Attorney General MacDonald,

I represent TALX Corporation (“TALX”), a wholly owned subsidiary of Equifax, Inc., and write regarding a data security incident that may have exposed personal information of some New Hampshire residents, who are employees or former employees of Whole Foods Market (“Whole Foods”). In a limited number of instances, the residents may be family members of employees or former employees of Whole Foods.

TALX provides payroll-related services for Whole Foods and other companies, which in the case of Whole Foods, includes providing current and former employees with online access to their W-2 and 1095-C tax forms through TALX’s online portal available at [www.mytaxform.com](http://www.mytaxform.com) (the “online portal”). On April 27, 2017, Whole Foods informed TALX that certain Whole Foods employees had been contacted by the IRS regarding potentially fraudulent tax returns. At the time, TALX was investigating similar reports from certain of its other customers and had engaged a leading cybersecurity firm to assist with its analysis. Upon learning of the reports from Whole Foods, TALX and Whole Foods promptly worked together to understand what happened and determine the scope of the incident. Based on the analysis to date, TALX believes that an unauthorized third-party(ies) gained access to the online portal accounts primarily by successfully answering personal questions about the affected employees in order to reset the employees’ PINs (*i.e.*, the password to access the online portal). There is no indication that either TALX or Whole Foods was the source of any of the information used to reset the PINs and access the employee accounts.

Because the account accesses generally appear legitimate (*e.g.*, successful use of login credentials), TALX cannot confirm forensically exactly which accounts were, in fact, accessed

Attorney General Gordon MacDonald  
Office of the Attorney General  
July 21, 2017

without authorization. Nonetheless, on June 26, 2017, TALX identified a broad universe of current and former employees (and in some instances family members) whose information might have been accessed without authorization between April 18, 2016 and April 23, 2017. Although TALX believes that only a small percentage of these potentially affected accounts were actually affected, out of an abundance of caution, TALX and Whole Foods are notifying the broad universe of current and former Whole Foods employees identified as potentially affected during the investigation, as well as the covered individuals (*i.e.*, family members) whose information may have been accessed through a current or former employee's 1095-C form.

Access to the employees' online portal accounts would have permitted the unauthorized third-party(ies) access to the employees' W-2 forms and, in a limited number of instances, 1095-C forms, which, for some employees, include personal information relating to family members covered by Whole Foods' health insurance. The unauthorized third-party(ies) would have also been able to access other information maintained in the employees' respective online portal accounts, including the employee's name, address, date of birth, employee identification number, email address, gender, and marital status.

TALX has notified federal law enforcement, the Internal Revenue Service (IRS), and state tax authorities of the incident. Additionally, to help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring. TALX also removed the personal questions as an option to reset PINs from the online portal and worked with Whole Foods to reset potentially affected employees' PINs, removed unverified contact information (email addresses and phone numbers) associated with employees' accounts, and added valid contact information from Whole Foods, where available, for the purpose of utilizing one-time passcodes as part of multi-factor authentication.

On July 20, 2017, TALX, working with Whole Foods, notified by mail the 12 New Hampshire residents who may have been affected by the incident and fit within the broad universe. Unaddressed copies of the notifications (which vary depending on the type of personal information affected) are attached to this letter. Additionally, the affected individuals are being offered two (2) years of ID Patrol identity protection service free of charge. This service will provide the individual with comprehensive credit file monitoring and automated alerts of any key changes to their credit report, as well as \$1 million in identity fraud expense coverage.

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

Sincerely,



Nicholas A. Oldham  
*Counsel for TALX Corporation*



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>

<<Name1>>

<<Address 1>>

<<Address 2>>

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

<<Country>>

<<Date>>

## **RE: Notice of Data Security Incident**

Dear <<Name1>>:

Talx Corporation (“TALX”), a wholly owned subsidiary of Equifax, Inc., is writing to inform you about a data security incident that may have resulted in the unauthorized access to an electronic copy of your Whole Foods Market (“Whole Foods”) W-2 tax form. We take the protection and proper use of your information very seriously. While the investigation is ongoing, out of an abundance of caution, we are notifying a broad group of individuals who may have been affected.

### **What Happened**

TALX provides payroll-related services for Whole Foods, your current or former employer, which includes providing you with online access to your W-2 tax form through TALX’s W-2 eXpress website at [www.mytaxform.com](http://www.mytaxform.com) (the “online portal”). We recently discovered that an unauthorized third-party(ies) accessed the online accounts of certain team members during various time periods from April 18, 2016 through April 23, 2017. Upon learning of the unauthorized access, TALX and Whole Foods promptly worked together to understand what happened and the scope of the incident. TALX determined that, in some instances, the unauthorized third-party(ies) successfully answered personal questions about Whole Foods’ affected team members in order to reset the team members’ PINs (i.e., the password to access the online portal).

We have no indication that either TALX or Whole Foods was the source of any of the information used to reset the PINs and access team member accounts.

### **What Information Was Involved**

An unauthorized third-party(ies) may have accessed an electronic copy of your W-2 tax form, which includes your name, Social Security number, and earnings information. The unauthorized third-party(ies) may have also accessed other information maintained in your online portal account, including your address, phone number, date of birth, team member identification number, email address, gender, and marital status.

### **What We Are Doing**

We have notified federal law enforcement, the Internal Revenue Service (“IRS”), and state tax authorities of the incident, who we understand will monitor affected individuals’ accounts for the purposes of attempting to prevent fraudulent tax refunds.

To help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring. In addition, TALX has disabled authentication by personal questions, reset your PIN to the original default PIN assigned by Whole Foods, removed unverified contact information (email addresses and phone numbers) associated with your account, and added valid contact information from Whole Foods, where available, for the purpose of resetting your PIN. To access your account, you will need to go to the website listed above and log-in with

your team member ID. You will then be prompted to choose the best available contact method and verify your identity by receiving a one-time-passcode (OTP) to the email or phone number supplied by Whole Foods if one was available. Once you access your online portal account, you will be prompted to create a new PIN for your account and you are encouraged to ensure that your contact information is up to date. If you are unable to reset your PIN or you otherwise cannot access your online portal account, please call the TALX Customer Service Center at 1-888-594-3729.

### **What You Can Do**

We are notifying you so that you can take appropriate steps to protect yourself and to offer you two years of ID Patrol identity protection service at no cost to you. For more information on the ID Patrol identity protection services, including instructions on how to activate your complimentary two-year membership, please see the “ID Patrol Enrollment Instructions” provided in this letter.

Even if you choose not to enroll in the service, there are other steps you can take to help protect yourself. Please see the information in the “More Information on Ways to Protect Yourself” attachment about how you can obtain a free copy of your credit report, place a fraud alert and/or credit freeze on your credit report, and steps to consider taking if you suspect you are a victim of tax-related identity theft.

### **For More Information**

We deeply regret that this incident occurred and are committed to ensuring that your personal information remains protected. If you have any questions, please call 1-800-538-0658, Monday-Friday between the hours of 8 a.m. and 8 p.m. CST.

Sincerely,

TALX Corporation

## **ID Patrol Enrollment Instructions**

TALX is offering Equifax's ID Patrol identity theft protection product to you for 24 months at no charge. Information about ID Patrol, your personal Activation Code and enrollment instructions follow:

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to \$1 million in identity theft insurance with \$0 deductible

Please visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) for more information and to enroll for ID Patrol.

**Your Activation Code is <<Activation Code>>. You must use this Activation Code to activate the product by October 14, 2017. Please note that this Activation Code is non-transferable. Coverage under ID Patrol will expire 24 months from the date you activate your code by enrolling for ID Patrol online.**

### ENROLLMENT TIPS:

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!**)
2. Enter the Activation Code provided above and click the "Submit" button
3. The platform will walk you through the enrollment. Please enter the information requested and click the Continue button to step through the account setup screens
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button
5. You will see an order confirmation page and you can click View My Product to access the product features
6. You will receive a confirmation email

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information and to provide personalized identity theft victim assistance and assistance in initiating an investigation of inaccurate information.

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

We encourage you to take the following steps to protect your personal information:

- **Contact the IRS.** If you suspect you are a victim of tax-related identity theft, please consider taking the following steps:
  - Visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> or <https://www.irs.gov/individuals/data-breach-information-for-taxpayers> for more information.
  - Contact the IRS at 1-800-908-4490 for additional information.
  - Complete IRS Form 14039, Identity Theft Affidavit, available at <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>. Once you have fully completed the form, print it and submit it to the IRS according to the instructions on the form.
- **Contact your State Tax Agency.** If you suspect you are a victim of tax-related identity theft, please consider contacting your state tax agency. Information to contact our state tax agency is available at <http://www.taxadmin.org/state-tax-agencies>.
- **Order Your Free Credit Report.** We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

- **Report Incidents.** If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission (“FTC”). You may also contact the FTC to obtain additional information about avoiding identity theft.

**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)

- **Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

As soon as that agency processes your fraud alert, it will notify the other two, which then must also place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/).

- **Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (e.g., a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

---

**If you are a resident of Maryland**, you may contact the Maryland Attorney General’s Office at 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

---

**If you are a resident of New Mexico**, note that 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. A list of the primary rights created by the FCRA is available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. For more information, including information about additional rights, please visit [www.ftc.gov/credit](http://www.ftc.gov/credit).

---

**If you are a resident of North Carolina**, you may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716- 6400.

---

**If you are a resident of Oregon**, you may contact the Oregon Attorney General’s Office at 1162 Court Street NE, Salem, OR 97301-4096, <http://www.doj.state.or.us>, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400.

---

**If you are a resident of Rhode Island**, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401)-274-4400. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

---

**If you are a resident of West Virginia**, you have the right to the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>

<<Name1>>

<<Address 1>>

<<Address 2>>

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

<<Country>>

<<Date>>

## **RE: Notice of Data Security Incident**

Dear <<Name1>>:

Talx Corporation (“TALX”), a wholly owned subsidiary of Equifax, Inc., is writing to inform you about a data security incident that may have resulted in the unauthorized access to an electronic copy of your Whole Foods Market (“Whole Foods”) W-2 and 1095-C tax forms. We take the protection and proper use of your information very seriously. While the investigation is ongoing, out of an abundance of caution, we are notifying a broad group of individuals who may have been affected.

### **What Happened**

TALX provides payroll-related services for Whole Foods, your current or former employer, which includes providing you with online access to your W-2 and 1095 C tax forms through TALX’s W-2 eXpress website at [www.mytaxform.com](http://www.mytaxform.com) (the “online portal”). We recently discovered that an unauthorized third-party(ies) accessed the online accounts of certain employees during various time periods from April 18, 2016 through April 23, 2017. Upon learning of the unauthorized access, TALX and Whole Foods promptly worked together to understand what happened and the scope of the incident. TALX determined that, in some instances, the unauthorized third-party(ies) successfully answered personal questions about Whole Foods’ affected employees in order to reset the employees’ PINs (i.e., the password to access the online portal).

We have no indication that either TALX or Whole Foods was the source of any of the information used to reset the PINs and access team member accounts.

### **What Information Was Involved**

An unauthorized third-party(ies) may have accessed electronic copies of your W-2 and 1095-C tax forms. Your W-2 tax form includes your name, Social Security number, and earnings information, and your 1095-C includes your name, Social Security number, and health insurance coverage information. The unauthorized third-party(ies) may have also accessed other information maintained in your online portal account, including your address, phone number, date of birth, team member identification number, email address, gender, and marital status.

### **What We Are Doing**

We have notified federal law enforcement, the Internal Revenue Service (“IRS”), and state tax authorities of the incident, who we understand will monitor affected individuals’ accounts for the purposes of attempting to prevent fraudulent tax refunds.

To help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring. In addition, TALX has disabled authentication by personal questions, reset your PIN to the original default PIN assigned by Whole Foods, removed unverified contact information (email addresses and phone numbers) associated with your account, and added valid contact information from Whole Foods, where available, for the

purpose of resetting your PIN. To access your account, you will need to go to the website listed above and log-in with your team member ID. You will then be prompted to choose the best available contact method and verify your identity by receiving a one-time-passcode (OTP) to the email or phone number supplied by Whole Foods if one was available. Once you access your online portal account, you will be prompted to create a new PIN for your account and you are encouraged to ensure that your contact information is up to date. If you are unable to reset your PIN or you otherwise cannot access your online portal account, please call the TALX Customer Service Center at 1-888-594-3729.

### **What You Can Do**

We are notifying you so that you can take appropriate steps to protect yourself and to offer you two years of ID Patrol identity protection service at no cost to you. For more information on the ID Patrol identity protection services, including instructions on how to activate your complimentary two-year membership, please see the “ID Patrol Enrollment Instructions” provided in this letter.

Even if you choose not to enroll in the service, there are other steps you can take to help protect yourself. Please see the information in the “More Information on Ways to Protect Yourself” attachment about how you can obtain a free copy of your credit report, place a fraud alert and/or credit freeze on your credit report, and steps to consider taking if you suspect you are a victim of tax-related identity theft.

### **For More Information**

We deeply regret that this incident occurred and are committed to ensuring that your personal information remains protected. If you have any questions, please call 1-800-538-0658, Monday-Friday between the hours of 8 a.m. and 8 p.m. CST.

Sincerely,

TALX Corporation

## **ID Patrol Enrollment Instructions**

TALX is offering Equifax's ID Patrol identity theft protection product to you for 24 months at no charge. Information about ID Patrol, your personal Activation Code and enrollment instructions follow:

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to \$1 million in identity theft insurance with \$0 deductible

Please visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) for more information and to enroll for ID Patrol.

**Your Activation Code is <<Activation Code>>. You must use this Activation Code to activate the product by October 14, 2017. Please note that this Activation Code is non-transferable. Coverage under ID Patrol will expire 24 months from the date you activate your code by enrolling for ID Patrol online.**

### ENROLLMENT TIPS:

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!**)
2. Enter the Activation Code provided above and click the "Submit" button
3. The platform will walk you through the enrollment. Please enter the information requested and click the Continue button to step through the account setup screens
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button
5. You will see an order confirmation page and you can click View My Product to access the product features
6. You will receive a confirmation email

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information and to provide personalized identity theft victim assistance and assistance in initiating an investigation of inaccurate information.

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

We encourage you to take the following steps to protect your personal information:

- **Contact the IRS.** If you suspect you are a victim of tax-related identity theft, please consider taking the following steps:
  - Visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> or <https://www.irs.gov/individuals/data-breach-information-for-taxpayers> for more information.
  - Contact the IRS at 1-800-908-4490 for additional information.
  - Complete IRS Form 14039, Identity Theft Affidavit, available at <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>. Once you have fully completed the form, print it and submit it to the IRS according to the instructions on the form.
- **Contact your State Tax Agency.** If you suspect you are a victim of tax-related identity theft, please consider contacting your state tax agency. Information to contact our state tax agency is available at <http://www.taxadmin.org/state-tax-agencies>.
- **Order Your Free Credit Report.** We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

- **Report Incidents.** If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission (“FTC”). You may also contact the FTC to obtain additional information about avoiding identity theft.

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)

- **Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

As soon as that agency processes your fraud alert, it will notify the other two, which then must also place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/).

- **Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (e.g., a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

---

**If you are a resident of Maryland**, you may contact the Maryland Attorney General’s Office at 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

---

**If you are a resident of New Mexico**, note that 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. A list of the primary rights created by the FCRA is available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. For more information, including information about additional rights, please visit [www.ftc.gov/credit](http://www.ftc.gov/credit).

---

**If you are a resident of North Carolina**, you may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716- 6400.

---

**If you are a resident of Oregon**, you may contact the Oregon Attorney General’s Office at 1162 Court Street NE, Salem, OR 97301-4096, <http://www.doj.state.or.us>, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400.

---

**If you are a resident of Rhode Island**, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401)-274-4400. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

---

**If you are a resident of West Virginia**, you have the right to the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name1>>  
<<Address 1>>  
<<Address 2>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

**RE: Notice of Data Security Incident**

Dear <<Name1>>:

Talx Corporation (“TALX”), a wholly owned subsidiary of Equifax, Inc., is writing to inform you about a data security incident that may have resulted in the unauthorized access to an electronic copy of your Whole Foods Market (“Whole Foods”) W-2 tax form and 1095-C tax form. We take the protection and proper use of your information very seriously. While the investigation is ongoing, out of an abundance of caution, we are notifying a broad group of individuals who may have been affected.

**What Happened**

TALX provides payroll-related services for Whole Foods, your current or former employer, which includes providing you with online access to your W-2 and 1095-C tax forms through TALX’s W-2 eXpress website at [www.mytaxform.com](http://www.mytaxform.com) (the “online portal”). We recently discovered that an unauthorized third-party(ies) accessed the online accounts of certain team members during various time periods from April 18, 2016 through April 23, 2017. Upon learning of the unauthorized access, TALX and Whole Foods promptly worked together to understand what happened and the scope of the incident. TALX determined that, in some instances, the unauthorized third-party(ies) successfully answered personal questions about Whole Foods’ affected team members in order to reset the team members’ PINs (i.e., the password to access the online portal).

We have no indication that either TALX or Whole Foods was the source of any of the information used to reset the PINs and access team member accounts.

**What Information Was Involved**

An unauthorized third-party(ies) may have accessed an electronic copy of your W-2 tax form and 1095-C tax form. Your 1095-C tax form contains personal information, including name, Social Security number, and health insurance coverage information relating to you and the family members listed on your 1095-C tax form. Your W-2 tax form also includes your earnings information. Each family member listed on your 1095-C tax form is being mailed a separate notification related to this incident. The unauthorized third-party(ies) may have also accessed other information maintained in your online portal account, including your address, phone number, date of birth, team member identification number, email address, gender, and marital status.

**What We Are Doing**

We have notified federal law enforcement, the Internal Revenue Service (“IRS”), and state tax authorities of the incident, who we understand will monitor affected individuals’ accounts for the purposes of attempting to prevent fraudulent tax refunds.

To help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring. In addition, TALX has disabled authentication by personal questions, reset your PIN to the original default PIN assigned by Whole Foods, removed unverified contact information (email addresses and phone numbers) associated with your account, and added valid contact information from Whole Foods, where available, for the purpose of resetting your PIN. To access your account, you will need to go to the website listed above and log-in with your team member ID. You will then be prompted to choose the best available contact method and verify your identity by receiving a one-time-passcode (OTP) to the email or phone number supplied by Whole Foods if one was available. Once you access your online portal account, you will be prompted to create a new PIN for your account and you are encouraged to ensure that your contact information is up to date. If you are unable to reset your PIN or you otherwise cannot access your online portal account, please call the TALX Customer Service Center at 1-888-594-3729.

### **What You Can Do**

We are notifying you so that you can take appropriate steps to protect yourself and to offer you two years of ID Patrol identity protection service at no cost to you. For more information on the ID Patrol identity protection services, including instructions on how to activate your complimentary two-year membership, please see the “ID Patrol Enrollment Instructions” provided in this letter.

Even if you choose not to enroll in the service, there are other steps you can take to help protect yourself. Please see the information in the “More Information on Ways to Protect Yourself” attachment about how you can obtain a free copy of your credit report, place a fraud alert and/or credit freeze on your credit report, and steps to consider taking if you suspect you are a victim of tax-related identity theft.

### **For More Information**

We deeply regret that this incident occurred and are committed to ensuring that your personal information remains protected. If you have any questions, please call 1-800-538-0658, Monday-Friday between the hours of 8 a.m. and 8 p.m. CST.

Sincerely,

TALX Corporation

## **ID Patrol Enrollment Instructions**

TALX is offering Equifax's ID Patrol identity theft protection product to you for 24 months at no charge. Information about ID Patrol, your personal Activation Code and enrollment instructions follow:

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to \$1 million in identity theft insurance with \$0 deductible

Please visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) for more information and to enroll for ID Patrol.

**Your Activation Code is <<Activation Code>>. You must use this Activation Code to activate the product by October 14, 2017. Please note that this Activation Code is non-transferable. Coverage under ID Patrol will expire 24 months from the date you activate your code by enrolling for ID Patrol online.**

### ENROLLMENT TIPS:

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!**)
2. Enter the Activation Code provided above and click the "Submit" button
3. The platform will walk you through the enrollment. Please enter the information requested and click the Continue button to step through the account setup screens
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button
5. You will see an order confirmation page and you can click View My Product to access the product features
6. You will receive a confirmation email

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information and to provide personalized identity theft victim assistance and assistance in initiating an investigation of inaccurate information.

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

We encourage you to take the following steps to protect your personal information:

- **Contact the IRS.** If you suspect you are a victim of tax-related identity theft, please consider taking the following steps:
  - Visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> or <https://www.irs.gov/individuals/data-breach-information-for-taxpayers> for more information.
  - Contact the IRS at 1-800-908-4490 for additional information.
  - Complete IRS Form 14039, Identity Theft Affidavit, available at <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>. Once you have fully completed the form, print it and submit it to the IRS according to the instructions on the form.
- **Contact your State Tax Agency.** If you suspect you are a victim of tax-related identity theft, please consider contacting your state tax agency. Information to contact our state tax agency is available at <http://www.taxadmin.org/state-tax-agencies>.
- **Order Your Free Credit Report.** We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

- **Report Incidents.** If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission (“FTC”). You may also contact the FTC to obtain additional information about avoiding identity theft.

**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)

- **Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

As soon as that agency processes your fraud alert, it will notify the other two, which then must also place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/).

- **Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (e.g., a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

---

**If you are a resident of Maryland**, you may contact the Maryland Attorney General’s Office at 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

---

**If you are a resident of New Mexico**, note that 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. A list of the primary rights created by the FCRA is available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. For more information, including information about additional rights, please visit [www.ftc.gov/credit](http://www.ftc.gov/credit).

---

**If you are a resident of North Carolina**, you may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716- 6400.

---

**If you are a resident of Oregon**, you may contact the Oregon Attorney General’s Office at 1162 Court Street NE, Salem, OR 97301-4096, <http://www.doj.state.or.us>, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400.

---

**If you are a resident of Rhode Island**, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401)-274-4400. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

---

**If you are a resident of West Virginia**, you have the right to the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.



Return Mail Processing Center  
PO Box 6336  
Portland, OR 97228-6336

<<Mail ID>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<City>><<State>><<Zip>>  
<<Country>>

<<Date>>

**RE: Notice of Data Security Incident**

Dear <<Name2>>:

Talx Corporation (“TALX”), a wholly owned subsidiary of Equifax, Inc., is writing to inform you about a data security incident that may have resulted in the unauthorized access to your personal information contained in <<Name1>>’s Whole Foods Market (“Whole Foods”) 1095-C tax form. We take the protection and proper use of your information very seriously. While the investigation is ongoing, out of an abundance of caution, we are notifying a broad group of individuals who may have been affected.

**What Happened**

TALX provides payroll-related services for Whole Foods, <<Name1>>’s current or former employer, which includes providing Whole Foods’ current and former team members with online access to their 1095-C tax form through TALX’s W-2 eXpress website at [www.mytaxform.com](http://www.mytaxform.com) (the “online portal”). We recently discovered that an unauthorized third-party(ies) accessed the online accounts of certain team members during various time periods from April 18, 2016 through April 23, 2017. Upon learning of the unauthorized access, TALX and Whole Foods promptly worked together to understand what happened and the scope of the incident. TALX determined that, in some instances, the unauthorized third-party(ies) successfully answered personal questions about Whole Foods’ affected team members in order to reset the team members’ PINs (i.e., the password to access the online portal).

We have no indication that either TALX or Whole Foods was the source of any of the information used to reset the PINs and access team member accounts.

**What Information Was Involved**

An unauthorized third-party(ies) may have accessed your personal information contained in <<Name1>>’s Whole Foods 1095-C tax form, including your name, Social Security number, and health insurance coverage information.

**What We Are Doing**

We have notified federal law enforcement, the Internal Revenue Service (“IRS”), and state tax authorities of the incident, who we understand will monitor affected individuals’ accounts for the purposes of attempting to prevent fraudulent tax refunds.

To help prevent recurrence of this type of incident, TALX has implemented additional security measures, including enhanced fraud monitoring.

### **What You Can Do**

We are notifying you so that you can take appropriate steps to protect yourself and to offer you two years of ID Patrol identity protection service at no cost to you. For more information on the ID Patrol identity protection services, including instructions on how to activate your complimentary two-year membership, please see the “ID Patrol Enrollment Instructions” provided in this letter.

Even if you choose not to enroll in the service, there are other steps you can take to help protect yourself. Please see the information in the “More Information on Ways to Protect Yourself” attachment about how you can obtain a free copy of your credit report, place a fraud alert and/or credit freeze on your credit report, and steps to consider taking if you suspect you are a victim of tax-related identity theft.

### **For More Information**

We deeply regret that this incident occurred and are committed to ensuring that your personal information remains protected. If you have any questions, please call 1-800-538-0658, Monday-Friday between the hours of 8 a.m. and 8 p.m. CST.

Sincerely,

TALX Corporation

## **ID Patrol Enrollment Instructions**

TALX is offering Equifax's ID Patrol identity theft protection product to you for 24 months at no charge. Information about ID Patrol, your personal Activation Code and enrollment instructions follow:

ID Patrol will provide you with an "early warning system" to changes to your credit file and help you to understand the content of your credit file at the three major credit-reporting agencies.

ID Patrol provides you with the following key features and benefits:

- Comprehensive credit file monitoring and automated alerts of key changes to your Equifax, Experian, and TransUnion credit reports
- Wireless alerts and customizable alerts available
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Ability to receive alerts if your Social Security Number or credit card numbers are found on Internet trading sites (available online only)
- Ability to lock and unlock your Equifax Credit Report
- Up to \$1 million in identity theft insurance with \$0 deductible

Please visit [www.myservices.equifax.com/patrol](http://www.myservices.equifax.com/patrol) for more information and to enroll for ID Patrol.

**Your Activation Code is <<Activation Code>>. You must use this Activation Code to activate the product by October 14, 2017. Please note that this Activation Code is non-transferable. Coverage under ID Patrol will expire 24 months from the date you activate your code by enrolling for ID Patrol online.**

If you are under the age of 18, please have a parent or guardian call 1-800-538-0658, Monday-Friday between the hours of 8 a.m. and 8 p.m. CST to receive an Activation Code for Equifax Child Monitoring. The Activation Code you receive may then be used for registration at [www.myservices.equifax.com/minor](http://www.myservices.equifax.com/minor).

### **ENROLLMENT TIPS:**

1. Use the link above to access your custom ID Patrol Enrollment page (**your activation code will NOT work if you use a different link!**)
2. Enter the Activation Code provided above and click the "Submit" button
3. The platform will walk you through the enrollment. Please enter the information requested and click the Continue button to step through the account setup screens
4. The system will then ask you up to four security questions to verify your identity. Please answer the questions and click the "Submit Order" button
5. You will see an order confirmation page and you can click View My Product to access the product features
6. You will receive a confirmation email

Once enrolled, your ID Patrol comes with 24/7 live agent Customer Service (877-474-8273) to assist you in understanding the content of your Equifax credit information and to provide personalized identity theft victim assistance and assistance in initiating an investigation of inaccurate information.

**MORE INFORMATION ON WAYS TO PROTECT YOURSELF**

We encourage you to take the following steps to protect your personal information:

- **Contact the IRS.** If you suspect you are a victim of tax-related identity theft, please consider taking the following steps:
  - Visit <https://www.irs.gov/individuals/how-irs-id-theft-victim-assistance-works> or <https://www.irs.gov/individuals/data-breach-information-for-taxpayers> for more information.
  - Contact the IRS at 1-800-908-4490 for additional information.
  - Complete IRS Form 14039, Identity Theft Affidavit, available at <https://www.irs.gov/uac/taxpayer-guide-to-identity-theft>. Once you have fully completed the form, print it and submit it to the IRS according to the instructions on the form.
- **Contact your State Tax Agency.** If you suspect you are a victim of tax-related identity theft, please consider contacting your state tax agency. Information to contact our state tax agency is available at <http://www.taxadmin.org/state-tax-agencies>.
- **Order Your Free Credit Report.** We recommend that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit reports. You may obtain a free copy of your credit report from each company listed below once every 12 months by requesting your report online at [www.annualcreditreport.com](http://www.annualcreditreport.com), calling toll-free 1-877-322-8228, or mailing an Annual Credit Report Request Form (available at [www.annualcreditreport.com](http://www.annualcreditreport.com)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting any of the credit reporting agencies below:

Equifax  
PO Box 740241  
Atlanta, GA 30374  
[www.equifax.com](http://www.equifax.com)  
888-766-0008

Experian  
PO Box 9554  
Allen, TX 75013  
[www.experian.com](http://www.experian.com)  
888-397-3742

TransUnion  
PO Box 2000  
Chester, PA 19016  
[www.transunion.com](http://www.transunion.com)  
800-680-7289

- **Report Incidents.** If you believe you are the victim of identity theft, you should contact the proper law enforcement authorities, including local law enforcement, and you should consider contacting your state attorney general and/or the Federal Trade Commission (“FTC”). You may also contact the FTC to obtain additional information about avoiding identity theft.

**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)

- **Consider Placing a Fraud Alert on Your Credit File.** To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide consumer reporting agencies. Contact information for each of the three credit reporting agencies is as follows:

Equifax	Equifax Credit Information Services, Inc. P.O. Box 740241 Atlanta, GA 30374	1-800-525-6285	<a href="http://www.equifax.com">www.equifax.com</a>
Experian	Experian Inc. P.O. Box 9554 Allen, TX 75013	1-888-397-3742	<a href="http://www.experian.com">www.experian.com</a>
TransUnion	TransUnion LLC P.O. Box 2000 Chester, PA 19022-2000	1-800-680-7289	<a href="http://www.transunion.com">www.transunion.com</a>

As soon as that agency processes your fraud alert, it will notify the other two, which then must also place fraud alerts in your file. You may choose between two types of fraud alert. An initial alert (Initial Security Alert) stays in your file for at least 90 days. An extended alert (Extended Fraud Victim Alert) stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit [www.ftc.gov/idtheft/](http://www.ftc.gov/idtheft/).

- **Consider Placing a Security Freeze on Your Credit File.** You may wish to place a “security freeze” (also known as a “credit freeze”) on your credit file. A security freeze is designed to prevent potential creditors from accessing your credit file at the consumer reporting agencies without your consent. There may be fees for placing, lifting, and/or removing a security freeze, which generally range from \$5-\$20 per action. *Unlike a fraud alert, you must place a security freeze on your credit file at each consumer reporting agency individually.* For more information on security freezes, you may contact the three nationwide consumer reporting agencies or the FTC as described above.

As the instructions for establishing a security freeze differ from state to state, please contact the three nationwide consumer reporting agencies to find out more information. The consumer reporting agencies may require proper identification prior to honoring your request. For example, you may be asked to provide:

- Your full name with middle initial and generation (such as Jr., Sr., II, III)
- Your Social Security number
- Your date of birth
- Addresses where you have lived over the past five years
- A legible copy of a government-issued identification card (e.g., a state driver’s license or military ID card)
- Proof of your current residential address (such as a current utility bill or account statement)

---

**If you are a resident of Maryland**, you may contact the Maryland Attorney General’s Office at 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us](http://www.oag.state.md.us), 1-888-743-0023.

---

**If you are a resident of New Mexico**, please note 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. A list of the primary rights created by the FCRA is available at <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>. For more information, including information about additional rights, please visit [www.ftc.gov/credit](http://www.ftc.gov/credit).

---

**If you are a resident of North Carolina**, you may contact the North Carolina Attorney General’s Office at 9001 Mail Service Center, Raleigh, NC 27699, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716- 6400.

---

**If you are a resident of Oregon**, you may contact the Oregon Attorney General’s Office at 1162 Court Street NE, Salem, OR 97301-4096, <http://www.doj.state.or.us>, (877) 877-9392 (toll-free in Oregon) or (503) 378-4400.

---

**If you are a resident of Rhode Island**, you may obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General at 150 South Main Street Providence, RI 02903, [www.riag.ri.gov](http://www.riag.ri.gov), (401)-274-4400. You have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to \$10 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security number, date of birth, and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

---

**If you are a resident of West Virginia**, you have the right to the right to ask that nationwide consumer reporting agencies place “fraud alerts” in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.