



MULLEN
COUGHLIN^{LLC}

STATE OF NH
DEPT OF JUSTICE
2017 FEB -7 AM 11:03

Edward J. Finn
Office: 267-930-4776
Fax: 267-930-4771
Email: efinn@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

February 3, 2017

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Foster:

We represent The Mitchell Gold Co. d/b/a Mitchell Gold + Bob Williams ("Mitchell Gold + Bob Williams" or the "Company"), 135 One Comfortable Place, Taylorsville, NC 28681, and are writing to notify your office of an incident that may affect the security of personal information relating to 2 New Hampshire residents. The investigation into this event is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Mitchell Gold + Bob Williams does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Data Event

Mitchell Gold + Bob Williams was the victim of an email spoofing attack on January 23, 2017, by an individual pretending to be Mr. Mitchell Gold, the Company's co-founder and CEO. A request was made from what appeared to be a legitimate Mitchell Gold + Bob Williams email address for all 2016 Mitchell Gold + Bob Williams employee W-2 information. Unfortunately, copies of all 2016 employee W-2 forms were provided before the company discovered that the request was made from a fraudulent account that appeared to belong to Mr. Gold. Mitchell Gold + Bob Williams discovered the fraudulent nature of the request on January 24, 2017 and has been working tirelessly to investigate and to mitigate the impact of the attack.

Notice to New Hampshire Residents

On January 25, 2017, Mitchell Gold + Bob Williams provided preliminary notice to current employees via email. A copy of this notice is attached here as ***Exhibit A***. On February 3, 2017 2017, Mitchell Gold + Bob Williams will begin providing written notice of this incident to all affected current and former employees, which includes 2 New Hampshire residents. Written notice will be provided in substantially the same form as the letter attached here as ***Exhibit B***.

Other Steps Taken and To Be Taken

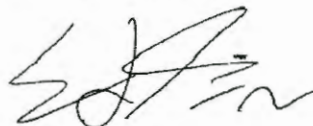
Upon discovering the fraudulent nature of the email, Mitchell Gold + Bob Williams moved quickly to identify those who may be affected, to put in place resources to assist them, and to provide them with notice of this incident.

Mitchell Gold + Bob Williams is providing all potentially affected individuals access to two free years of credit and identity monitoring services, including identity restoration services, through Equifax, and has established a dedicated hotline for potentially affected individuals to contact with questions or concerns regarding this incident. Additionally, Mitchell Gold + Bob Williams is providing potentially impacted individuals with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, and information on protecting against tax fraud. Mitchell Gold + Bob Williams also provided affected individuals with the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. Mitchell Gold + Bob Williams is also providing written notice of this incident to other state regulators as necessary. Mitchell Gold + Bob Williams has provided notice of this incident to the IRS, local police, and the FBI.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4776.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Ed Finn', is written over a horizontal line.

Ed Finn of
MULLEN COUGHLIN LLC

Exhibit A

MEMORANDUM

TO: Employees of Mitchell Gold + Bob Williams in 2016

DATE: January 25, 2017

RE: URGENT COMMUNICATION – Preliminary Notice of Data Incident

We recently discovered that our company was the targeted victim of an email spoofing attack on January 23, 2017, by an individual pretending to be Mitchell Gold; a request was made from what appeared to be a legitimate Mitchell Gold email address for all 2016 employee W-2 forms. Unfortunately, copies of all 2016 employee W2 forms were provided before we discovered that the request was made from a fraudulent account by someone using an email address that appeared to belong to Mitchell. We discovered the fraudulent nature of the request yesterday, and have been working tirelessly to investigate and to mitigate the impact of the attack. This includes our having notified the Internal Revenue Service yesterday, and our filing a report with the Alexander County Sheriff's Office this morning.

Please note that this incident affects you only if you were employed by Mitchell Gold + Bob Williams in 2016. If your employment did not begin with Mitchell Gold + Bob Williams until 2017, then your information has not been impacted.

The confidentiality, privacy, and security of our employee information is one of our highest priorities. While our investigation is ongoing, we felt it important to notify you about this incident, and what we are doing to investigate and respond, as quickly as possible. Here are some actions in addition to those above that we are taking and that we encourage you to take:

- Identity Protection. As a precaution, for those individuals affected by this incident, we will arrange for a credit monitoring service to protect your identity at no cost to you. The cost of this service will be paid for by Mitchell Gold + Bob Williams, and instructions for activating your protection will be forthcoming. ***We strongly encourage you to act to take advantage of these free identity protections services as soon as offered.*** It is incumbent upon you to enroll in these services, as we are not able to act on your behalf to enroll you in the credit monitoring service.
- Notice to Affected Individuals. We also will be mailing information to all impacted current and former Mitchell Gold + Bob Williams 2016 employees.
- Call Center for Employee Questions. We will establish a call center to answer common questions regarding this incident. Instructions on how you may reach the call center toll free will also be forthcoming.
- Notice to Law Enforcement and the IRS. We are notifying federal and local law enforcement of the incident, and we will be notifying any necessary state Attorneys General as well. We look forward to cooperating with the FBI and state law enforcement agencies in their investigations of this incident. As noted above, we have already reported this incident to the IRS so that they may take steps to monitor for attempts to file fraudulent tax returns using Mitchell Gold + Bob Williams employee information. The IRS will take steps, as necessary, to notify appropriate state taxing authorities of the incident.

- Filing of 2016 Tax Returns. We encourage you to file your 2016 tax return as soon as possible, if you have not already done so. If you have not yet filed your 2016 tax return, when you file, we also encourage you to file IRS Form 14039 (an identity theft affidavit) with your tax return. We have attached IRS Form 14039 to this memo for your convenience. You can contact the IRS at <http://www.irs.gov/Individuals/Identity-Protection> for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit <https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft> for more information.
- Employee Training. Unfortunately, even the best technology cannot prevent all cyber-attacks, particularly those intended to fool employees into providing sensitive company information. We will continue and improve upon our information security awareness and training programs for all employees.

We apologize for any inconvenience this incident causes you. Please know that we are working diligently to remedy this incident and to prevent any similar incidents from occurring in the future.

If you have questions, please direct them to Dan Gauthreaux or Melissa Childers, or to anyone else in Human Resources. You may also direct any questions or inquiries to 2016-W2-response@mgbwhome.com. Someone will be monitoring this email address and will respond as promptly as possible.

Identity Theft Affidavit

Complete this form if you need the IRS to mark an account to identify questionable activity.

Section A - Check the following boxes in this section that apply to the specific situation you are reporting (Required for all filers)

- ☐ 1. I am submitting this Form 14039 for myself
- ☐ 2. I am submitting this Form 14039 in response to a mailed 'Notice' or 'Letter' received from the IRS. If person in **Section C** received IRS 'Notice CP 2000', or other IRS Notice questioning income, follow the instructions on that IRS 'Notice' or 'Letter'.
• Please provide 'Notice' or 'Letter' number(s) on the line to the right
- ☐ 3. I am submitting this Form 14039 on behalf of my dependent.
Please complete **Section F** on reverse side of this form.
Caution: If you are filing this on behalf of a Minor or Dependent, filing this form will protect his or her tax account but it will **not** prevent the dependent in **Section C** below from being claimed as a dependent by another person.
- ☐ 4. I am submitting this Form 14039 on behalf of another person (other than my dependent).
• Please complete **Section F** on reverse side of this form.

Section B - Reason For Filing This Form (Required)Check only **ONE** of the following boxes that apply to the person listed in **Section C** below.

- ☐ 1. **Federal tax records affected** and I am a victim of identity theft
- ☐ 2. **Federal tax records not affected** and I am a victim of identity theft, or an event has affected/compromised my personal information placing me at-risk to be a future victim of identity theft.

Please provide an explanation of the identity theft issue, how you became aware of it and provide relevant dates.

Section C - Name and Contact Information of Identity Theft Victim or Potential Victim (Required)

Taxpayer's last name	First name	Middle initial	Taxpayer Identification Number (Please provide your 9-digit SSN or ITIN)
----------------------	------------	----------------	--

Current mailing address (apartment or suite number and street, or P.O. Box) If deceased, please provide last known address.

City	State	ZIP code
------	-------	----------

Tax Year(s) in which you experienced identity theft (If not known, enter 'Unknown' in one of the boxes below)	Last tax year a return was filed								
<table><tr><td></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></tr></table>									

Address used on last filed tax return (If different than 'Current')	Names used on last filed tax return (If different than 'Current')
--	--

City (on last tax return filed)	State	ZIP code
---------------------------------	-------	----------

Telephone number with area code (Optional) If deceased, please indicate 'Deceased'	Best time(s) to call
Home telephone number Cell phone number	

Language in which you would like to be contacted ☐ English ☐ Spanish**Section D - State or Federal Issued Identification** (Required)Submit this completed form and a **clear and legible** photocopy of **at least one of the following** documents to verify the identity of the person listed in **Section C** above. **If necessary, enlarge photocopies so all information is clearly visible.**

Check the box next to the document(s) you are submitting:

- ☐
- Driver's license
- ☐
- Social Security Card
- ☐
- Passport
- ☐
- Valid U.S. Federal or State government issued identification**

** Federal employees should not copy his or her employee identification cards as 18 U.S.C. prohibits doing so.

Section E - Penalty of Perjury Statement and Signature (Required)

Under penalty of perjury, I declare that, to the best of my knowledge and belief, the information entered on this Form 14039 is true, correct, complete, and made in good faith.

Signature of taxpayer, or representative, conservator, parent or guardian	Date signed
--	--------------------

Section F – Representative, conservator, parent or guardian information (Required if completing Form 14039 on someone else's behalf)Check only **ONE** of the following five boxes next to the reason you are submitting this form

- ☐ **1. The taxpayer is deceased and I am the surviving spouse.** (No attachments are required, including death certificate)
- ☐ **2. The taxpayer is deceased and I am the court-appointed or certified personal representative.**
Attach a copy of the court certificate showing your appointment.
- ☐ **3. The taxpayer is deceased and a court-appointed or certified personal representative has not been appointed.**
o Attach copy of death certificate or formal notification from a government office informing next of kin of the decedent's death.
o Indicate your relationship to decedent: ☐ Spouse ☐ Child ☒ Parent/Legal Guardian ☐ Other _____
- ☐ **4. The taxpayer is unable to complete this form and I am the appointed conservator or have Power of Attorney/Declaration of Representative authorization per IRS Form 2848.**
o Attach a **copy** of documentation showing your appointment as conservator or POA authorization.
o If you have an IRS issued **Centralized Authorization File (CAF)** number, enter the nine-digit number:

--	--	--	--	--	--	--	--	--
- ☐ **5. The victim or potential victim is a 'minor'. 'Minor' as defined per the state in which 'minor' resides.**
By checking this box and signing below you are indicating that you are an authorized representative, as parent, guardian or legal guardian, to file a legal document on the child's behalf.
o Indicate your relationship to minor: ☐ Parent/Legal Guardian ☐ Fiduciary Relationship per IRS Form 56
☒ Power of Attorney ☐ Other _____

Representative's name

Last name	First name	Middle initial
-----------	------------	----------------

Last four digits of Representative's Taxpayer ID number	Representative's telephone number (include area code)
---	---

Representative's current mailing address (apt., suite no. and street, or P.O. Box)

City	State	ZIP code
------	-------	----------

Instructions for Submitting this Form

Submit this to the IRS via **Mail** or **FAX** to specialized IRS processing areas dedicated to assist you. In **Section C** of this form, be sure to include your Social Security Number or Individual Taxpayer Identification Number in the 'Taxpayer Identification Number' field.

Help us avoid delays:

Choose one method of submitting this form either by Mail or by FAX, not both. Please provide clear and readable photocopies. Note that 'tax returns' may not be submitted to either the mailing address or FAX number provided below.

Submitting by Mail	Submitting by FAX
<ul style="list-style-type: none"> If you checked Box 1 in Section B of Form 14039, are unable to file your tax return electronically because the primary and/or secondary SSN was misused, attach Form 14039 and documentation to your paper tax return and submit to the IRS location where you normally file your tax return. If you have already filed your paper return, submit this Form 14039 and documentation to the IRS location where you normally file. Refer to the 'Where Do You File' section of your return instructions or visit IRS.gov and input the search term 'Where to File'. If you checked Box 1 in Section B and are submitting this Form 14039 in response to a notice or letter received from the IRS, return this form and documentation with a copy of the notice or letter to the address contained in the notice or letter. If you checked Box 2 in Section B of Form 14039 (no current tax-related issue), mail this form and documentation to: Internal Revenue Service Fresno, CA 93888-0025 	<ul style="list-style-type: none"> If you checked Box 1 in Section B of Form 14039 and are submitting this form in response to a notice or letter received from the IRS that shows a reply FAX number, FAX completed Form 14039 and documentation with a copy of the notice or letter to that number. Include a cover sheet marked 'Confidential'. If no FAX number is shown on the notice or letter, follow the mailing instructions on the notice or letter. If you checked Box 2 in Section B of Form 14039 (no current tax-related issue), FAX this form and documentation toll-free to: 855-807-5720

Privacy Act and Paperwork Reduction Notice

Our legal authority to request the information is 26 U.S.C. 6001. The primary purpose of the form is to provide a method of reporting identity theft issues to the IRS so that the IRS may document situations where individuals are or may be victims of identity theft. Additional purposes include the use in the determination of proper tax liability and to relieve taxpayer burden. The information may be disclosed only as provided by 26 U.S.C. 6103. Providing the information on this form is voluntary. However, if you do not provide the information it may be more difficult to assist you in resolving your identity theft issue. If you are a potential victim of identity theft and do not provide the required substantiation information, we may not be able to place a marker on your account to assist with future protection. If you are a victim of identity theft and do not provide the required information, it may be difficult for IRS to determine your correct tax liability. If you intentionally provide false information, you may be subject to criminal penalties. You are not required to provide the information requested on a form that is subject to the Paperwork Reduction Act unless the form displays a valid OMB control number. Books or records relating to a form or its instructions must be retained as long as their contents may become material in the administration of any Internal Revenue law. Generally, tax returns and return information are confidential, as required by section 6103. Public reporting burden for this collection of information is estimated to average 15 minutes per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. If you have comments concerning the accuracy of these time estimates or suggestions for making this form simpler, we would be happy to hear from you. You can write to the Internal Revenue Service, Tax Products Coordinating Committee, SE:W/CAR:MP:T:T:SP, 1111 Constitution Ave. NW, IR-6526, Washington, DC 20224. Do not send this form to this address. Instead, see the form for filing instructions. Notwithstanding any other provision of the law, no person is required to respond to, nor shall any person be subject to a penalty for failure to comply with, a collection of information subject to the requirements of the Paperwork Reduction Act, unless that collection of information displays a currently valid OMB Control Number.

Exhibit B

Mitchell Gold + Bob Williams

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

<<Mail ID>>
<<Name 1>>
<<Address>>
<<City>>, <<State>> <<ZIP>>

<<Date>>

Dear <<Name 1>>:

The Mitchell Gold Co. d/b/a Mitchell Gold + Bob Williams, ("MGBW"), is writing to notify you of a recent email spoofing attack that may affect the security of your personal information. If you are a current employee of MGBW, you received a preliminary notice regarding this incident on January 25, 2017. We take this incident very seriously and are providing you with information and access to resources so that you can protect your personal information.

What Happened? On January 23, 2017, we discovered that our company was the targeted victim of an email spoofing attack whereby a document containing copies of W2 forms of 2016 MGBW employees was obtained by an unauthorized person. While the document was password-protected, it is likely that your information was compromised. Upon discovering the fraudulent nature of the spoofing attack on January 24, 2017, we began working tirelessly to investigate and to mitigate the impact of the attack. The day we discovered the fraudulent nature of the fraudulent spoofing attack we notified the Internal Revenue Service, and the following morning we met with the Alexander County Sheriff and Sheriff's Office detectives to commence an investigation.

What Information Was Involved? A file, including a copy of your IRS Tax Form W-2, was sent in response to the fraudulent email. An IRS Tax Form W-2 includes the following categories of information: (1) the employee's name; (2) the employee's address; (3) the employee's Social Security number; and (4) the employee's wage information. Other than information contained on the IRS Tax Form W-2, no personal financial information of yours or your family's was emailed to the external email account.

What We Are Doing. The confidentiality, privacy, and security of our employee information is one of our highest priorities. MGBW has stringent security measures in place to protect the security of information in our possession. We do not believe that the individuals who sent the fraudulent emails accessed our computer network or that our IT systems were otherwise compromised by this attack. In addition, as part of our ongoing commitment to the security of personal information in our care, we are working to implement additional safeguards and provide additional mandatory training to our employees on safeguarding the privacy and security of information on our systems. As noted above, we have contacted the IRS and the Alexander County Sheriff's Office, the latter of which is working with the Federal Bureau of Investigation, and we have contacted the relevant state Attorneys General.

As an added precaution, we have arranged to have Equifax, one of the leading U.S. credit reporting agencies, provide identity theft protection services for **two years** at no charge to you. A description of this product, instructions on how to enroll in the services, and your unique personal activation code are in the attached documents. Enrolling in the credit monitoring service will provide you with a notification of any changes to your credit information, \$1 million Identity Fraud Expense Coverage, and access to your credit report. You may use the code to enroll any time before **April 30, 2017**. If you wait to enroll in the program after April 30, 2017, the code will no longer be valid. If you already received this information from us and have already enrolled, you **do not** need to enroll again.

The cost of this service will be paid for by MGBW. **We strongly encourage you to act to take advantage of these free identity protection services as soon as possible.** Please note that you must enroll in these services yourself, as we are not able to act on your behalf to enroll you in credit monitoring services.

What You Can Do. You can review the enclosed "Steps You Can Take to Prevent Identity Theft and Fraud." You can also enroll to receive the free credit monitoring and identity restoration services described above. In addition, if you have not already done so, we encourage you to file your 2016 tax return as soon as possible. We also encourage you to file IRS Form 14039 (an identity theft affidavit) as soon as possible.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, please call our dedicated assistance line at 844-616-6626 (toll free), Monday through Friday/Saturday, 9:00 a.m. to 9:00 p.m. EST. And please feel free to direct any questions you may have to Dan Gauthreaux, Melissa Childers or to anyone else in our HR department.

Please know that we take the privacy and security of your personal information in our care very seriously.

Sincerely,

A handwritten signature in black ink that reads "Mitchell Gold". The signature is written in a cursive, flowing style.

Mitchell Gold



Activation Code: INSERT Credit Monitoring Code

About the Equifax Credit Watch™ Gold with 3-in-1 Monitoring identity theft protection product

Equifax Credit Watch 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. Note: You must be over age 18 with a credit file in order to take advantage of the product.

Equifax Credit Watch 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 (available online only)
- One 3-in-1 Credit Report and access to your Equifax Credit Report™
- Up to \$1 million in identity theft insurance ¹ with \$0 deductible, at no additional cost to you
- 24 by 7 live agent Customer Service to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance and in initiating an investigation of inaccurate information.
- 90 day Fraud Alert ² placement with automatic renewal functionality* (available online only)

How to Enroll: You can sign up online or over the phone

To sign up online for **online delivery** go to www.myservices.equifax.com/tri

1. **Welcome Page:** Enter the Activation Code provided at the top of this page in the “Activation Code” box and click the “Submit” button.
2. **Register:** Complete the form with your contact information (name, gender, home address, date of birth, Social Security Number and telephone number) and click the “Continue” button.
3. **Create Account:** Complete the form with your email address, create a User Name and Password, check the box to accept the Terms of Use and click the “Continue” button.
4. **Verify ID:** 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. **Order Confirmation:** This page shows you your completed enrollment. Please click the “View My Product” button to access the product features.

To sign up for **US Mail delivery**, dial 1-866-937-8432 for access to the Equifax Credit Watch automated enrollment process. Note that all credit reports and alerts will be sent to you via US Mail only.

1. **Activation Code:** You will be asked to enter your enrollment code as provided at the top of this letter.
2. **Customer Information:** You will be asked to enter your home telephone number, home address, name, date of birth and Social Security Number.
3. **Permissible Purpose:** You will be asked to provide Equifax with your permission to access your credit file and to monitor your file. Without your agreement, Equifax cannot process your enrollment.
4. **Order Confirmation:** Equifax will provide a confirmation number with an explanation that you will receive your Fulfillment Kit via the US Mail (when Equifax is able to verify your identity) or a Customer Care letter with further instructions (if your identity can not be verified using the information provided). Please allow up to 10 business days to receive this information.

1 - Identity Theft Insurance underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions. This product is not intended for minors (under 18 years of age)

2 - The Automatic Fraud Alert feature made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC

STEPS YOU CAN TAKE TO PREVENT IDENTITY THEFT AND FRAUD

While we continue to investigate, you may take direct action to further protect against possible identity theft or financial loss.

We encourage you to file your tax return as soon as possible, if you have not already done so. You can also contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to prevent a fraudulent tax return from being filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports and explanation of benefits forms for suspicious activity. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax
P.O. Box 105069
Atlanta, GA 30348
800-525-6285
www.equifax.com

Experian
P.O. Box 2002
Allen, TX 75013
888-397-3742
www.experian.com

TransUnion
P.O. Box 2000
Chester, PA 19106
800-680-7289
www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been a victim of identity theft and you provide the credit bureau with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111
(NY residents please
Call 800-349-9960)
www.freeze.equifax.com

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872
www.transunion.com/credit-freeze

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. The Federal Trade Commission can be reached at 600 Pennsylvania Avenue, NW, Washington, DC 20580; 1-877-438-4338 and online at <http://www.ftc.gov/complaint>.

For Maryland residents, the Attorney General can be reached at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; and www.oag.state.md.us. **For North Carolina residents**, the Attorney General can be contacted by mail at 9001 Mail Service Center, Raleigh, NC 27699-9001; toll-free at 1-877-566-7226; by phone at 1-919-716-6400; and online at www.ncdoj.gov.

Instances of known or suspected identity theft should also be reported to law enforcement. This notice was not delayed by a law enforcement investigation.