



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

<<MailID>>  
<<Name 1>>  
<<Name 2>>  
<<Address 1>>  
<<Address 2>>  
<<Address 3>>  
<<City>>, <<State>> <<Zip>>

<<Maildate>>

<<Variable Header>>

Dear <<Name 1>>:

Harding, Shymanski & Company, P.S.C. ("HSC") is writing to inform you of a data security incident that may have involved your personal information as described below. We take the privacy and security of all information very seriously, and are providing you with information about the incident, our response, and steps you can take to help protect your information, should you feel it is appropriate to do so.

**What Happened:** On March 15, 2023, we became aware that 2022 tax returns of certain HSC clients were fraudulently filed by an unknown third party. Unfortunately, the filing of fraudulent tax returns is a widespread issue. Upon discovery, we immediately took steps to review our network security, contacted federal law enforcement and the IRS, and began an investigation with the assistance of third-party forensic specialists. The investigation revealed the compromise of a single user's credentials that led to the potential unauthorized access of client 2021 tax returns and other files containing client information. We immediately undertook a comprehensive review process in order to identify the specific clients impacted and what information was contained within the impacted files. That process was completed on March 27, 2023. This process revealed that your information was impacted.

**What Information Was Involved:** The information believed to be at risk may include your first and last name, in combination with one or more of the following: date of birth, Social Security number, driver's license number, bank account number, routing number, and/or investment or brokerage account information.

**What We Are Doing:** Upon discovery, we immediately began an internal investigation and engaged third-party forensic specialists to determine the full nature and scope of the incident. We have also arranged for you to activate, at no cost to you, an online credit monitoring service for <<CM Length>> months provided by Equifax. Additional information regarding how to activate the complimentary credit monitoring service is enclosed. We have also provided additional information about steps you can take to help protect yourself against fraud and identity theft.

**What You Can Do:** We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports and account statements for suspicious activity and to detect errors. If you discover any suspicious or unusual activity on your accounts, please promptly contact your financial institution or company. You may also enroll in the <<12/24>> months of complimentary credit monitoring and identity protection services we are making available to you. Information regarding how to enroll is enclosed in the attached "Steps You Can Take to Help Protect Your Information." Due to privacy laws, we cannot register you directly.

**For More Information:** Should you have additional questions or concerns regarding this matter, please do not hesitate to contact us at 888-345-0706 9:00AM – 9:00PM Monday through Friday, Eastern Time. You may also write to us at 21 SE 3rd St, Evansville, IN 47708.

We take the privacy and security of the information in our care seriously, and sincerely regret any worry or inconvenience this incident may cause you and your family.

Sincerely,

Harding, Shymanski & Company, P.S.C.

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in a credit monitoring service for <<CM Length>> provided by Equifax, one of the three nationwide credit reporting companies.

**Your Activation Code:** <<ACTIVATION CODE>>

**Enrollment Deadline:** <<Enrollment Deadline>>

### Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications<sup>1</sup> when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts<sup>2</sup>, which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock<sup>3</sup>
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft<sup>4</sup>

### Enrollment Instructions

Go to [www.equifax.com/activate](http://www.equifax.com/activate)

Enter your unique Activation Code of <<ACTIVATION CODE>> then click “Submit” and follow these 4 steps:

1. **Register:**

Complete the form with your contact information and click “Continue”.

*If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header.*

*Once you have successfully signed in, you will skip to the Checkout Page in Step 4*

2. **Create Account:**

Enter your email address, create a password, and accept the terms of use.

3. **Verify Identity:**

To enroll in your product, we will ask you to complete our identity verification process.

4. **Checkout:**

Upon successful verification of your identity, you will see the Checkout Page.

Click ‘Sign Me Up’ to finish enrolling.

**You’re done!**

The confirmation page shows your completed enrollment.

Click “View My Product” to access the product features.

<sup>1</sup>WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded. <sup>2</sup>The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC. <sup>3</sup>Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit [www.optoutprescreen.com](http://www.optoutprescreen.com) <sup>4</sup>The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

## **ADDITIONAL ACTIONS TO HELP PROTECT YOUR INFORMATION**

### **Monitor Your Accounts**

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your credit reports/account statements for suspicious activity and to detect errors. Under U.S. law, you are entitled to one free credit report annually from each of the three major credit reporting bureaus, TransUnion, Experian, and Equifax. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call 1-877-322-8228. Once you receive your credit report, review it for discrepancies and identify any accounts you did not open or inquiries from creditors that you did not authorize. If you have questions or notice incorrect information, contact the credit reporting bureau.

You have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a one-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any of the three credit reporting bureaus listed below.

As an alternative to a fraud alert, you have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without your express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., III, etc.);
2. Social Security number;
3. Date of birth;
4. Address for the prior two to five years;
5. Proof of current address, such as a current utility or telephone bill;
6. A legible photocopy of a government-issued identification card (e.g., state driver’s license or identification card); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft, if you are a victim of identity theft.

Should you wish to place a fraud alert or credit freeze, please contact the three major credit reporting bureaus listed below:

<b>TransUnion</b> 1-800-680-7289 <a href="http://www.transunion.com">www.transunion.com</a>  <b>TransUnion Fraud Alert</b> P.O. Box 2000 Chester, PA 19016-2000  <b>TransUnion Credit Freeze</b> P.O. Box 160 Woodlyn, PA 19094	<b>Experian</b> 1-888-397-3742 <a href="http://www.experian.com">www.experian.com</a>  <b>Experian Fraud Alert</b> P.O. Box 9554 Allen, TX 75013  <b>Experian Credit Freeze</b> P.O. Box 9554 Allen, TX 75013	<b>Equifax</b> 1-888-298-0045 <a href="http://www.equifax.com">www.equifax.com</a>  <b>Equifax Fraud Alert</b> P.O. Box 105069 Atlanta, GA 30348-5069  <b>Equifax Credit Freeze</b> P.O. Box 105788 Atlanta, GA 30348-5788
---	---	--

### **Additional Information**

You can further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the credit reporting bureaus, the Federal Trade Commission (FTC), or your state Attorney General. The FTC also encourages those who discover that their information has been misused to file a complaint with them. The FTC may be reached at 600 Pennsylvania Ave. NW, Washington, D.C. 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261.

You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim.

Instances of known or suspected identity theft should also be reported to law enforcement, your state Attorney General, and the FTC. This notice has not been delayed by law enforcement.

*For North Carolina residents*, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and [www.ncdoj.gov](http://www.ncdoj.gov).