



RECEIVED

JUL 25 2016

OFFICE OF CONSUMER PROTECTION

**IMPORTANT INFORMATION  
PLEASE READ CAREFULLY**

Dear [REDACTED]

The privacy and security of your personal information is of utmost importance to Primoris Services Corporation ("Primoris") and we take significant measures to protect it. I am writing to you with important information about a recent incident which may involve the security of some of your personal information that was supplied to us. We want to provide you with information regarding the incident, explain the services we are making available to help safeguard you against identity fraud, and provide steps you can take to help further protect your information.

Primoris uses Hein & Associates LLP ("Hein") to assist in the testing of financial and information technology general controls. On June 2, 2016, we learned that Hein experienced a theft of a laptop computer on April 26, 2016. On June 13, 2016, Hein learned that the laptop contained personal information that may have been accessible. Upon learning of the incident, Primoris immediately commenced a full investigation. As part of this investigation, we have been working closely with external professionals who regularly investigate and analyze these types of incidents. Local law enforcement has been involved and efforts to recover the laptop continue.

We have confirmed that the laptop that was stolen contained electronic files with your name and your Social Security number. Although the laptop was encrypted, Hein is concerned that information on the computer may be accessible.

**To date, we have no evidence that the person who stole the computer has misused or disclosed any personal information contained in it, or whether they were even able to gain access to the information at all.** However, we wanted to inform you of this incident and provide best practices to help protect your identity.

Enclosed with this letter you will find information on enrolling in a 12-month membership of Equifax Credit Watch™ Gold, that Hein is providing at no cost to you, along with other precautionary measures you can take to protect your personal information, including placing a Fraud Alert, placing a Security Freeze, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.

On behalf of Primoris, please accept my sincere apology that this incident occurred. We are committed to maintaining the privacy of your information and have taken many precautions to help safeguard it. We continually evaluate and modify our practices to enhance the security and privacy of your information.

**If you have any further questions regarding this incident, please call our dedicated and confidential toll-free response line that we have set up to respond to questions at [REDACTED].** The response line is available Monday through Friday, 8:00 am to 8:00 p.m. Central Time.

Sincerely,  
[REDACTED]  
[REDACTED]



# RECEIVED

JUL 25 2016

– ADDITIONAL PRIVACY SAFEGUARDS INFORMATION –

OFFICE OF CONSUMER PROTECTION

1. **Enrolling in Complimentary 12-Month Credit Monitoring.**

**EQUIFAX®**

Activation Code: [REDACTED]

**About the Equifax Credit Watch™ Gold identity theft protection product**

Equifax Credit Watch will provide you with an “early warning system” to changes to your credit file. 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** credit report
- Wireless alerts and customizable alerts available (available online only)
- Access to your Equifax Credit Report™
- Up to \$25,000 in identity theft insurance with \$0 deductible, at no additional cost to you †
- Live agent Customer Service 7 days a week from 8 a.m. to 3 a.m. to assist you in understanding the content of your Equifax credit information, to provide personalized identity theft victim assistance, and help initiate an investigation of inaccurate information.
- 90 day Fraud Alert 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 [REDACTED]

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 [REDACTED] 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 Activation 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.

**Your must enroll with your Activation Code by October 1, 2016.**

† 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)

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



JUL 25 2016

## 2. Placing a Fraud Alert.

OFFICE OF CONSUMER PROTECTION

Whether or not you choose to use the complimentary 12-month credit monitoring services, we recommend that you place an initial 90-day "Fraud Alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax  
P.O. Box 105069  
Atlanta, GA 30348  
www.equifax.com  
1-800-525-6285

Experian  
P.O. Box 2002  
Allen, TX 75013  
www.experian.com  
1-888-397-3742

TransUnion  
P.O. Box 2000  
Chester, PA 19022  
www.transunion.com  
1-800-680-7289

## 3. Consider Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "Security Freeze" be placed on your credit file. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by sending a request in writing, by mail, to all three nationwide credit reporting companies. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze  
PO Box 105788  
Atlanta, GA 30348  
https://www.freeze.equifax.com  
1-800-685-1111

Experian Security Freeze  
PO Box 9554  
Allen, TX 75013  
http://experian.com/freeze  
1-888-397-3742

TransUnion Security Freeze  
P.O. Box 2000  
Chester, PA 19022  
http://www.transunion.com/securityfreeze  
1-800-680-7289

## 4. Obtaining a Free Credit Report.

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

## 5. Additional Helpful Resources.

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

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

If you live in **Iowa**, you may also report suspected incidents of identity theft to local law enforcement or the Iowa Attorney General:

Office of the Iowa Attorney General  
Consumer Protection Division  
1305 East Walnut Street  
Des Moines, IA 50319  
(515) 281-5164  
1-888-777-4590  
Fax: (515) 281-6771  
[www.iowaattorneygeneral.gov](http://www.iowaattorneygeneral.gov)

If you live in **Maryland**, in addition to the FTC, the Maryland Office of the Attorney General can also be contacted to obtain information on the steps you can take to avoid identity theft:

Office of the Attorney General  
Consumer Protection Division  
200 St. Paul Place  
Baltimore, MD 21202  
1-888-743-0023  
[www.oag.state.md.us](http://www.oag.state.md.us)

If you live in **North Carolina**, in addition to the FTC, the North Carolina Office of the Attorney General can also be contacted to obtain information on the steps you can take to prevent identity theft:

North Carolina Department of Justice  
Office of the Attorney General  
9001 Mail Service Center  
Raleigh, NC 27699-9001  
1-877-566-7226  
[www.ncdoj.com](http://www.ncdoj.com)

**6. Reporting Identity Fraud to the IRS.**

If you believe that you are a victim of identity fraud AND it is affecting your federal tax records (or may affect them at some time in the future), such as your attempt to file your federal tax returns electronically was rejected or if you received a notice from the IRS indicating someone was otherwise using your Social Security number, it is recommended that you do the following:

- Contact your tax preparer, if you have one.
- File an Identity Theft Affidavit (Form 14039) with the IRS. The form can be downloaded at: <https://www.irs.gov/pub/irs-pdf/f14039.pdf>
- Call the IRS at (800) 908-4490, ext 245 to report the situation. The unit office is open Monday through Friday from 7 am to 7 pm.
- Report the situation to your local police department.

Additional information regarding preventing tax related identity theft can be found at <http://www.irs.gov/uac/Identity-Protection>