



RECEIVED
FEB 17 P 3:57

Richard G. Goerss
Chief Privacy Officer and Regulatory Counsel

Equifax Inc.
1550 Peachtree Street, N.W.
Atlanta, GA 30309
(404) 885-8034
FAX (404) 885-8800
Email richard.goerss@equifax.com

February 10, 2010

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Dear Sir/Madam:

Pursuant to the Personal Information Protection Act, we are writing to notify you of a security incident involving seven Maryland residents.

Equifax's payroll vendor sent Internal Revenue Service W-2 forms to most current and former Equifax employees via US mail. On January 19th, we became aware that for some US-based employees, the Control Number field on the form was partially or fully viewable through the envelope's return address window. In some instances, the nine-digit Control Number field contained the individual's Social Security number (SSN). Control Numbers were intended to be a unique number, not a SSN. We notified all possibly affected current employees by email on January 22, 2010. We also sent a letter to possibly affected former employees on January 25, 2010. We are sending a subsequent notice with additional information to both current and former employees who may have been affected by this situation. A copy of the notifications provided to the affected Maryland consumers is enclosed.

Equifax is notifying the affected consumers and providing them, upon request, with one year of free credit monitoring of their credit files maintained by Equifax. The notification letter also provides information regarding protection from identity theft, and a toll free number to call for questions and additional assistance.

Equifax is working with its payroll vendor to prevent this situation from happening again in the future. Please let me know if you have any questions regarding this matter.

Sincerely yours,

Richard G. Goerss

Enclosures.



To All Employees - U.S.

cc

bcc

Coretha Rushing .

Subject Important Notice Regarding Your W-2

01/22/2010 03:39 PM

Early last week, our payroll vendor mailed Internal Revenue Service W-2 forms to our current and former employees via US Mail. On January 19 we became aware that for some US-based employees the Control Number field on the form was partially or fully viewable through the envelope's return address window. In some instances, the nine-digit Control Number field contained the individual's Social Security number (SSN). Control Numbers were intended to be a unique number, not a SSN. This incident did not impact employees at TALX, Rapid Reporting and IXI business units.

I am sending this communication to make you aware of this unfortunate occurrence. You can determine if the Control Number field was viewable by visually inspecting your W-2 form within the envelope and how it aligns with the return address window.

If your SSN was in the Control Number field and was viewable, and you are concerned about the risk of identity theft, you may want to monitor your Equifax credit file by accessing your Credit Watch Gold™ service. Credit Watch Gold is provided free to all Equifax employees, and if you have not enrolled for it, you can sign up by sending an email to CreditWatch Employee Benefits.

We apologize for the incident and we are exploring various avenues so this does not happen again. We will be following up shortly with additional information, but we wanted to advise you at this time.

Coretha Rushing
Chief HR Officer

<<DATE>>

<<NAME>>

<<ADDRESS>>

<<CITY/STATE/ZIP>>

Dear <<consumer name>>,

As recently communicated to you, Equifax's payroll vendor sent your Internal Revenue Service W-2 form to you via US mail. On January 19th, we became aware that for some US-based employees, the Control Number field on the form was partially or fully viewable through the envelope's return address window. In some instances, the nine-digit Control Number field contained the individual's Social Security number (SSN). Control Numbers were intended to be a unique number, not a SSN.

What This Means to You

As a result of this possible exposure of your SSN, you may be at risk for identity theft.

What You Can Do To Protect Your Identity

If your SSN was in the Control Number field and was viewable through the envelope's return address window, and you are concerned about the risk of identity theft, you may want to monitor your Equifax credit file by accessing your Credit Watch Gold service. Credit Watch Gold is provided free to all Equifax employees and you can sign up by visiting the secure site at www.myservices.equifax.com/gold. If you have registered with Equifax previously, you can sign in using your existing Username and Password. If you have never registered with Equifax, you can enter the required information and create a new Username and Password. When you get to the "Select Payment Type" section, enter your Promotion Code in the "Enter Promotion Code" field (do not enter credit card information). Your promotion code is the prefix "EFXEMP" in all capital letters followed by the numeric portion of your Equifax employee identification number. For example, if your employee identification number is "E12345678," your promotion code would be "EFXEMP12345678."

You may also want to consider placing a fraud alert on your credit file. You can place this alert on your credit file by accessing our website at <https://www.alerts.equifax.com>, or by calling Equifax at 800-525-6285, and request that a fraud alert message be placed on your Equifax credit file. By placing this alert on your Equifax credit file, any company that requests your credit file will receive a message warning them that you may have been a victim of fraud. Companies that receive this alert may request that you provide proof of your identity. Although this step may create some inconvenience, it will enable the company to confirm your identity and help to protect you from accounts being opened or used by anyone other than yourself.

Additionally, when you request the alert, you can request a current copy of your Equifax credit file at no charge.

Once you contact Equifax to place a fraud alert, we will also notify the two other national credit reporting agencies, Experian and Trans Union, on your behalf to request that they place a fraud alert, and provide you with instructions on obtaining a copy of your credit file from each of them.

In the meantime, if you want to contact them directly, please use the following contact information:

- Experian: 888-397-3742 or <http://www.experian.com/credit-education/victim-assistance.html> or P.O. Box 9530, Allen, TX 75013
- TransUnion: 800-680-7289 or <https://www.transunion.com/corporate/personal/fraud/identityTheft/recoveringFraud/aboutFVAD.page> or P.O. Box 1000, Chester, PA 19022

Upon receipt of your credit files, please review them for any accounts or companies that may have requested your credit file that you do not recognize. If there is any activity that is not familiar to you, you should contact the consumer credit reporting agency that provided the credit file to you either by the toll-free telephone number provided or by sending the research request form to it. It will then remove any information that does not pertain to you.

Report Cases of Identity Theft:

Once you have reviewed copies of your credit files, if you believe you are a victim of identity theft, please contact your local police department.

You can also contact the Equifax Customer Service Center using the telephone number provided in your credit report and ask to speak with a Fraud Resolution Specialist. This specialist will work with you in connection with any questions you have about your credit file or other assistance that we can provide.

We take the protection of consumer information very seriously. That is why we are writing you today and including information to help you protect your personal information. Here are some tips about how you can protect yourself from identity theft:

1. Keep a close eye on your credit card activity.
2. Review all your statements, such as credit card and bank statements.
3. Monitor your Credit Report at all three national consumer credit reporting agencies — Experian, Equifax and TransUnion.
4. Go online to www.equifax.com, or to the Federal Trade Commission's website at www.ftc.gov to see additional tips to combat ID theft and steps to take if you become a victim. You can also call the FTC's Identity Theft helpline at 1-877-IDTHEFT (1-877-438-4338) or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. **For Maryland Residents:** You may also contact the Maryland Attorney General's office at (410) 576-6491 or visit their website at <http://www.oag.state.md.us/index.htm>. You can write to them at Office of the Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

If you have any questions or concerns relating to this situation, please contact the Human Resources Information Center at 1-800-316-3022.

We apologize for the incident and we are exploring various avenues so this does not happen again.

Sincerely,

Coretha Rushing

To US-Based Former Employees:

Early last week, our payroll vendor mailed Internal Revenue Service W-2 forms to our current and former employees via US Mail. On January 19th we became aware that for some US-based employees and former employees the Control Number field on the form was partially or fully viewable through the envelope's return address window. In some instances, the nine-digit Control Number field contained the individual's Social Security number (SSN). Control Numbers were intended to be a unique number, not a SSN. This incident did not impact employees at TALX, Rapid Reporting and IXI business units.

I am sending this communication to make you aware of this unfortunate occurrence. You can determine if the Control Number field was viewable by visually inspecting your W-2 form within the envelope and how it aligns with the return address window.

If your SSN was in the Control Number field and was viewable, and you are concerned about the risk of identity theft, Equifax will provide to you a free one year subscription to Equifax Credit Watch Gold monitoring product. In order to sign up for Credit Watch, please call 888-416-9401 Monday through Saturday, 8 am - 7 pm EST, and mention promo code EFXGOLD.

We apologize for the incident and we are exploring various avenues so this does not happen again. We will be following up shortly with additional information, but we wanted to advise you at this time.

Coretha Rushing

<<DATE>>

<<NAME>>

<<ADDRESS>>

<<CITY/STATE/ZIP>>

Dear <<consumer name>>,

As recently communicated to you, Equifax's payroll vendor sent your Internal Revenue Service W-2 form to you via US mail. On January 19th, we became aware that for some US-based employees, the Control Number field on the form was partially or fully viewable through the envelope's return address window. In some instances, the nine-digit Control Number field contained the individual's Social Security number (SSN). Control Numbers were intended to be a unique number, not a SSN.

What This Means to You

As a result of this possible exposure of your SSN, you may be at risk for identity theft.

What You Can Do To Protect Your Identity

If your SSN was in the Control Number field and was viewable through the envelope's return address window, and you are concerned about the risk of identity theft, Equifax will provide to you a free one year subscription to Equifax Credit Watch Gold monitoring product. In order to sign up for Credit Watch, please call 888-416-9401 Monday through Saturday, 8 am – 7 pm EST, and mention promo code EFXGOLD.

You may also want to consider placing a fraud alert on your credit file. You can place this alert on your credit file by accessing our website at <https://www.alerts.equifax.com>, or by calling Equifax at 800-525-6285, and request that a fraud alert message be placed on your Equifax credit file. By placing this alert on your Equifax credit file, any company that requests your credit file will receive a message warning them that you may have been a victim of fraud. Companies that receive this alert may request that you provide proof of your identity. Although this step may create some inconvenience, it will enable the company to confirm your identity and help to protect you from accounts being opened or used by anyone other than yourself.

Additionally, when you request the alert, you can request a current copy of your Equifax credit file at no charge.

Once you contact Equifax to place a fraud alert, we will also notify the two other national credit reporting agencies, Experian and Trans Union, on your behalf to request that they place a fraud alert, and provide you with instructions on obtaining a copy of your credit file from each of them.

In the meantime, if you want to contact them directly, please use the following contact information:

- Experian: 888-397-3742 or <http://www.experian.com/credit-education/victim-assistance.html> or P.O. Box 9530, Allen, TX 75013
- TransUnion: 800-680-7289 or <https://www.transunion.com/corporate/personal/fraudIdentityTheft/recoveringFraud/aboutFVAD.page> or P.O. Box 1000, Chester, PA 19022

Upon receipt of your credit files, please review them for any accounts or companies that may have requested your credit file that you do not recognize. If there is any activity that is not familiar to you, you should contact the consumer credit reporting agency that provided the credit file to you either by the toll-free telephone number provided or by sending the research request form to it. It will then remove any information that does not pertain to you.

Report Cases of Identity Theft:

Once you have reviewed copies of your credit files, if you believe you are a victim of identity theft, please contact your local police department.

You can also contact the Equifax Customer Service Center using the telephone number provided in your credit report and ask to speak with a Fraud Resolution Specialist. This specialist will work with you in connection with any questions you have about your credit file or other assistance that we can provide.

We take the protection of consumer information very seriously. That is why we are writing you today and including information to help you protect your personal information. Here are some tips about how you can protect yourself from identity theft:

1. Keep a close eye on your credit card activity.
2. Review all your statements, such as credit card and bank statements.
3. Monitor your Credit Report at all three national consumer credit reporting agencies — Experian, Equifax and TransUnion.
4. Go online to www.equifax.com, or to the Federal Trade Commission's website at www.ftc.gov to see additional tips to combat ID theft and steps to take if you become a victim. You can also call the FTC's Identity Theft helpline at 1-877-IDTHEFT (1-877-438-4338) or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. **For Maryland Residents:** You may also contact the Maryland Attorney General's office at (410) 576-6491 or visit their website at <http://www.oag.state.md.us/index.htm>. You can write to them at Office of the Attorney General, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

If you have any questions or concerns relating to this situation, please contact the Human Resources Information Center at 1-800-316-3022.

We apologize for the incident and we are exploring various avenues so this does not happen again.

Sincerely,

Coretha Rushing