



an affiliate of THE GOLDEN LADY GROUP

102 Corporate Center Boulevard Greensboro, NC 27408 336 852-2030

November 4, 2010

Attorney General Michael A. Delaney  
New Hampshire Attorney General's Office  
33 Capitol Street  
Concord, NH 03301

Dear Attorney General Delaney:

Pursuant to NHRSA 359-C:20, Kayser-Roth Corporation is providing notice of a security breach that occurred in its Greensboro, North Carolina corporate office.

**NATURE OF THE SECURITY BREACH OR UNAUTHORIZED USE OR ACCESS**

On October 15th, 2010, Kayser-Roth learned that a laptop computer was missing from its Corporate Payroll Department. It is believed that the laptop went missing between 4:30 pm on October 14th and 7:15 am on October 15<sup>th</sup>. Although the laptop is password protected, it contains personal information on current and former Kayser-Roth employees such as social security numbers for both current and former employees and bank account information for current employees. At this time, Kayser-Roth has no evidence that any of the information has been used by unauthorized persons.

**APPROXIMATE NUMBER OF NEW HAMPSHIRE RESIDENTS AFFECTED**

The laptop contained information relating to five (5) New Hampshire residents.

**ANTICIPATED DATE OF NOTICE TO THE INDIVIDUALS**

Each of the New Hampshire residents affected, as well as all other affected individuals, are being provided with written notice of this incident pursuant to NHRSA 359-C:20, as explained below. Kayser-Roth started distributing notices regarding this incident on October 15 and had mailed out or hand delivered notices to all affected persons by October 22, 2010.

**STEPS TAKEN OR PLANNED IN RESPONSE TO THE INCIDENT**

A copy of the notices and attachments provided to New Hampshire residents are enclosed. The enclosed notices and attachments include a description of the incident, the type of personal information that was contained on the stolen laptop, the steps Kayser-Roth is taking to further reduce the risk of unauthorized access to such information, contact information for the person at Kayser-Roth they can call for further information and assistance, advice that directs them to remain vigilant by reviewing personal bank and credit card account statements and monitoring credit reports, and other steps these individuals can take to try to prevent their confidential information from being used by an unauthorized person including, but limited to, security freezes and fraud alerts. The notices also contain contact information for all three credit reporting agencies and the Federal Trade Commission and refer individuals to their state

Attorney General for additional information relating to security breach issues. Kayser-Roth has also provided state specific information relating to security freezes.

Kayser-Roth also reported the incident to the Greensboro, North Carolina Police Department. A copy of the police report is attached. Additionally, Kayser-Roth provided notice of the incident to the three major credit reporting agencies.

If you have any questions or need further information, please feel free to contact me.

Lisa Furdas  
Corporate HR & Benefits Manager

Enclosures

October 20, 2010

Former Kayser-Roth Corporation Employee (outside NC):

On Friday, October 15<sup>th</sup>, we learned that a laptop was missing from KR's Corporate Payroll Department. We believe that the laptop disappeared from the corporate office sometime between 4:30 pm on October 14<sup>th</sup> and 7:15 am on October 15<sup>th</sup>. This laptop contains personal information on former KR employees such as name, address, and social security numbers. Although the laptop is password protected, which will make it more difficult for anyone to access this information, we are providing this notice to immediately inform you as to what happened, what steps KR is taking in response to this incident, and what steps you should take to try to prevent your confidential personal information from being used by an unauthorized person. We regret that this incident has occurred.

We are currently investigating the incident and are working with law enforcement to try to recover KR's laptop and the information contained on the laptop. We are taking steps to further reduce the risk of unauthorized access to employees' personal information.

In the meantime, you should remain vigilant by reviewing personal bank and credit card account statements and monitoring your credit reports. You may receive a free copy of your credit report by contacting one of the three major credit reporting agencies or from the website: [www.annualcreditreport.com](http://www.annualcreditreport.com). The three credit reporting agencies are listed below:

[www.transunion.com](http://www.transunion.com) (800-680-7289)  
[www.equifax.com](http://www.equifax.com) (800-525-6285)  
[www.experian.com](http://www.experian.com) (888-397-3742)

In most states, you have the right to have a security freeze placed on your credit report. A security freeze is designed to prevent new credit, loans and services from being approved in your name without your consent. Information regarding security freeze services in your state, should you decide to pursue that option, is enclosed. Some states may require a police report which is also enclosed. We recommend that you pursue a security freeze as well as a fraud alert with the three credit reporting bureaus.

You can obtain a security freeze by telephone, online, or by mail by contacting each of the three credit reporting agencies (You must contact all three):

<u>Equifax</u>	<u>Experian</u>	<u>TransUnion</u>
PO Box 105788	PO Box 9554	PO Box 6790
Atlanta, GA 30348	Allen, TX 75103	Fullerton, CA 92834
1-800-685-1111	1-866-997-0418	1-888-909-8872

You also have the right to ask that the three credit reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name and is available at no cost to you. You can place a fraud alert on your credit report by contacting just one of the three credit reporting agencies. As soon as that agency processes your fraud alert, it must notify the other two agencies, which then must place fraud alerts in your file. An initial fraud alert stays in your file for at least 90 days, while an extended alert stays in your file for seven years. You will need to provide the credit reporting agencies with a copy of the police report regarding the stolen laptop and any other required information to obtain an extended fraud alert.

[www.transunion.com](http://www.transunion.com) (800-680-7289)  
[www.equifax.com](http://www.equifax.com) (800-525-6285)  
[www.experian.com](http://www.experian.com) (888-397-3742)

Your state Attorney General's Office may have additional information regarding steps you can take if you become or are likely to become a victim of identity theft. Additional information about preventing identity theft is also available from the Federal Trade Commission.

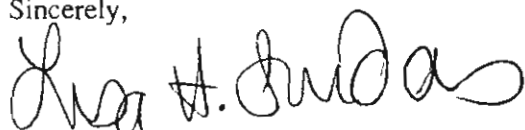
Federal Trade Commission  
1-877-ID THEFT (1-877-438-4338)  
[www.ftc.gov](http://www.ftc.gov)

Enclosed is information from the FTC's website as to how to detect identity theft.

At this time, we do not have any information to suggest that employees' personal information has been used inappropriately. However, we wanted you to be fully aware of what occurred. If you have questions, please contact Lisa Furdas in Corporate Human Resources at 336-547-4676.

If you wish to receive additional information about this issue, as it becomes available, via email, please send an email to [lisafurdas@kayser-roth.com](mailto:lisafurdas@kayser-roth.com), indicating the email address you would like KR to use and that you consent to receiving future notifications and information at that email address.

Sincerely,

A handwritten signature in black ink, appearing to read "Lisa H. Furdas". The signature is fluid and cursive, with the first name "Lisa" being the most prominent part.

Lisa H. Furdas  
Corporate HR Manager

The best way to detect identity theft is to monitor your accounts and bank statements each month, and check your credit report on a regular basis.

- [What are the signs of identity theft?](#)
- [How do you find out if your identity was stolen?](#)
- [What personal information should I monitor regularly?](#)
- [How do I get my free annual credit reports?](#)
- [Should I use a credit monitoring service?](#)

**What are the signs of identity theft?**

Stay alert for the signs of identity theft, like:

- accounts you didn't open and debts on your accounts that you can't explain.
- fraudulent or inaccurate information on your credit reports, including accounts and personal information, like your Social Security number, address(es), name or initials, and employers.
- failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- receiving credit cards that you didn't apply for.
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

[back to top](#)

**How do you find out if your identity was stolen?**

Unfortunately, many consumers learn they their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

[back to top](#)

**What personal information should I monitor regularly?**

Early detection of a potential identity theft can make a big difference. Keep an eye out for any suspicious activity by routinely monitoring:

**Hot Links**

[What is phishing?](#)

[Use Our Materials In Your Community](#)



[Watch the video](#)

[The President's Identity Theft Task Force](#)

[File a Complaint with the FTC](#)

[2006 Identity Theft Survey Report](#)

[Test Your Knowledge about Identity Theft - Take the OnGuard Online Quiz](#)

**Key Publications**

[How To Plan and Host \*Protect Your Identity Days\* Kit \(PDF 6MB\)](#)

[To Buy or Not To Buy: Identity Theft Spawns New Products and Services To Help Minimize Risk \(PDF 229KB\)](#)

[Take Charge: Fighting Back Against Identity Theft \(PDF 4.9MB\)](#)

[Information Compromise and the Risk of Identity Theft: Guidance for Your Business](#)

**Your financial statements.** Monitor your financial accounts and billing statements regularly, looking closely for charges you did not make.

[\(PDF 152KB\)](#)

**Your credit reports.** Credit reports contain information about you, including what accounts you have and how you pay your bills. The law requires each of the major nationwide consumer reporting agencies to provide you with a free copy of your credit report, at your request, once every 12 months. If an identity thief is opening credit accounts in your name, these accounts are likely to show up on your credit report. To find out, order a copy of your credit reports.

Protecting Personal Information:  
A Guide for Business [\(PDF 3.17MB\)](#)

Once you get your reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See [Correcting Fraudulent Information in Credit Reports](#) to learn how. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

[back to top](#)

#### How do I get my free annual credit reports?

An amendment to the federal [Fair Credit Reporting Act](#) requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.

To order your free annual report from one or all the national consumer reporting companies, visit [www.annualcreditreport.com](http://www.annualcreditreport.com), call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from [ftc.gov/credit](http://ftc.gov/credit). Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through [www.annualcreditreport.com](http://www.annualcreditreport.com), 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Under federal law, you're also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company that supplied the information about you. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to \$9.50 for any other copies of your report.

To buy a copy of your report, contact:

Equifax: 800-685-1111; [www.equifax.com](http://www.equifax.com)

Experian: 888-EXPERIAN (888-397-3742); [www.experian.com](http://www.experian.com)

TransUnion: 800-916-8800; [www.transunion.com](http://www.transunion.com)

[back to top](#)

#### Should I use a credit monitoring service?

There are a variety of commercial services that, for a fee, will monitor your credit reports for activity and alert you to changes to your accounts. Prices and services vary widely. Many of the services only monitor one of the three major consumer reporting companies. If you're considering signing up for a service, make sure you understand what you're getting before you buy. Also check out the company with your local Better Business Bureau, consumer protection agency and state Attorney General to see if they have any complaints on file.

[back to top](#)





Search

Credit Education Products Disputes

### New Hampshire Security Freeze Process

Consumers in your state have the right to place a "security freeze" on their credit reports, which will prohibit us from releasing any information in their credit reports without their express authorization, except to those with whom the consumer has an existing account or a collection agency acting on behalf of the existing account, for purposes of reviewing (account maintenance, monitoring, credit line increases and amount upgrades and enhancements) or collecting the account. If you place a security freeze on your credit report, your information also may be used for the purposes of prescreening as provided for by the federal Fair Credit Reporting Act, even if a security freeze is on the report. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent; however, using a security freeze may delay, interfere with, or prohibit the timely approval of any subsequent requests or applications regarding a new loan, credit, mortgage, insurance, government services or payments, rental housing, employment, investment, service, cellular phone, utilities, digital signature, internet credit card transaction, or other services, including an extension of credit at point of sale.

The fee for placing a security freeze on a credit report is \$10. If you are a victim of identity theft and submit a valid investigative or incident report, compliant with a law enforcement agency or the Department of Motor Vehicles (DMV), the fee will be waived. To request a security freeze, log on to [www.experian.com/freeze](http://www.experian.com/freeze) or send all of the requested information via certified mail, as required by law, to Experian Security Freeze, P.O. Box 9554, Allen TX 75013. Include your full name, with middle initial and generation, such as J.R., Sr., II, III, etc., Social Security number, date of birth (month, day and year), current address and previous addresses for the past two years, and \$10 fee or a valid investigative or incident report or complaint with a law enforcement agency or the DMV. In addition, enclose one copy of a government issued identification card, such as a driver's license, state or military ID card, etc., and one copy of a utility bill, bank or insurance statement, etc. Make sure that each copy is legible (enlarge if necessary), displays your name and current mailing address, and the date of issue (statement dates must be recent). We are unable to accept credit card statements, voided checks, lease agreements, magazine subscriptions or postal service forwarding orders as proof. To protect your personal identification information, Experian does not return correspondence sent to us. Copies of any documents should be sent, and you should always retain your original documents. We will send you a confirmation notice once the security freeze has been added, and you will be given a personal identification number (PIN) that will be required in order to remove the freeze temporarily (in order to apply for credit or for any transaction that requires that another party access your personal credit report) or permanently.

To temporarily remove a security freeze for a period of time in order to apply for credit or for any transaction that requires that another party access your personal credit report, log on to [www.experian.com/freeze](http://www.experian.com/freeze) or call 1-888-EXPERIAN (1-888-397-3742); then enter your identification information and PIN. The fee for temporarily removing a security freeze is \$10. There is no fee for victims of identity theft who provide a valid copy of an identity theft report filed with a law enforcement agency. To temporarily remove a security freeze for a specific party, provide your PIN to the party you wish to grant access to your report.

To permanently remove a security freeze, log on to [www.experian.com/freeze](http://www.experian.com/freeze) or call 1-888-EXPERIAN (1-888-397-3742). You also may write to us and provide all your identification information and PIN. If you write to us, always include a copy of your personal identification information and proof of your address as specified in this letter. The fee for permanently removing a security freeze is \$10. There is no fee for victims of identity theft who provide a valid copy of an identity theft report filed with a law enforcement agency. Mail the requested information and payment to the address above.

Notification of Rights for New Hampshire Consumers

State Select **Select your State**

Personal Services

© 2010 Experian Information Solutions, Inc. All rights reserved.

Legal Terms & Conditions Privacy Policy Rates & Credits Investor Relations Online Community Site Map Contact Us

By using the Experian.com website, you agree to our privacy policy and terms of use. For more information, please visit [www.experian.com/privacy](http://www.experian.com/privacy) or [www.experian.com/terms](http://www.experian.com/terms). The Online Services provided by Experian Information Solutions, Inc. are provided as a service to our customers and are not intended to be used for any other purpose.