<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

<<Date>> (Format: Month Day, Year)

NOTICE OF DATA BREACH

Dear <<MemberFirstName>> <<MemberLastName>>,

We are writing to follow up on our internal communications dated May 3, 2016 and May 5, 2016 regarding a security incident that may have involved your personal information, as well as steps we are taking in response, and the resources we have made available to you.

What Happened?

While the investigation is ongoing, it appears that beginning in late January of this year, unknown individuals accessed the Equifax W-2Express website using default login information based on Social Security numbers and dates of birth, which we believe were obtained from some other source, such as a prior data breach at another institution. The Equifax W-2Express website provides online access to electronic W-2 forms for the Kroger family of companies and other groups. We have no indication that Kroger's systems have been compromised. Equifax has also confirmed to Kroger that its systems were not compromised, and that the Social Security numbers and dates of birth did not originate from Equifax.

We believe individuals gained access to some current and former Kroger associates' electronic W-2 forms and may have used the information to file tax returns in their names to claim a refund. If the Internal Revenue Service (IRS) believes a fraudulent return has been filed in your name, they should alert you through the mail after you have filed your taxes.

Based on our further investigation, we have determined that your Equifax W-2Express account was set for the default PIN and showed indications of potentially suspicious activity, and so we are providing you this notice and recommended steps to help protect yourself.

What Information Was Involved?

It appears that unidentified individuals may have used your date of birth and your Social Security number to log in and access information on your W-2 Express account. IRS W-2 forms include your name, address, and Social Security number along with income and withholding information.

What We Are Doing

As soon as we discovered the security incident on the evening of April 27, 2016, we began working closely with Equifax, the Internal Revenue Service (IRS) and the FBI to understand what happened and determine who may be affected. Equifax has reset PINs for those associates with the default PIN, which prevents further such access to this data. Accordingly, the next time you log in to the Equifax W-2Express site, you may be prompted to create a new password if you haven't done so already. We are working closely with federal law enforcement and the IRS in their investigation, and we have provided information on potentially affected individuals in order to help the IRS detect and deter the filing of fake tax returns in order to claim fraudulent tax refunds. We have also arranged for identity and credit monitoring services at no cost to you.

What You Can Do

If you have been contacted by the IRS and think you may have been affected, please email ReportMyW2@kroger.com and share your **first name, last name and location** (store number, plant or distribution center).

If you believe someone else claimed a tax refund in your name, or if you are notified by the IRS of a potential fraudulently filed tax return, the IRS recommends the following initial steps to notify authorities:

- Respond immediately to the IRS notice by calling the number provided, contacting the IRS Identity Protection Specialized Unit at 1-800-908-4490, or going to www.IDVerify.irs.gov.
- Complete IRS Form 14039, Identity Theft Affidavit. Use a fillable form at IRS.gov, print, then attach the form to your return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- File a complaint with the Federal Trade Commission.
- You may also visit https://www.irs.gov/Individuals/Identity-Protection for more information.

We encourage you to regularly review your financial accounts and credit reports, and report any suspicious or unrecognized activity immediately to your financial institution. You should be particularly vigilant for the next 12 to 24 months and report any suspected incidents of fraud to your financial institution. As your Social Security number may have been affected, you may wish to consider placing a fraud alert or security freeze on your accounts. More information about these options is detailed below.

Other Important Information

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring services at no cost to you for one year. Kroll is a global leader in risk mitigation and response. Your identity monitoring services include Credit Monitoring and Web Watcher.

Visit **kroll.idMonitoringService.com** to enroll and take advantage of your identity monitoring services.

Membership Number: <<Member ID>>

Certain identity monitoring services and other precautions related to credit reports may not be available for individuals under the age of 18; however Kroll's Identity Consultation and Identity Restoration services are available to minors as well at no cost for three years. Additional information describing your services is included with this letter.

In order to take advantage of the identity monitoring services through Kroll you must enroll by August 31, 2016.

In the event you have questions related to fraud or identity theft you also have access to Kroll's licensed investigators for Identity Consultation and Identity Restoration support for three years.

We have also included additional steps you could consider if you suspect you've been the victim of identity theft. We offer this out of an abundance of caution so that you have the information you need to protect yourself.

For More Information

If you have questions, please call 1-877-309-0010, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time. Please have your membership number ready.

We are disappointed this happened. We take the security of your information very seriously, and we regret any uncertainty or inconvenience that this incident may have caused you.

Sincerely,

Mike Schlotman
Executive Vice President
Chief Financial Officer

Tim Massa
Group Vice President
HR & Labor Relations

Important Identity Theft Information: Additional Steps You Can Take to Protect Your Identity

The following are additional steps you may wish to take to protect your identity.

Review Your Accounts and Credit Reports

Regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies.

You may obtain a free copy of your credit report online at www.annualcreditreport.com by calling toll free 1.877.322.8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to: Annual Credit Report Request Service. P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

- TransUnion, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016. 1.800.916.8800. www.transunion.com
- Experian, P.O. Box 9532, Allen, TX 75013, 1.888.397.3742. www.experian.com
- Equifax, P.O. Box 740241, Atlanta, Georgia 30374-0241. 1.800.685.1111. www.equifax.com

Consider Placing a Fraud Alert

You may wish to consider contacting the fraud department of the three major credit bureaus to request that a "fraud alert" be placed on your file. A fraud alert notifies potential lenders to verify your identification before extending credit in your name.

TransUnion: 1.800.680.7289

Experian: 1.888.397.3742

Equifax: 1.800.525.6285

Security Freeze for Credit Reporting Agencies

You may wish to request a security freeze on your credit reports. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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 reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $10.00, (or in certain states such as Massachusetts, no more than $5.00) each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the following addresses:

- TransUnion Security Freeze, Fraud Victim Assistance Department, 2 Baldwin Place, P.O. Box 1000, Chester, PA 19016
- Experian Security Freeze, P.O. Box 9554, Allen, TX 75013
- Equifax Security Freeze, P.O. Box 105788, Atlanta, GA 30348

To request a security freeze, you will need to provide the following:

- Your full name (including middle initial, Jr., Sr., Roman numerals, etc.),
- Social Security number
- Date of birth
- Address(es) where you have lived over the prior five years
- Proof of current address such as a current utility bill
- A photocopy of a government-issued ID card
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Don't send cash through the mail.

The credit reporting agencies have three business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include (1) proper identification (name, address, and Social Security number), (2) the PIN number or password provided to you when you placed the security freeze; and (3) the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze all together, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three business days after receiving your request to remove the security freeze.

Suggestions if You Are a Victim of Identity Theft

- File a police report. Get a copy of the report to submit to your creditors and others that may require proof of a crime.
- Contact the U.S. Federal Trade Commission (FTC). The FTC provides useful information to identity theft victims and maintains a database of identity theft cases for use by law enforcement agencies. File a report with the FTC by calling the FTC's Identity Theft Hotline: 1- 877-IDTHEFT (438-4338); online at http://www.ftc.gov/idtheft; or by mail at Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580. Also request a copy of the publication, "Take Charge: Fighting Back Against Identity Theft" from http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf.
- Keep a record of your contacts. Start a file with copies of your credit reports, the police reports, any correspondence, and copies of disputed bills. It is also helpful to keep a log of your conversations with creditors, law enforcement officials, and other relevant parties.

State Specific Disclosures:

Further information can be obtained from the FTC about steps to take to avoid identity theft at: http://www.ftc.gov/idtheft; calling 1-877-IDTHEFT (438-4338); or write to Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave., N.W., Washington, D.C. 20580.

Iowa residents are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

Maryland residents can learn more about preventing identity theft from the Maryland Office of the Attorney General, by visiting their web site at https://www.oag.state.md.us/idtheft/, calling the Identity Theft Unit at 410.567.6491, or requesting more information at the Identity Theft Unit, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

Massachusetts residents are reminded that you have the right to obtain a police report and request a security freeze as described above. The consumer reporting agencies may charge you a fee of up to $5 to place a security freeze on your account, and may require that you provide certain personal information (such as your name, Social Security Number, date of birth and address) and proper identification (such as a copy of a government-issued ID card and a bill or statement) prior to honoring your request. There is no charge, however, to place, lift or remove a security freeze if you have been a victim of identity theft and you provide the consumer reporting agencies with a valid police report.

North Carolina residents can learn more about preventing identity theft from the North Carolina Office of the Attorney General, by visiting their web site at http://www.ncdoj.gov/Help-for-Victims/ID-Theft-Victims.aspx, calling 919.716.6400 or requesting more information from the North Carolina Attorney General's Office, 9001 Mail Service Center Raleigh, NC 27699-9001.

Oregon residents are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

Kroll.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Credit Monitoring through TransUnion

You'll receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll investigator, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals buy, sell, and trade personal information. You'll be promptly notified if evidence of your identity information being traded or sold is discovered.

Identity Consultation

You have unlimited access to consultation with a dedicated licensed investigator at Kroll. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Restoration

If you become a victim of identity theft, an experienced licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and will do most of the work for you. Your investigator can dig deep to uncover all aspects of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.