PRMI | Primary Residential Mortgage, Inc.

May 9, 2016

SENT VIA UPS OVERNIGHT DELIVERY
Office of the Attorney General – New Hampshire
Consumer Protection
33 Capitol St.
Concord, NH 03307

Re: Security Breach – Primary Residential Mortgage, Inc.

To Whom It May Concern:

I am writing to let you know of a security breach that was recently discovered involving Primary Residential Mortgage, Inc. (PRMI) employee data. Upon investigation, it was discovered that the breach occurred February 25, 2016, at which time PRMI was the target of a "phishing" attack that resulted in the release of a copy of both our current and former employees' 2015 W-2 forms to an unknown unauthorized third party. In total, 48 New Hampshire residents were impacted as a result of this breach. The personal information listed on the employee W-2 forms, including year-end salary, address and Social Security Number, was compromised. To our knowledge, no other information was compromised.

Immediately following our discovery, we worked to uncover all those impacted by the breach and prepare a comprehensive notification. New Hampshire residents impacted that are current employees were notified initially on May 6, 2016 via a company-wide email. In tandem, we set up branch manager phone calls to help communicate the information and answer any questions. A hard-copy notice was sent to all New Hampshire residents impacted by the breach on Monday, May 9, 2016.

We have implemented and will continue to implement additional security measures, including employee training, designed to prevent a reoccurrence of such an attack. We are actively working with the investigative units of the U.S. Inspection Service and the Internal Revenue Service to ensure that the issue is properly investigated. We have also notified the Federal Trade Commission and the Office of the Inspector General. Additionally, PRMI has contracted with a third party, LifeLock, to provide one year of identity theft protection services for all those impacted by the breach.

PRMI | Primary Residential Mortgage, Inc.

I have included with this notification a copy of the notice we are providing to all those impacted. If you have any further questions or concerns, please contact me with the information provided below.

Sincerely,

Katrina Loken
Vice President of Compliance
Primary Residential Mortgage, Inc.
Phone: (801) 596-8707 ext. 1000155
kloken@primeres.com

PRMI | Primary Residential Mortgage, Inc.

Name
Address
City, State Zip

May 6, 2016

Re: Notice of Data Breach

Dear Name:

We value all our employees, both current and former, and respect the privacy of your information. That is why, as a precautionary measure, we are writing to let you know about a data security incident that involves some of your personal information.

What Happened?

We just discovered that on February 25, 2016, Primary Residential Mortgage, Inc. was the target of a "phishing" attack that resulted in the release of a copy of your 2015 W-2 form to an unknown third party.

What Information Was Involved?

This means that the information on your W-2, including your year-end salary information, address and Social Security number were compromised. This breach involved every PRMI current and former employee who was employed by the Company during 2015. To our knowledge, no other information was compromised.

PRMI deeply regrets that the company and our employees have fallen victim to this attack.

What We Are Doing.

Rest assured that we have implemented and will continue to implement additional security measures and employee training designed to prevent a reoccurrence of such an attack, and to protect everyone's privacy.

The company is also working closely with the investigative units of the U. S. Inspection Service and the Internal Revenue Service to ensure that this issue is properly investigated and addressed.

To help relieve concerns and restore confidence following this attack, we have contracted with LifeLock to provide identity monitoring at no cost to you for one year. LifeLock is a proven leader in identity theft protection services and has a proven record of success in protecting millions of consumers against identity theft.

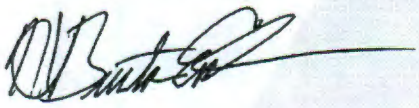
What Can You Do?

Attached to this letter is an informational packet describing a number of actions you can take to protect your information. In Section 4 of the attachment, we have detailed the steps you can take to sign up for the free LifeLock® service. Also attached are IRS publications 5027 and 4524, respectively titled "Identity Theft Information for Taxpayers" and "Security Awareness for Taxpayers".

For More Information.

If you have any questions or for further information and assistance, please contact Leo McIsaac, Vice President of Human Resources at (800) 255-2792, Ext. 1000109 between 9:00 a.m. - 5:30 p.m. MDT. You can also communicate with Mr. McIsaac via email at lmcisaac@primeres.com.

Sincerely,



Burton Embry

EVP & Chief Compliance Officer

STEPS YOU CAN TAKE TO FURTHER PROTECT YOUR INFORMATION

1. ***Review your Bank and Credit Card Statements and Notify Law Enforcement of Suspicious Activity.***

As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained.

You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission.

To file a complaint with the FTC, go to www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, which is a database made available to law enforcement agencies.

Iowa residents are advised to report any suspected identity theft to local law enforcement and/or the Iowa Attorney General Consumer Protection Division. The Iowa Attorney General, Consumer Protection Division can be contacted by email at consumer@iowa.gov, by phone at (515) 281-5926, or by mail at Hoover State Office Building, 1305 E. Walnut Street, Des Moines, IA 50319-0106.

Massachusetts residents have the right to obtain a police report if you are a victim of identity theft.

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

2. ***Obtain a Copy of your Credit Report.***

You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting http://www.annualcreditreport.com, calling toll-free 877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You can print a copy of the request form at https://www.annualcreditreport.com/cra/requestformfinal.pdf. Or you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Contact information for the three national credit reporting agencies for the purpose of requesting a copy of your credit report or for general inquiries is provided below:

Equifax	Experian	TransUnion
(866) 547-2695	(888) 397-3742	(800) 916-8800
www.equifax.com	www.experian.com	www.transunion.com
P.O. Box 740241	535 Anton Blvd., Suite 100	P.O. Box 6790
Atlanta, GA 30374	Costa Mesa, CA 92626	Fullerton, CA 9283

3. ***Consider placing a fraud alert on your credit report.***

An initial fraud alert is free and will stay on your credit file for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at http://www.annualcreditreport.com.

4. ***Credit Report Monitoring.***

In addition, Primary Residential Mortgage, Inc. has arranged with LifeLock to provide you with credit monitoring for one year, at no cost to you. The package provides you with three levels of protection:

Detection – LifeLock will search a trillion data points each day looking for potential threats

Alert – As soon as LifeLock detects a threat, you will be notified by text, phone or email

Restore – If you become a victim, LifeLock specialists will be available 24/7 to assist you

To take advantage of this offer, you must enroll within 90 days from receipt of this letter. The Promotional Enrollment Code that you will need to sign up for this service is PRMUT2016. You may enroll with LifeLock either by phone at (800) 899-0180, or online at www.lifelock.com. You will need a User ID, which will initially be your last name and your zip code as printed on your 2015 W-2. The enrollment period for this free service ends July 31, 2016.

5. ***Security Freeze.***

In some states, you have the right to put a security freeze on your credit file. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. Be advised that using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. Additionally, if you request a security freeze from a consumer reporting agency there may be a fee up to $5 to place, lift or remove the security freeze. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

6. ***Additional Free Resources on Identity Theft.***

You may wish to review the tips provided by the Federal Trade Commission on how to avoid identity theft. For more information, please visit http://www.ftc.gov/idtheft or call 1-877-ID-THEFT (877-438-4338).

Maryland residents may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 410-576-6491.

North Carolina residents may wish to review information provided by the North Carolina Attorney General at http://www.ncdoj.gov, by calling 919-716-6400, or writing to 9001 Mail Service Center, Raleigh, NC 27699.

IRS

TAXES. SECURITY. TOGETHER.

The IRS, the states and the tax industry are committed to protecting you from identity theft. We've strengthened our partnership to fight a common enemy – the criminals – and to devote ourselves to a common goal – serving you. Working together, we've made many changes to combat identity theft, and we are making progress. However, cybercriminals are constantly evolving, and so must we. The IRS is working hand-in-hand with your state revenue officials, your tax software provider and your tax preparer. But, we need your help. We need you to join with us. By taking a few simple steps, you can better protect your personal and financial data online and at home.

Please consider these steps to protect yourselves from identity thieves:

Keep Your Computer Secure

- Use security software and make sure it updates automatically; essential tools include:
  - Firewall
  - Virus/malware protection
  - File encryption for sensitive data
- Treat your personal information like cash, don't leave it lying around
- Check out companies to find out who you're really dealing with
- Give personal information only over encrypted websites – look for "https" addresses.
- Use strong passwords and protect them
- Back up your files

Avoid Phishing and Malware

- Avoid phishing emails, texts or calls that appear to be from the IRS and companies you know and trust, go directly to their websites instead
- Don't open attachments in emails unless you know who sent it and what it is
- Download and install software only from websites you know and trust
- Use a pop-up blocker
- Talk to your family about safe computing

Protect Personal Information

Don't routinely carry your social security card or documents with your SSN. Do not overshare personal information on social media. Information about past addresses, a new car, a new home and your children help identity thieves pose as you. Keep old tax returns and tax records under lock and key or encrypted if electronic. Shred tax documents before trashing.

Avoid IRS Impersonators. The IRS will not call you with threats of jail or lawsuits. The IRS will not send you an unsolicited email suggesting you have a refund or that you need to update your account. The IRS will not request any sensitive information online. These are all scams, and they are persistent. Don't fall for them. Forward IRS-related scam emails to phishing@irs.gov. Report IRS-impersonation telephone calls at www.tigta.gov.

Additional steps:

- Check your credit report annually; check your bank and credit card statements often;
- Review your Social Security Administration records annually: Sign up for My Social Security at www.ssa.gov.
- If you are an identity theft victim whose tax account is affected, review www.irs.gov/identitytheft for details.

Publication 4524 (Rev. 9-2015) Catalog Number 48359Q Department of the Treasury **Internal Revenue Service** www.irs.gov

Identity Theft Information for Taxpayers

Identity theft places a burden on its victims and presents a challenge to many businesses, organizations and governments, including the IRS. The IRS combats this crime with an aggressive strategy of prevention, detection and victim assistance.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses your stolen Social Security number (SSN) to file a tax return claiming a fraudulent refund. If you become a victim, we are committed to resolving your case as quickly as possible.

You may be unaware that this has happened until you e-file your return and discover that a return already has been filed using your SSN. Or, the IRS may send you a letter saying it has identified a suspicious return using your SSN.

Know the warning signs

Be alert to possible tax-related identity theft if you are contacted by the IRS about:

- More than one tax return was filed for you,
- You owe additional tax, have a refund offset or have had collection actions taken against you for a year you did not file a tax return, or
- IRS records indicate you received wages or other income from an employer for whom you did not work.

Steps for victims of identity theft

If you are a victim of identity theft, the Federal Trade Commission recommends these steps:

- File a complaint with the FTC at identitytheft.gov.
- Contact one of the three major credit bureaus to place a 'fraud alert' on your credit records:
  - www.Equifax.com 1-888-766-0008
  - www.Experian.com 1-888-397-3742
  - www.TransUnion.com 1-800-680-7289
- Close any financial or credit accounts opened by identity thieves

If your SSN is compromised and you know or suspect you are a victim of tax-related identity theft, the IRS recommends these additional steps:

- Respond immediately to any IRS notice; call the number provided or, if instructed, go to IDVerify.irs.gov.
- Complete IRS Form 14039, *Identity Theft Affidavit*, if your e-file return rejects because of a duplicate filing under your SSN or you are instructed to do so. Use a fillable form at IRS.gov, print, then attach form to your paper return and mail according to instructions.
- Continue to pay your taxes and file your tax return, even if you must do so by paper.
- If you previously contacted the IRS and did not have a resolution, contact us for specialized assistance at 1-800-908-4490. We have teams available to assist.

More information is available at: IRS.gov/identitytheft or FTC's identitytheft.gov.

About data breaches and your taxes

Not all data breaches or computer hacks result in tax-related identity theft. It's important to know what type of personal information was stolen.

If you've been a victim of a data breach, keep in touch with the company to learn what it is doing to protect you and follow the "Steps for victims of identity theft." Data breach victims should submit a Form 14039, *Identity Theft Affidavit,* only if your Social Security number has been compromised and IRS has informed you that you may be a victim of tax-related identity theft or your e-file return was rejected as a duplicate.

How you can reduce your risk

Join efforts by the IRS, states and tax industry to protect your data. Taxes. Security. Together. We all have a role to play. Here's how you can help:

- Always use security software with firewall and anti-virus protections. Use strong passwords.
- Learn to recognize and avoid phishing emails, threatening calls and texts from thieves posing as legitimate organizations such as your bank, credit card companies and even the IRS.
- Do not click on links or download attachments from unknown or suspicious emails.
- Protect your personal data. Don't routinely carry your Social Security card, and make sure your tax records are secure.

See Publication 4524, *Security Awareness for Taxpayers* to learn more.

NOTE: The IRS does not initiate contact with taxpayers by email to request personal or financial information. This includes any type of electronic communication, such as text messages and social media channels.

Publication 5027 (Rev. 12-2015) Catalog Number 67495R Department of the Treasury **Internal Revenue Service** www.irs.gov