PayneWest INSURANCE

IDAHO
MONTANA
OREGON
WASHINGTON
paynewest.com

March 17, 2016

John Doe
123 Any Address
Billings, MT 59101

Dear John,

We are writing to follow up on the email you received on Wednesday to notify you of an incident affecting your personal information. Although we are not aware at this time of identity theft specifically linked to this incident, we take privacy and security very seriously and wanted to inform you about this situation, the steps we are taking to protect your information, and steps you may take to help protect yourself.

What happened?
On March 15, PayneWest Insurance ("PayneWest") learned that an unidentified attacker had used an email phishing scheme to attempt to obtain access to personal information relating to current and former PayneWest employees. The attacker sent an email message that was carefully designed to appear as though it had been sent by a PayneWest executive, requesting that a PayneWest employee forward 2015 W-2 forms to the executive. Believing the email to be legitimate, the employee replied with the information as requested. The types of personal data affected included information listed on W-2 forms such as names, addresses, Social Security numbers, and wage information, as well as certain payroll details such as title, department, location, and income.

PayneWest is notifying law enforcement authorities, including the FBI and the IRS, about the scam and is cooperating with their investigations and remediation efforts, which are ongoing at this time. The IRS has reported that multiple other companies have been targeted by this type of scheme.

What is PayneWest doing to protect you?
We recognize this issue can be frustrating and we are taking steps to help protect you and to safeguard employee personal information going forward. As an added precaution, we have arranged to have AllClear ID protect your identity for 24 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 24 months.

AllClear SECURE: The team at AllClear ID is ready and standing by if you need identity repair assistance. This service is automatically available to you with no enrollment required. If a problem arises, simply call 877-676-0379 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear PRO: This service offers additional layers of protection including credit monitoring and a $1 million identity theft insurance policy. To use the PRO service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com using the following redemption code: **1378557001**.

Regardless of whether you choose to take advantage of the identity protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit reports, bank account activity, and financial statements for any unauthorized transactions. More information about preventing identity theft is included with this letter.

To help prevent a similar incident from happening in the future, we are evaluating our controls and will be implementing additional protections, and we will be taking further actions to enhance our information security safeguards moving forward. Thankfully, this phishing attack did not involve hacking or malicious software, and it did not compromise the integrity of our systems. Employees should contact ithelpdesk@paynewest.com immediately regarding any potentially fraudulent emails sent to their PayneWest email accounts.

If you have further questions regarding this incident, you may email security@paynewest.com or call Renee King at 406-327-6449 or Peggy Kerins at 406-457-2116.

Sincerely,

Sarah Walsh
Chief Operating Officer

AllClear Secure Terms of Use

If you become a victim of fraud using your personal information without authorization, AllClear ID will help recover your financial losses and restore your identity. Benefits include:

- 24 months of coverage with no enrollment required;
- No cost to you – ever. AllClear Secure is paid for by the participating Company.

Services Provided
If you suspect identity theft, simply call AllClear ID to file a claim. AllClear ID will provide appropriate and necessary remediation services ("Services") to help restore the compromised accounts and your identity to the state prior to the incident of fraud. Services are determined at the sole discretion of AllClear ID and are subject to the terms and conditions found on the AllClear ID website. AllClear Secure is not an insurance policy, and AllClear ID will not make payments or reimbursements to you for any financial loss, liabilities or expenses you incur.

Coverage Period
Service is automatically available to you with no enrollment required for 24 months from the date of the breach incident notification you received from Company (the "Coverage Period"). Fraud Events that occurred prior to your Coverage Period are not covered by AllClear Secure services.

Eligibility Requirements
To be eligible for Services under AllClear Secure coverage, you must fully comply, without limitations, with your obligations under the terms herein, you must be a citizen or legal resident eighteen (18) years of age or older, and have a valid U.S. Social Security number. Minors under eighteen (18) years of age may be eligible, but must be sponsored by a parent or guardian. The Services cover only you and your personal financial and medical accounts that are directly associated with your valid U.S. Social Security number, including but not limited to credit card, bank, or other financial accounts and/or medical accounts.

How to File a Claim
If you become a victim of fraud covered by the AllClear Secure services, you must:

- Notify AllClear ID by calling 1.855.434.8077 to report the fraud prior to expiration of your Coverage Period.
- Provide proof of eligibility for AllClear Secure by providing the redemption code on the notification letter you received from the sponsor Company.
- Fully cooperate and be truthful with AllClear ID about the Event and agree to execute any documents AllClear ID may reasonably require;
- Fully cooperate with AllClear ID in any remediation process, including, but not limited to, providing AllClear ID with copies of all available investigation files or reports from any institution, including, but not limited to, credit institutions or law enforcement agencies, relating to the alleged theft;

Coverage under AllClear Secure Does Not Apply to the Following:
Any expense, damage or loss:

- Due to
  - Any transactions on your financial accounts made by authorized users, even if acting without your knowledge
  - Any act of theft, deceit, collusion, dishonesty or criminal act by you or any person acting in concert with you, or by any of your authorized representatives, whether acting alone or in collusion with you or others (collectively, your "Misrepresentation")
- Incurred by you from an Event that did not occur during your coverage period;
- In connection with an Event that you fail to report to AllClear ID prior to the expiration of your AllClear Secure coverage period.

Other Exclusions:

- AllClear ID will not pay or be obligated for any costs or expenses other than as described herein, including without limitation fees of any service providers not retained by AllClear ID; AllClear ID reserves the right to investigate any asserted claim to determine its validity;
- AllClear ID is not an insurance company, and AllClear Secure is not an insurance policy; AllClear ID will not make payments or reimbursements to you for any loss or liability you may incur; and
- AllClear ID is not a credit repair organization, is not a credit counseling service, and does not promise to help you improve your credit history or rating beyond resolving incidents of fraud;
- AllClear ID reserves the right to reasonably investigate any asserted claim to determine its validity. All recipients of Secure coverage are expected to protect their personal information in a reasonable way at all times. Accordingly, recipients will not deliberately or recklessly disclose or publish their Social Security number or any other personal information to those who would reasonably be expected to improperly use or disclose that Personal Information.

Opt-out Policy
If for any reason you wish to have your information removed from the AllClear Secure eligibility database, please contact AllClear ID:

E-mail	Mail	Phone
support@allclearid.com	AllClear ID, Inc. 823 Congress Avenue Suite 300 Austin, Texas 78701	1.855.434.8077

- Note: you should submit a Form 14039 **only** if your Social Security number has been compromised ***and*** your e-file return was rejected as a duplicate, or if the IRS has informed you that you may be a victim of tax-related identity theft.

- 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 your situation was not resolved, you may contact the IRS for specialized assistance at (800) 908-4490.

INFORMATION ABOUT PREVENTING IDENTITY THEFT

Even if you choose not to take advantage of the identity theft protection services we are offering, we recommend that you remain vigilant to the possibility of fraud and identity theft by reviewing your credit card, bank, and other financial statements for any unauthorized activity. You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting agencies once every 12 months. To order your credit report, please visit www.annualcreditreport.com or call toll free at 877-322-8228. Contact information for the three nationwide credit reporting agencies is as follows:

Equifax	**Experian**	**TransUnion**
P.O. Box 740241	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
(800) 525-6285	(888) 397-3742	(800) 680-7289

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should contact the Federal Trade Commission and/or the Office of the Attorney General in your home state. You may contact the FTC by visiting www.ftc.gov/idtheft, calling (877) 438-4338, or writing to 600 Pennsylvania Avenue, NW, Washington, D.C., 20580.

The FTC's website includes information about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You also should contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records.

Fraud Alerts

You also may request that the nationwide credit reporting agencies place a "fraud alert" 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 because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies. Contact information for each of the three credit reporting agencies is listed above. Once one credit reporting agency processes your fraud alert, it will notify the other two, which then also must place a fraud alert in your file.

There are two types of fraud alerts. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and have obtained the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. If you ask for an extended alert, you will have to provide an identity theft report (generally a copy of a report you have filed with a federal, state, or local law enforcement agency), and additional information the credit reporting agency may require you to submit.

You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the toll-free numbers listed below:

Equifax	**Experian**	**TransUnion**
(888) 766-0008	(888) 397-3742	(800) 680-7289

Security Freezes

You also may place a security "freeze" on your credit report to protect your privacy and help ensure that credit is not granted in your name without your knowledge. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without your express written authorization or approval. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. Be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of requests you make for new loans, credit mortgages, employment, housing, or other services. Fees for placing and/or lifting a security freeze on a credit report vary by state and by agency, and may be waived under certain circumstances, such as if you have been the victim of identity theft.

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

Equifax Security Freeze PO Box 105788 Atlanta, GA 30374 www.equifax.com	Experian Security Freeze PO Box 9554 Allen, TX 75013 www.experian.com	TransUnion Fraud Victim Assistance Department PO Box 2000 Chester, PA 19016 www.transunion.com

In order to request a security freeze, you may need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security number;
- Date of birth;
- If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.);
- If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The agencies also must send written confirmation to you within five (5) 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.

A security freeze does not apply to circumstances in which you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of account review, collection, fraud control, or similar activities.

To lift the security freeze in order 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 proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you would like for the credit report to be available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

If you are actively seeking credit, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, a few days before actually applying for new credit.

To remove the security freeze, 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 (3) business days after receiving your request to remove the security freeze.

Tax-related Identity Theft

We also recommend that you review the IRS website's resources regarding tax-related identity theft at https://www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft.

For 2016, the IRS, state governments, and the tax industry joined together to enact new safeguards and take additional actions to combat tax-related identity theft. Many of these safeguards may be invisible to taxpayers, but invaluable in the fight against criminal syndicates. If you prepare your own tax return using software, you will encounter new log-on standards. Some states also have taken additional steps to help prevent fraud.

What is tax-related identity theft?

Tax-related identity theft occurs when someone uses a stolen Social Security number (SSN) to file a tax return and claim a refund that does not belong to them. You may be unaware that this has happened until you attempt to 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 that they have identified a suspicious return using your SSN and require further verification to process the return.

Know the warning signs

Be alert to the signs of tax-related identity theft. For example, you may be contacted by the IRS or your tax professional/provider indicating that:

- More than one tax return was filed using your SSN;
- You owe additional tax, 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 income from an employer for whom you did not work.

Steps to take if you become a victim

In addition to the steps outline above, 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-filed return is rejected because of a duplicate filing under your SSN, or if you are instructed to do so. IRS Form 14039 (Identity Theft Affidavit) is available here: https://www.irs.gov/pub/irs-pdf/f14039.pdf. You may use the fillable form that can be found on the IRS.gov website at the link above, then print and attach the completed form to your tax return and mail it to the IRS.

- Note: you should submit a Form 14039 **only** if your Social Security number has been compromised ***and*** your e-file return was rejected as a duplicate, or if the IRS has informed you that you may be a victim of tax-related identity theft.

- 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 your situation was not resolved, you may contact the IRS for specialized assistance at (800) 908-4490.