

Melissa K. Ventrone
T (312) 360-2506
F (312) 517-7572
Email: mventrone@ClarkHill.com

Clark Hill
130 E. Randolph Street, Suite 3900
Chicago, Illinois 60601
T (312) 985-5900
F (312) 985-5999

July 6, 2022

Via Portal

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

To Whom It May Concern:

We represent Petersen International Underwriters (“PIU”) with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. PIU provides insurance solutions for disability, life, medical, and contingency risks. PIU is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

On December 20, 2021, PIU discovered a security incident impacting their ability to access their systems. As soon as PIU learned of the incident, they took the impacted systems offline and took steps to secure the network. PIU also engaged independent computer forensic experts to assist with the investigation. The investigation determined that an unauthorized actor gained access to a limited number of documents stored on their systems. PIU conducted a review of this data and determined that the personal information of some of their client(s) and employees may have been included in these documents. The sensitive information stored on the system at the time of the incident includes names, and some combination of the following data elements: addresses, Social Security numbers, financial account information, and health insurance policy number or certificate.

2. Number of residents affected.

Ten (10) Maine residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on July 6, 2022 (a copy of the form notification letter is enclosed as Exhibit A).

July 6, 2022

Page 2

3. Steps taken in response to the incident.

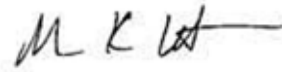
PIU took steps to address this incident and to prevent similar incidents in the future, including deploying endpoint threat detection and response software, changing all user and system passwords, and implementing additional security controls. Affected individuals were offered 12 months of credit monitoring and identity protection services through IDX.

4. Contact information.

PIU takes the security of their client and employee's information very seriously and is committed to ensuring information within its control is protected. If you have any questions or need additional information, please do not hesitate to contact me at mventrone@clarkhill.com or (312) 360-2506.

Sincerely,

CLARK HILL



Melissa K. Ventrone
Member

MKV
Enclosure

cc: Mariah Leffingwell



Petersen International Underwriters
P.O Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<Enrollment Code>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zipcode>>

July 6, 2022

Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>,

Petersen International Underwriters (“PIU”) recently experienced a data security incident that may have impacted your personal information. PIU provides insurance solutions for disability, life and medical and contingency risks and may have your information if you are or have been a Producer for PIU. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information, and resources we are making available to help you.

What Happened?

On December 20, 2021, we discovered a security incident impacting our ability to access our systems. As soon as we learned of the incident, we took the impacted systems offline and took steps to secure our network. We also engaged independent computer forensic experts to assist with our investigation. The investigation determined that an unauthorized actor gained access to a limited number of documents stored on our system. We conducted a review of these documents, and on April 7, 2022, determined that your personal information may have been included. We have no indication that any information has been misused but wanted to let you know about this incident out of an abundance of caution.

What Information Was Involved?

Information stored in our systems at the time of the incident may include your name, Social Security number, and for some individuals, their financial account number.

While we do not have any evidence that any personal information has been misused, in addition, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: <<12 months/ 24 months>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do

You should remain vigilant against incidents of identity theft by reviewing bank accounts and other financial statements as well as any credit reports for suspicious activity. You can also visit [identitytheft.gov](https://www.identitytheft.gov) for recommendations by the Federal Trade Commission regarding identity theft protection.

We encourage you to contact IDX with any questions and to enroll in the free identity protection services by calling 1-833-423-0592 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 9 am - 9 pm Eastern Time. Please note the deadline to enroll is October 6, 2022.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering. IDX representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information

For questions and enrollment assistance, please call 1-833-423-0592 Monday through Friday between 9 am – 9 pm Eastern Time. Your trust is a top priority for us, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in black ink that reads "Thomas R. Petersen". The signature is written in a cursive style with a prominent initial "T" and a stylized "P".

Thomas R. Petersen
Petersen International Underwriters

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your IDX identity protection membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, IDX will be able to assist you.

3. Telephone. Contact IDX at 1-833-423-0592 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in IDX credit monitoring, notify them immediately by calling 1-833-423-0592 from 9:00 am to 9:00 pm Eastern, Monday through Friday.

A representative will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be able to work with a representative who will assist you with resolving any fraudulent activity.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.ca.gov/privacy) for additional information on protection against identity theft.

District of Columbia: Office of the Attorney General, 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 1-877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 1-401-274-4400. You have the right to obtain any police report filed in regard to this incident. There were 8 Rhode Island residents impacted by this incident.

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.