

Buchanan Ingersoll & Rooney PC

Sue Friedberg
412 562 8436
sue.friedberg@bipc.com

Jason McLean
412 562 1474
Jason.mclean@bipc.com

Union Trust Building
501 Grant Street, Suite 200
Pittsburgh, PA 15219-4413
T 412 562 8800
F 412 562 1041

January 14, 2022

The Attorney General Brian Frosh
Office of the Attorney General
200 St. Paul Place
Baltimore, MD 21202

Attn: Security Breach Incident

Dear Attorney General Frosh:

We are submitting this notification on behalf of Title Guaranty Company of Lewis County and Coast Title & Escrow, Inc. ("Title Companies") in accordance with Md. Code Ann., Com. Law § 14-3504(h). The Title Companies recently experienced unauthorized access to their computer systems. Based on investigation, the Title Companies believe the personal data of one Maryland resident was involved.

On October 28, 2021, the Title Companies were the victims of a ransomware attack that originated when an IT service provider used by the Title Companies was compromised by unauthorized access to its computer system. The Title Companies immediately shut down their computer systems and internet connections for a few days while confirming that all malware had been eradicated. The Title Companies also engaged nationally-recognized experts in cybersecurity and forensic investigations to enhance efforts in responding to the incident, to assist in investigating the scope and impact of the incident, and to monitor the activity in the Title Companies' system. On or around November 23, 2021, employees at the Title Companies noticed issues with their company email accounts. The forensic investigation disclosed that the mailboxes of three employees at Title Guaranty Company had been hacked.

Each component of the Title Companies' systems has been examined carefully before being returned to operation. All potentially impacted equipment has been either removed or remediated and data files have been restored from backup as needed. The Title Companies have installed monitoring devices to detect any suspicious activity. All affected email boxes have been isolated,

January 14, 2022

Page - 2 -

remediated, and secured before bringing them back into operation. The Title Companies are considering other ways to enhance their security.

The investigation revealed that personal information related to some customers of the Title Companies was accessed and possibly obtained. The personal information involved included first and last names and some combination of social security numbers, dates of birth, financial account information, and driver's license numbers.

The Title Companies will be providing notice to all affected individuals. Attached you will find a copy of the notice letter that will be sent to the affected individuals. If you have any questions or would like additional information, please contact me.

Sincerely,



Sue Friedberg



Jason McLean



COAST TITLE & ESCROW
522 W WISHKAH ST
P.O. BOX 287
ABERDEEN, WA 98520

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Security Breach

Dear Valued Customer,

Title Guaranty Company of Lewis County and Coast Title & Escrow are writing to let you know that our companies recently experienced a data breach. We are concerned that some of your personal information was involved. Even though we have no indication that your information has or will be misused, we want to provide ways to help you avoid the possibility of identity theft.

We have arranged for you to sign up for credit monitoring and identity theft protection for one year at no cost to you. The sign up process is explained below. This letter also has information about what happened and other steps to consider to help protect your information.

Who Are We? We provide title insurance and escrow services in Lewis County and Grays Harbor County. You likely provided some personal information to us when you purchased or sold a home.

What Happened? In late October 2021, we were the victims of a ransomware attack that probably originated with one of the threat actors that's been in the news. We immediately shut down our computer systems and internet connections for a few days to be sure the attacker was removed. There was also suspicious activity in the e-mail accounts of several employees. We retained a nationally recognized cybersecurity forensic firm to conduct a thorough investigation.

What Information Was Involved? The investigation revealed that some data records were likely accessed and obtained by the attackers. These records held some of your personal information, including your name and Social Security number. The records also may have contained your date of birth, some bank account information, and/or driver's license number. At this time, we are not aware of any actual or attempted misuse of your personal information.

What We Are Doing. Each component of our systems was examined carefully before being returned to operation. All potentially impacted equipment was either removed or thoroughly cleaned, and our data files were restored from backup. The cybersecurity firm installed more threat monitoring equipment and is helping us strengthen our defenses against future attacks. We also notified law enforcement. We will continue to evaluate other measures to protect the security of our network, systems, and personal information records.

What You Can Do. We are offering you one year of credit monitoring and identity theft protection through Experian at no cost. We encourage you to sign up for these services by going to <https://www.experianidworks.com/3bcredit> and using the personal ID number contained here: <<b2b_text_1(personal ID number)>>. Be prepared to provide engagement number <<b2b_text_2(engagement number)>> as proof of eligibility. To take advantage of these services, you must sign up before enrollment ends on <<b2b_text_6(activation deadline)>>.

Experts recommend being on alert for identity theft and fraud. You can do this by signing up for the credit monitoring and identity protection services, checking your account statements and credit reports regularly for suspicious activity, and considering putting a "freeze" on your accounts. Some additional precautions and resources are described below under "Additional Steps to Help Protect Your Information."

For More Information. If you have questions, please call our dedicated call center at 1-877-288-8057, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time (excluding some U.S. holidays).

We deeply regret the concern or inconvenience this data security incident may cause you.

Sincerely,

Title Guaranty Company of Lewis County
Coast Title & Escrow

IDENTITY RESTORATION SERVICES—NO ENROLLMENT NEEDED

Identity Restoration assistance is immediately available to you through Experian. You do not need to enroll. If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. Be prepared to provide **engagement number** <<b2b_text_2(engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that the Identity Restoration service is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

ENROLL IN EXPERIAN IDENTITYWORKS

How to Enroll

We encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary one year membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** <<b2b_text_6(activation deadline)>> (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://experianidworks.com/3bcredit>
- Provide your **activation code**: <<activation code s_n>>
- Provide your **engagement number**: <<b2b_text_2(engagement number)>>

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 1-877-288-8057 by March 29, 2022. Be prepared to provide engagement number <<b2b_text_2(engagement number)>> as proof of eligibility for the Identity Restoration services by Experian.

Additional Details Regarding Your One Year Experian Identityworks Membership

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Additional Steps to Help Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant and review 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 should also 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 ("FTC").

Copy of 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 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 also contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-877-322-8228
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for one year. 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 www.annualcreditreport.com.

Security Freeze: You have the right to place a security freeze on your credit file. This will prevent new credit from being opened in your name without your express authorization. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, 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. There is no fee 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.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the Federal Trade Commission or from your state Attorney General about steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to your state Attorney General.

Federal Trade Commission (FTC): The FTC can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and, TTY: 1-866-653-4261. The Federal Trade Commission encourages those who discover that their information has been misused to file a complaint with them as explained on their website. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General.

Fair Credit Reporting Act (FCRA): 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 violators. 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. We encourage you to 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.

For California residents: You may visit the California Office of Privacy Protection at www.oag.ca.gov/privacy for additional information on protection against identity theft.

For Kentucky residents: You can contact the State Attorney General at the Office of the Attorney general of Kentucky, 700 Capitol Avenue, Suite 188, Frankfort, Kentucky 40601; 502-696-5300; or at www.ag.ky.gov.

For Maryland residents: You can contact the State Attorney General at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; toll-free at 1-888-743-0023; by phone at (410) 576-6300; consumer hotline (410) 528-8662; and online at www.marylandattorneygeneral.gov.

For 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 violators. 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. We encourage you to 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.

For North Carolina residents: You can contact the State Attorney General at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For Oregon residents: You can contact the State Attorney General at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096; 877-877-9392; and online at <https://www.doj.state.or.us/>.