



June 18, 2021

<First Name> <Last Name>
<Street>
<City>, <State> <Zip>

Re: Notice of Data Breach

Dear <First Name> <Last Name>

At Vista Title and Escrow, we value transparency and respect the privacy of your information, which is why, as a precautionary measure, we are writing to let you know about a data security incident that may involve your personal information. As such, we are providing you with background about the incident, what we did in response, and steps you can take to protect yourself against possible misuse of your personal information.

What Happened

On April 30, 2021, we began suspecting an unauthorized individual gained access to one of our email accounts. Upon discovery, we immediately engaged third-party forensic experts who promptly secured and removed the unauthorized access to the account and began a thorough investigation to determine the nature and scope of the incident. The initial investigation revealed that the unauthorized individual gained access to the email account on April 21, 2021, and remained hidden until April 30, 2021. The investigation and analysis of the information potentially involved are ongoing, but on May 26, 2021, we discovered that the impacted email account contained some of your information. As of now, we have no evidence indicating misuse of your information. However, out of an abundance of caution, we wanted to ensure you knew of this incident.

What Information Was Involved

The information that could have been involved included your <PII>

What We Are Doing

The security and privacy of the information contained within our systems is a top priority for us. As stated above, while we have no evidence indicating your information was misused, we strongly recommend you remain vigilant, monitor and review all of your financial and account

statements, and report any unusual activity to the institution that issued the record and law enforcement. Please see “other important information” on the following pages for guidance on how to best protect your identity.

Additionally, in response to this attack, we implemented additional safeguards and employee training related to cybersecurity. Further, we are working with our external legal and cybersecurity experts to improve our cybersecurity policies, procedures, and protocols to attempt to minimize the likelihood of this type of attack succeeding again.

Finally, we are providing you with access to Triple Bureau Credit Monitoring/Triple Bureau Credit Report/Triple Bureau Credit Score/Cyber Monitoring* services at no charge. These services provide you with alerts for twelve months from the date of enrollment when changes occur to any of one of your Experian, Equifax or TransUnion credit files. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal data on the dark web and alert you if your personally identifiable information is found online.

To enroll in Credit Monitoring* services at no charge, please log on to <URL> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter.

For More Information

We sincerely regret this incident, and we understand that you may have questions about it beyond what is covered in this letter. If you have any additional questions, please call me at 509-328-7171.

Sincerely yours,

[REDACTED]

Anthony Carollo
CEO

OTHER IMPORTANT INFORMATION

Obtain and Monitor Your Credit Report

We recommend that you obtain a free copy of your credit report from each of the three nationwide 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 access the request form at <https://www.annualcreditreport.com/requestReport/requestForm.action>.

Alternatively, you can elect to purchase a copy of your credit report by contacting one of the three national credit reporting agencies. Provided below are the three nationwide credit reporting agencies' contact information to request a copy of your credit report or general identified above inquiries.

Equifax
(866) 349-5191
www.equifax.com
P.O. Box 740241
Atlanta, GA 30374

Experian
(888) 397-3742
www.experian.com
P.O. Box 4500
Allen, TX 75013

TransUnion
(800) 888-4213
www.transunion.com
2 Baldwin Place
P.O. Box 1000
Chester, PA 19016

Remain Vigilant, Review Your Financial Account Statements and Notify Law Enforcement of Suspicious Activity

As a precautionary measure, we recommend that you remain vigilant by closely reviewing your financial account statements and credit reports. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company that maintains the account. You also should immediately report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, including your state attorney general and the Federal Trade Commission (FTC). Complaints filed with the FTC will be added to the FTC's Identity Theft Data Clearinghouse, a database made available to law enforcement.

To file a complaint or to contact the FTC, you can (1) send a letter to the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580; (2) go to IdentityTheft.gov/databreach; or (3) call 1-877-ID-THEFT (877-438-4338).

Consider Placing a Fraud Alert on Your Credit Report

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 at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you before establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three nationwide credit reporting

agencies identified above. Additional information is available at <https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/>

Security Freeze (also known as a Credit Freeze)

You may have the right to put a credit or security freeze on your credit file. A security freeze makes it harder for someone to open a new account in your name. It 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 apply for a new credit card, wireless phone, or any service that requires a credit check.

You must separately place a security freeze on your credit file with each credit reporting agency. 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. There is no charge to request a security freeze or to remove a security freeze. Since the instructions for how to establish a security freeze differ based on your state residency, to find out more information, please contact the three nationwide credit reporting agencies (contact information provided above in the **“Obtain and Monitor Your Credit Report”** section).

Take Advantage of Additional Free Resources on Identity Theft

We recommend that you review the tips provided by the Federal Trade Commission’s Consumer Information website, a valuable resource with some helpful tips on how to protect your information. Additional information is available at <https://www.consumer.ftc.gov/topics/privacy-identity-online-security>

For more information, please visit IdentityTheft.gov or call 1-877-ID-THEFT (877-438-4338). A copy of Identity Theft – A Recovery Plan, a comprehensive guide from the FTC to help you guard against and deal with identity theft, can be found on the FTC’s website at https://www.consumer.ftc.gov/articles/pdf-0009_identitytheft_a_recovery_plan.pdf