

Kevin M. Scott
Tel 312.456.1040
Fax 312.456.8435
kevin.scott@gtlaw.com

October 13, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Identity Theft Unit
200 St. Paul Place
Baltimore, MD 21202

Dear Attorney General Frosh:

We represent Vellum Mortgage, Inc. (“Vellum”) located at 12700 Fair Lakes Circle, Suite 400, Fairfax, VA 22033, and are writing to notify your office of an incident that may affect the security of some personal information relating to 491 Maryland residents.

Vellum was the target of a ransomware attack on its computer systems. Vellum moved quickly to contain the incident and conducted a thorough investigation with the assistance of security experts. On August 15, 2022, Vellum discovered that client personal information may have been accessed. Vellum believes it is likely the attacker only wanted money and not the information on its computers but, in an abundance of caution, is notifying its clients that their information may have been accessed by the attackers. The information at risk contained clients’ names, addresses, Social Security numbers, driver’s license numbers and/or other government identification, financial account information and/or the results of a credit check.

Vellum takes the security of its clients’ information seriously and is taking measures to reduce the likelihood of a future cyberattack, including enhanced network security measures and increasing its defenses against these rampant attacks. Vellum is also offering all potentially affected individuals 24 months of complimentary credit monitoring and identity theft restoration from IDX.

On or about October 12, 2022, Vellum began mailing notifications to all potentially affected individuals. An example of the notification is attached. Notification has also been made to the three major credit reporting agencies.

Attorney General Brian Frosh

October 13, 2022

Page 2

Should you have any questions regarding this notification or other aspects of the data security event, please contact me for any additional information.

Best Regards,

A handwritten signature in blue ink, appearing to read "Kevin M. Scott", with a long horizontal flourish extending to the right.

Kevin M. Scott
Shareholder

Vellum Mortgage
Return Mail to IDX
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223



To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: [XXXXXXXXXX]

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

October 12, 2022

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

We are writing to inform you of a data security incident that may have impacted some of your personal information. We take the security of your information very seriously, and we sincerely apologize for any concern this incident may cause. This letter contains information about what happened, actions we have taken to prevent a reoccurrence, and steps you can take to protect your information.

What Happened?

Recently, we were the target of a ransomware attack on our computer systems. Ransomware is a computer virus that encrypts computer systems until and unless we pay money (i.e., the ransom) demanded by the attackers. These rampant attacks continue to challenge everyone. We moved quickly to contain the incident and conducted a thorough investigation with the assistance of security experts. On August 15, 2022, our recently concluded investigation identified that your personal information may have been accessible. We believe it is likely the attacker only wanted money and not the information on our computers but, in an abundance of caution, we are letting you know that your information may have been accessed by the attackers.

What information was involved?

Our investigation determined that the incident may have impacted one or more of the following types of information related to you, *if you provided that information to Vellum Mortgage*: your name, address, Social Security number, driver's license or other government identification, financial account information, or the results of a credit check. If you would like more information about which specific pieces of information were associated with you, you can request that information by calling the number below.

What We Are Doing

We take the security of your information seriously and are taking measures to reduce the likelihood of a future cyberattack, including enhanced network security measures and increasing our defenses against these rampant attacks. In addition, out of an abundance of caution, we are offering identity theft protection services through IDX, the data breach and recovery services expert. IDX identity protection services include: 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. Please note deadline to enroll is January 12, 2023.

Additional information describing your services is included with this letter.

What You Can Do

Please review the enclosed “Additional Important Information” section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission (FTC) regarding identity theft protection and details on how to place a fraud alert or security freeze on your credit file. As an added precaution, you may want to closely monitor your personal accounts for any suspicious activity.

For More Information

We have established a dedicated call center to answer questions or concerns you may have about this incident. You can reach the call center at 1-800-939-4170, Monday through Friday from 9:00 am – 9:00 pm Eastern Time, excluding major U.S. national holidays.

Protecting your information is of the utmost importance to us. We appreciate your patience and understanding, and we sincerely apologize for any inconvenience or concern this incident may cause you.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jay Curley', with a stylized, cursive script.

Jay Curley

Principal



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 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

Important Additional Information

For residents of Iowa: You are advised to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon: You are advised to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of New Mexico: You are advised to review personal account statements and credit reports, as applicable, to detect errors resulting from the security incident. You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf or see the contact information for the Federal Trade Commission listed below.

For residents of District of Columbia, Maryland, New York, North Carolina, and Rhode Island:

You can obtain information from the District of Columbia, Maryland, North Carolina, New York, and Rhode Island Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

DC Attorney General	Maryland Office of Attorney General	New York Attorney General	North Carolina Attorney General	Rhode Island Office of Attorney General
441 4th St NW Washington, DC 20001 1-202-727-3400 www.oag.dc.gov	200 St. Paul Pl Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us	120 Broadway, 3rd Fl New York, NY 10271 1-800-771-7755 www.ag.ny.gov	9001 Mail Service Ctr Raleigh, NC 27699 1-877-566-7226 www.ncdoj.com	150 South Main St Providence RI 02903 1-401-274-4400 www.riag.ri.gov

Federal Trade Commission, Consumer Response Center
600 Pennsylvania Ave, NW Washington, DC 20580
1-877-IDTHEFT (438-4338) www.identitytheft.gov

Massachusetts and Rhode Island residents: You have the right to obtain a police report if you are a victim of identity theft.

For residents of all states:

You may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your free credit report, please visit www.annualcreditreport.com, or call toll-free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available at www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf), Experian (www.experian.com/fraud/center.html) or Transunion (www.transunion.com/fraud-victim-resource/place-fraud-alert). 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. Initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant for incidents of fraud and identity theft by reviewing payment card account statements and monitoring your credit reports for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency by visiting their websites below or by mail. In order to place the security freeze for yourself, your spouse, or a minor under the age of 16, you will need to provide your name, address for the past two years, date of birth, Social Security number, proof of identity and proof of address as requested by the credit reporting company. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password, which will be required to lift the freeze, which you can do either temporarily or permanently. It is free to place, lift, or remove a security freeze.

Equifax Security Freeze

P.O. Box 105788
Atlanta, GA 30348-5788
www.experian.com/freeze/center.html
1-800-525-6285

Experian Security Freeze

P.O. Box 9554
Allen, TX 75013-9544
www.experian.com/freeze/center.html
1-888-397-3742

TransUnion Security Freeze

P.O. Box 2000
Chester, PA 19016-2000
www.transunion.com/credit-freeze
1-800-680-7289