



MULLEN  
COUGHLIN<sup>LLC</sup>  
ATTORNEYS AT LAW

Kevin M. Mekler  
Office: (267) 930-2190  
Fax: (267) 930-4771  
Email: [Kmekler@mullen.law](mailto:Kmekler@mullen.law)

3001 N Rocky Point Dr East  
Suite 200  
Tampa, FL 33607

January 13, 2022

**VIA E-MAIL**

Office of the Attorney General  
Security Breach Notification  
200 St. Paul Place, 25th Floor  
Baltimore, MD 21202  
E-mail: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

**Re: Notice of Data Event**

Dear Sir or Madam:

We represent Elevated Title, LLC (“Elevated”), located at 1701 Barrett Lakes Blvd, Suite 260, Kennesaw, GA 30144. This notice is made by Elevated on behalf of Alcova Mortgage. This notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, neither Elevated nor Alcova Mortgage waives any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

**Nature of the Data Event**

Elevated provides titling services to certain lenders regarding the purchase of commercial and residential real estate. Elevated became aware of unusual activity involving a single company email account. In response, Elevated immediately began an investigation and the investigation determined that an unknown individual(s) accessed certain Elevated email accounts at various times from July 21, 2020 until December 19, 2020. Because the forensic investigation could not conclusively rule out unauthorized access to information in the account, Elevated immediately began a thorough review of the full contents of the email accounts to determine whether sensitive information was present at the time of the incident. Elevated completed this review on or about August 27, 2021, and determined that personal information for approximately five (5) Maryland residents associated with Alcova Mortgage was present in the account at the time of the incident. The incident was isolated to Elevated’s system. It was not caused by or related to any action on the part of Alcova, nor did it affect Alcova’s system. But Elevated did initially acquire the personal information subject to the incident through its work with Alcova.

The following types of information may have been impacted by this event: name, email address, phone number, mailing address, Social Security number, financial account information, payment card information, driver’s license and/or state identification number, passport number, military identification number,

medical information, health insurance information, dates of birth, and/or digital signature. To date, Elevated has not identified any actual or attempted misuse of the information.

Elevated notified Alcovia Mortgage, on November 17, 2021, upon making this determination and worked with Alcovia Mortgage in furtherance of providing individuals with notice of this incident. Elevated is providing this notice to the Maryland Attorney General, on behalf of Alcovia Mortgage, because this incident involved Elevated email accounts.

### **Notice to Maryland Residents**

On or about January 7, 2022, Elevated began providing written notice of this incident to potentially affected individuals. Written notice is being provided in substantially the same form as the letters attached hereto as *Exhibit A*.

### **Other Steps Taken and To Be Taken**

Upon discovering the event, Elevated moved quickly to investigate and respond to the incident, assess the security of Elevated's email system, and determine the scope of the incident. As part of Elevated's ongoing commitment to the security of information, Elevated is reviewing and enhancing existing policies and procedures and conducting additional workforce training to reduce the likelihood of a similar future event. Elevated is providing access to credit monitoring services for 1 year through IDX, to Maryland residents.

Additionally, Elevated is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

### **Contact Information**

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-2190.

Very truly yours,

Kevin M. Mekler of  
MULLEN COUGHLIN LLC

KMK/jc1

# EXHIBIT A



10300 SW Greenburg Rd.  
Suite 570  
Portland, OR 97223

To Enroll, Please Call:

1-833-909-3931

Or Visit:

<https://response.idx.us/elevated-title>

Enrollment Code: <<XXXXXXXX>>

<<First Name>> <<Middle Name>> <<Last Name>>

<<Address Line 1>>

<<Address Line 2>>

<<City>>, <<State>> <<Zip Code>>

January 3, 2022

## NOTICE OF DATA BREACH

Dear <<First Name>> <<Middle Name>> <<Last Name>>:

Elevated Title, LLC (“Elevated”) provides titling services to certain lenders regarding the purchase of commercial and residential real estate. We provided titling services to Alcova Mortgage (“Alcova”) as part of your recent mortgage transaction with that lender. Elevated is writing on behalf of Alcova to notify you of an incident that occurred within Elevated’s system that may affect the privacy of some of your information. This letter provides details of the incident, our response, and resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so. The incident was isolated to Elevated’s system. It was not caused by, nor did it affect, Alcova’s system.

**What Happened?** On or around November 18, 2020, Elevated became aware of unusual activity relating to a company email account. In response, we immediately began an investigation and the investigation determined that an unknown individual(s) accessed certain Elevated email accounts at various times from July 21, 2021 until December 19, 2020. An additional review was undertaken to identify the types of information that were present in the email accounts. While this investigation remains ongoing, on or around February 19, 2021, we determined that information related to individuals associated with some of our business partners was present in the accounts. We notified these business partners and then began notifying potentially affected individuals.

**What Information Was Involved?** Our investigation determined that the following types of information related to you were present in at least one email account at the time of the incident: your name and names, email addresses, phone numbers, address, social security, financial account information, payment card information, driver’s license and/or state identification numbers, passport number, military identification number, medical information, health insurance information, dates of birth, and/or digital signatures. To date, we are unaware of any actual or attempted misuse of your personal information as a result of this incident.

**What Are We Doing?** Upon learning of this incident, we moved quickly to investigate and respond to this incident. We assessed the security of our email tenant and continue to review and enhance existing policies and procedures to reduce the likelihood of a future similar event. As an added precaution, we are offering you complimentary access to identity theft protection services through IDX for twelve to twenty four months.

**What You Can Do.** We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity for the next twelve (12) to twenty-four (24) months. You may also review the information in the attached *Steps You Can Take to Help Protect Your Information*, which also includes information regarding the enrollment in the complimentary credit monitoring we are offering. While the credit monitoring is complimentary, you will need to enroll in this service yourself.

***For More Information.*** We recognize that you may have additional questions not addressed in this letter. To ensure your questions are answered in a timely manner, we established a dedicated assistance line at 1-833-909-3931 which can be reached Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. You may also write to us at Elevated Title, LLC, 1701 Barrett Lakes Blvd, Suite 260, Kennesaw, GA 30144.

Sincerely,

Elevated Title, LLC

## STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

### Enroll in IDX Protection Services

**1. Website and Enrollment.** Go to <https://response.idx.us/elevated-title> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter. Please note the enrollment deadline is April 3, 2022.

**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 1-833-909-3931 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

### Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a security freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

| <b>Equifax</b>                                                                                                                  | <b>Experian</b>                                                             | <b>TransUnion</b>                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <a href="https://www.equifax.com/personal/credit-report-services/">https://www.equifax.com/personal/credit-report-services/</a> | <a href="https://www.experian.com/help/">https://www.experian.com/help/</a> | <a href="https://www.transunion.com/credit-help">https://www.transunion.com/credit-help</a> |
| 1-888-298-0045                                                                                                                  | 1-888-397-3742                                                              | 1-833-395-6938                                                                              |
| Equifax Fraud Alert, P.O. Box 105069<br>Atlanta, GA 30348-5069                                                                  | Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013                        | TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016                                    |
| Equifax Credit Freeze, P.O. Box 105788<br>Atlanta, GA 30348-5788                                                                | Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013                      | TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094                                   |

## **Additional Information**

If you had a username and password involved in this incident, we recommend that you change the password and any security question or answer for that account immediately. If you reuse usernames and passwords for other online accounts, it is recommended that you change the password and any security question or answer for those online accounts, as well. Further, as a general precaution, you should never use the same password for more than one online account. When creating passwords, they should be complex and not contain personal information.

You can further educate yourself regarding data security best practices, identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; [www.identitytheft.gov](http://www.identitytheft.gov); 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. 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. This notice has not been delayed by law enforcement.

***For District of Columbia residents***, the District of Columbia Attorney General can be reached at: 441 4th Street NW #1100 Washington, D.C. 20001; 1-202-727-3400; email at [oag@dc.gov](mailto:oag@dc.gov).

***For Maryland residents***, the Attorney General can be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023 or 1-410-528-8662; [www.oag.state.md.us](http://www.oag.state.md.us).

***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 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. 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](http://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 Avenue NW, Washington, D.C. 20580.

***For 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; and <https://ag.ny.gov/>.

***For North Carolina residents***, the Attorney General can be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; [www.ncdoj.gov](http://www.ncdoj.gov).

***For Rhode Island residents***, the Rhode Island Attorney General can be reached at: 150 South Main Street, Providence Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.