



**Baker&Hostetler LLP**

999 Third Avenue  
Suite 3900  
Seattle, WA 98104-4076

T 206.332.1380  
F 206.624.7317  
www.bakerlaw.com

Andreas T. Kaltsounis  
direct dial: 206.566.7080  
akaltsounis@bakerlaw.com

February 11, 2022

**VIA EMAIL (IDTHEFT@OAG.STATE.MD.US)**

Brian E. Frosh  
Attorney General  
Office of the Attorney General  
Attn: Security Breach Notification  
200 St. Paul Place  
Baltimore, MD 21202

*Re: Incident Notification*

Dear Attorney General Frosh:

We are writing on behalf of our client, PrimeLending, A PlainsCapital Company (“PrimeLending”), to notify you of a security incident involving Maryland residents.

PrimeLending recently completed an investigation that involved unauthorized access to one PrimeLending employee’s email account. Upon learning of the unauthorized access, PrimeLending immediately took steps to secure its email environment and began an investigation. The investigation determined that an unauthorized person accessed the employee’s email account on November 4, 2021. The investigation was unable to determine all specific items the unauthorized person may have viewed in the email account. Therefore, out of an abundance of caution, PrimeLending completed a review process and, on December 22, 2021, learned that an email or attachment in the account contained the personal information of seven Maryland residents including their name and one or more of: Social Security number, financial account number and payment card number.

Beginning today, February 11, 2022, PrimeLending is providing written notice to the Maryland residents by mailing letters via United States Postal Service First-Class mail. A sample copy of the notification letter is enclosed. PrimeLending is offering a complimentary, one-year membership of identity monitoring services provided by Kroll to affected residents. PrimeLending has recommended that residents review their financial account statements and credit reports and

February 11, 2022

Page 2

report any unauthorized charges or activity. In addition, PrimeLending established a dedicated helpline where the individuals may obtain more information regarding the incident.

To help prevent something like this from happening in the future, we have implemented additional measures to enhance our existing security protocols and are continuing to provide cybersecurity training to our staff.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,



Andreas T. Kaltsounis

Partner

Enclosure



18111 Preston Road, Suite 900  
Dallas TX 75252

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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<b2b\_text\_2(Company/Trust name)>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country>>

Dear <<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>:

PrimeLending, A PlainsCapital Company, is committed to protecting customer information in its care. With regret, we are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, the measures we have taken, and some additional steps you may consider taking in response.

We recently completed an investigation that involved unauthorized access to one PrimeLending employee's email account. Upon learning of the unauthorized access, we immediately took steps to secure our email environment and began an investigation. The investigation determined that an unauthorized person accessed the employee's email account on November 4, 2021. The investigation was unable to determine all specific items the unauthorized person may have viewed in the email account. Therefore, out of an abundance of caution, we completed a review process and, on December 22, 2021, learned that an email or attachment in the account contained some of your information, including your <<b2b\_text\_1(name, data elements)>>.

We assure you that we take this incident very seriously. We also would like to remind you that it is always advisable to remain vigilant for signs of unauthorized activity by reviewing your account statements and credit reports. If you see charges or activity you did not authorize, we suggest that you contact your financial institution immediately.

As an added precaution, we are offering you a complimentary one-year membership to Kroll's identity monitoring services. These services are completely free to you and activating will not hurt your credit score. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services.

You have until <<b2b\_text\_6(activation deadline)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s\_n>>

For more information about Kroll and your Identity Monitoring services, you can visit [info.krollmonitoring.com](http://info.krollmonitoring.com).

If you prefer to activate these services offline and receive monitoring alerts via the US Postal Service, you may activate via our automated phone system by calling 1-888-653-0511, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number located in your letter ready when calling. Please note that to activate monitoring services, you will be required to provide your name, date of birth, and Social Security number through our automated phone system.

To learn about additional steps you can take in response to the incident, please see the pages that follow this letter.

To help prevent something like this from happening in the future, we have implemented additional measures to enhance our existing security protocols and are continuing to provide cybersecurity training to our staff. Once again, we deeply regret any inconvenience or concern this incident may cause you. If you have any questions, please call (855) 568-2054, Monday through Friday from 8:00 A.M. through 5:30 P.M Central Time, excluding major U.S holidays.

Sincerely,

A handwritten signature in black ink, appearing to be 'Steve Thompson', with a stylized, cursive script.

Steve Thompson  
President and CEO



## TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

### Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

### Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

### Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you will receive an alert.

### Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

### \$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

### Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

### Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.

## ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com), 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police

report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), [www.ftc.gov/idtheft](http://www.ftc.gov/idtheft)

### **Fraud Alerts and Credit or Security Freezes:**

***Fraud Alerts:*** There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

***Credit or Security Freezes:*** You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

*How do I place a freeze on my credit reports?* There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, [www.experian.com](http://www.experian.com)
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, [www.transunion.com](http://www.transunion.com)
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, [www.equifax.com](http://www.equifax.com)

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

*How do I lift a freeze?* A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

PrimeLending's address is 18111 Preston Road, Suite 900, Dallas TX 75252 and its phone number is 800-317-7463.

### **Additional information for residents of the following states:**

**Maryland:** You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, [www.oag.state.md.us](http://www.oag.state.md.us)

**New York:** You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection*, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and *New York State Office of the Attorney General*, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>

**North Carolina:** You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, [www.ncdoj.gov](http://www.ncdoj.gov)