

## Appendix

On December 7, 2020, Clear Mountain Bank (“CMB”) discovered suspicious activity pertaining to the email account of one CMB employee. Upon discovering the incident, CMB immediately took steps to ensure its email tenant was secure. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that there was unauthorized access to one CMB employee’s email account between December 6, 2020 and December 7, 2020. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the account containing personal information. In an abundance of caution, CMB reviewed emails and attachments in the account to identify individuals whose information may have been accessible to the unauthorized person. On February 3, 2021, the investigation first revealed that an email or attachment contained personal information. The investigation continued in subsequent time to identify the full scope of individuals whose information was involved in the incident. CMB concluded its investigation on March 5, 2021. CMB determined that an email or attachment contained the personal information of one Maine resident, including the resident’s name and Social Security number.

Beginning today, May 4, 2021, CMB is providing written notice to the Maine resident by mailing a letter via United States Postal Service First-Class mail.<sup>1</sup> A sample copy of the notification letter is enclosed. CMB is offering a complimentary, one-year membership of identity monitoring services provided by Kroll to the Maine resident. CMB also reported the incident to law enforcement and established a dedicated helpline where the individuals may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, CMB reset the password to the employee’s account, disabled Outlook Web Access, and increased monitoring of network activity.

---

<sup>1</sup> This report does not waive CMB’s objection that Maine lacks personal jurisdiction over it related to any claims that may arise from this incident.



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

<<first\_name>> <<middle\_name>> <<last\_name>> <<suffix>>  
<<address\_1>>  
<<address\_2>>  
<<city>>, <<state\_province>> <<postal\_code>>  
<<country >>

Dear <<first\_name>>,

Clear Mountain Bank is committed to protecting personal information. Regrettably, 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 in response, and some additional steps you may consider taking.

We recently completed an investigation into an incident involving unauthorized access to an email account belonging to one Clear Mountain Bank employee. Upon learning of the incident, we immediately took steps to ensure our email environment was secure. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that an unauthorized party accessed the employee's email account between December 6, 2020 and December 7, 2020. The investigation was unable to determine whether the unauthorized person actually viewed any emails or attachments in the account containing personal information. However, in an abundance of caution, we reviewed the emails and attachments in the account to identify individuals whose information may have been accessible to the unauthorized person. On February 3, 2021, the investigation first revealed that an email or attachment contained personal information. The investigation continued in subsequent time to identify the full scope of individuals whose information was involved in the incident. We concluded our investigation on March 5, 2021, at which time we determined that an email or attachment contained your <<b2b\_text\_1(DataElements)>>.

While we have no indication any individuals have experienced identity theft or financial fraud as a result of this incident, we want to make you aware of this incident and assure you we take it 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 financial account statements and credit reports. If you see charges or activity you did not authorize, we suggest that you contact your provider immediately.

As an added precaution, we have arranged for you to receive a complimentary one-year membership to identity monitoring services through Kroll. Kroll is a global leader in risk mitigation and response, and its team has extensive experience assisting people who have sustained an unintentional exposure of confidential data. 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.idheadquarters.com> to activate and take advantage of your identity monitoring services.

You have until **July 18, 2021** to activate your identity monitoring services.

Membership Number: <<Member ID>>

Additional information describing your services is included with this letter.

PO Box 205 • Bruceton Mills, WV 26525

[www.clearmountainbank.com](http://www.clearmountainbank.com)

We regret that this incident occurred and apologize for any inconvenience. To help prevent something like this from happening in the future, we reset the password to the employee's account, have implemented additional measures to enhance our existing security protocols, and are continuing to educate our staff on how to identify and avoid malicious emails. If you have any questions, please call 1-855-916-6130.

Sincerely,

A handwritten signature in black ink, appearing to read 'D M Thomas', with a long horizontal flourish extending to the right.

David M. Thomas, President and CEO  
Clear Mountain Bank



## 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 will 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.

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

**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).

**West Virginia:** You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

**A Summary of Your Rights Under the Fair Credit Reporting Act:** The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to [www.consumerfinance.gov/learnmore](http://www.consumerfinance.gov/learnmore) or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.