

Appendix

Banner Capital Bank (“Banner”) has completed an investigation of suspicious activity associated with one employee email account. Upon identifying the activity, Banner promptly took steps to secure the account and began its investigation. The investigation determined that an unauthorized person may have accessed the account between August 20, 2025, and September 11, 2025. Banner searched and reviewed messages in the account that the unauthorized person may have accessed for personal information. On February 20, 2026, Banner determined that one or more of those messages or attachments contained the name and financial account number of two (2) Maine residents. This incident did not involve access to any other bank systems, no customer account balances were accessed, and no funds were transferred or attempted to be transferred.

On March 6, 2026, Banner commenced mailing notifications to these Maine residents via U.S. First-Class mail in accordance with Me. Rev. Stat. Tit. 10, §1348. Banner has established a dedicated, toll-free call center for individuals to call with questions. An example notification is enclosed.

To help prevent something like this from happening again, Banner has taken, and will continue to take, steps to enhance the security of its email environment.



<<Return to Kroll>>
<<Return Address>>
<<City, State ZIP>>

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

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

Dear <<first_name>> <<last_name>>,

Banner Capital Bank is writing to make you aware of a data security incident that may have involved some of your information. This letter explains the incident, measures we have taken, and some steps you may consider taking.

We recently completed our investigation of suspicious activity associated with one of our employee’s email accounts. Upon identifying the activity, we promptly took steps to secure the account and began our investigation. The investigation determined that an unauthorized person may have accessed the account between August 20, 2025, and September 11, 2025. We identified messages and attachments in the account that the unauthorized actor may have accessed, which we searched and reviewed for personal information. We determined that one or more of those messages or attachments contained your <<b2b_text_1(DataElements)>>. This incident did not involve access to any other bank systems, no customer account balances were accessed, and no funds were transferred or attempted to be transferred.

To date, we are not aware of any fraud occurring as a result of this incident. Nevertheless, we remind you that it is always a good idea to be vigilant for incidents of fraud or identity theft by reviewing account statements for any unauthorized activity. If you identify any such activity, please immediately contact us. You can also review the enclosed *Additional Steps You Can Take*, which contains information about what you can do to safeguard against possible misuse of your information.

We apologize for any concern or inconvenience. We have taken, and will continue to take, steps to enhance the security of our email environment. If you have any questions about this incident, please call (844) 354-0271, Monday through Friday, 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays.

Sincerely,

Banner Capital Bank

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 12-24 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 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, 1-888-378-4329
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 1000, Chester, PA 19016, 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.identitytheft.gov

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 is because most creditors need to see your credit report before they approve a new account. If they cannot 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:

- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com
- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 160, Woodlyn, PA 19094, www.transunion.com

You will 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.