March 26, 2019

[Insert Recipient Name]
[Insert Recipient Address]

Dear **[Insert]**:

We are contacting you because some of your personal information may have been accessed by unauthorized individuals. However, your deposits remain safe and secure with us.

What Happened?

On January 14, 2019, we detected that unauthorized users had gained access to certain bank employee email mailboxes. We promptly began an investigation and determined that unauthorized users may have had access to certain bank employee email mailboxes from November 23, 2018, through January 14, 2019. Our investigation further revealed that some of your personally identifiable information may have been transmitted internally in one or more of the affected employees' email mailboxes. The employees' email was used to provide banking services, and as a consequence may have had some of your personal information saved in an email.

We cannot confirm the unauthorized users' intentions or purpose, but our investigation has concluded that these unauthorized users may have obtained documentation with your name, and some of your personal information. We cannot trace with certainty the location of the unauthorized users, but it is possible that they are located outside the United States. We are providing you with this notice because we cannot rule out the possibility that unauthorized users may have obtained your information.

Our investigation has not revealed that any customer deposits have been affected by this incident.

What Information Was Involved?

Your first and last name, address, and Social Security, debit card, and account numbers were contained in an unencrypted email located in a mailbox that was compromised. Your phone number may have also been included.

What We Are Doing

As soon as the unauthorized access was detected, we took prompt action to isolate and remove the unauthorized users. We contracted with an outside computer forensic company to monitor our email accounts for additional unauthorized access. We have also had our outside forensic company monitor our internal network and systems. We have not detected any indications that unauthorized users gained access to our internal network or our core system.

We have not detected any unauthorized access to our employees' email accounts since January 14, 2019. Since there was no detected intrusion into the bank's core systems, we remain secure and we are continuing to conduct business as usual. We have not detected any unauthorized transactions linked to this incident. We are remaining vigilant, and will try to act quickly if we become aware of any unauthorized transactions.

What You Can Do

Even though we are aware of the security incident and are taking precautionary actions, you should always closely monitor your account statements, especially over the next twelve to twenty four months, and notify us if you identify any fraudulent charges. You should contact us to inform us of any fraudulent charges by calling 888-492-3756 Monday through Thursday, 9 a.m. to 4 p.m. and Friday, 9 a.m. to 5 p.m. and Saturdays, 9 a.m. to Noon. You should call that same number if you have any questions or concerns about this incident.

In addition to notifying us of any fraudulent activity or identity theft, you can contact the FBI, your attorney general, and Federal Trade Commission (FTC) if you notice any fraudulent activity that involves your personally identifiable information. You should also periodically obtain your credit report from consumer reporting agencies: Experian, Equifax, and Transunion. You should request any fraudulent transactions be deleted from your credit report. You can obtain a copy of your credit report for free by going to the following website: https://www.consumer.ftc.gov/articles/0155-free-credit-reports, calling 1-877-322-8228, or mailing the Annual Credit Report Request Form to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can also obtain your credit report directly from each of the three consumer reporting agencies:

Experian
www.experian.com
(888)397-3742
P.O. Box 4500,
Allen, TX 75013

TransUnion
www.transunion.com
(800)888-4213
P.O. Box 1000
Chester, PA 19016

Equifax
www.equifax.com
(888)548-7878
P.O. Box 740241
Atlanta, GA 30374

While we do not believe that unauthorized users are attempting to use your personally identifiable information, we are offering twelve (12) months of credit monitoring at no cost to you. To activate your credit monitoring and start monitoring your personal information please follow the steps below:

- Ensure that you enroll by May 31, 2019 (Your code will not work after this date.)
- Visit the following website to enroll: https://www.experianidworks.com/credit
- Provide your activation code: **[Insert Code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-890-9332 by May 31, 2019. Be prepared to provide engagement number **[Insert Code]** as proof of eligibility for the identity restoration services by Experian.

We do not believe that the unauthorized users obtained all of the information they would need in order to use your debit card, so you can continue to use your existing debit card. If, however, you are concerned about the potential for unauthorized use of your debit card then you can obtain a new debit card at no cost to you at any of our branches. In addition, you can obtain a new account number from us at no charge by visiting one of our branches.

Other Important Information

You may also want to consider placing a fraud alert on your credit report. A fraud alert informs creditors that you may be the victim of fraud. You can place a fraud alert on your credit report by contacting one of the consumer reporting agencies. Once you create a fraud alert with one agency it will inform the other two. You can find contact information for the agencies at: https://www.consumer.ftc.gov/articles/0155-free-credit-reports. You can learn more and report incidents of identity theft by visiting https://www.consumer.ftc.gov/features/feature-0014-identity-theft or by calling 1-877-ID-THEFT (438-4338).

Unfortunately, it is impossible to completely prevent an attack by sophisticated and determined cyber-criminals. We care about the protection and security of your information, and will continue to use all reasonable efforts to safeguard your information. We apologize for any inconvenience you may experience as a result of this incident.

Call 888-492-3756 for more information.

Sincerely,

Kevin Klemesrud
President
American State Bank