18444

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Mail Date>>

Re: Notice of Data Breach

Dear <<Name 1>>:

American Bank Systems ("ABS") provides software to its bank partners, including NexTier Bank, and writes to notify you of an incident that may affect the security of some of your personal information. ABS takes the protection of your information very seriously, and this letter provides details of the incident, our response, and resources available to you to help protect your personal information from possible misuse.

What Happened? On October 22, 2020, ABS became aware that it was victimized by a cybercriminal and certain systems were infected with malware, which resulted in disruptions to certain ABS operations. We immediately took systems offline and launched an investigation into the nature and scope of the incident. With the assistance of third-party computer forensic specialists, we worked to investigate the source of the disruption, confirm its impact on our systems, and restore full functionality to our systems as soon as possible. The investigation determined that certain documents stored within ABS's environment were subject to unauthorized acquisition and were removed from our environment by the cybercriminal. On November 16, 2020, our investigation determined that information related to NexTier Bank customers was part of the information that was taken. ABS provided notice of the incident to NexTier Bank on November 18, 2020 and worked with NexTier Bank to determine address information to provide notice of the incident as quickly as possible. Please note that NexTier Bank's systems and networks were NOT affected by this incident. This incident involved only ABS's systems.

What Information Was Involved? Our investigation determined that the affected information may have included customer name and Social Security Number or Individual Taxpayer Identification Number as well as address, account number, loan information, and date of birth for some of our customers. Please note that not all data elements may have been involved for all customers. This incident did not include email addresses or login credentials for online or mobile banking.

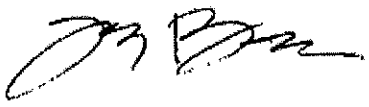
What We Are Doing. Information security is among our highest priorities. Upon discovering this incident, we immediately took steps to assess the security of our systems and mitigate the impact of this incident, including by resetting passwords of ABS users. We also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information in our care.

We are offering you access to <<CM Length>> months of credit monitoring and identity theft protection services through TransUnion at no cost to you as an added precaution. If you wish to activate these services, you may follow the instructions included in the attached *Steps You Can Take to Protect Your Information*. We encourage you to enroll in these services as we are unable to act on your behalf to do so.

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 and to detect errors for the next 12 to 24 months. If you suspect fraud in your accounts, please report such activity to NexTier Bank. Please also review the information contained in the attached *Steps You Can Take to Protect Your Information*.

For More Information. We understand that you may have questions about this incident that are not addressed in this letter. If so, please contact our toll-free dedicated assistance line at 855-914-4705 8:00 am to 8:00 pm Central Time, Monday through Friday. You may also write to ABS at 14000 Parkway Commons Drive, Oklahoma City, Oklahoma 73134.

Sincerely,



James Bruce
President/CEO & General Counsel
American Bank Systems

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Enroll in Credit Monitoring

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion,® one of the three nationwide credit reporting companies.

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at www.MyTrueIdentity.com and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter Activation Code>>** and follow the three steps to receive your credit monitoring service online within minutes.
- If you do not have access to the Internet and wish to enroll in a similar offline, paper-based credit monitoring service, via U.S. mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the six-digit telephone passcode **<<Insert static six- digit Telephone Pass Code>>** and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.
- The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion, including fraud alerts, new inquiries, new accounts, new public records, late payments, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

Free Credit Reports

Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. We recommend periodically obtaining credit reports from each nationwide credit reporting agency. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus listed below directly to request a free copy of your credit report. Upon receiving your credit report, review it carefully. Look for accounts you did not open. Look in the "inquiries" section for names of creditors from whom you have not requested credit. Some companies bill under names other than their store or commercial names; the credit bureau will be able to tell if this is the case. Look in the "personal information" section for any inaccuracies in information (such as home address and Social Security number).

If you see anything you do not understand, call the credit bureau at the telephone number on the report. Errors may be a warning sign of possible identity theft. You should notify the credit bureaus of any inaccuracies in your report, whether due to error or fraud, as soon as possible so the information can be investigated and, if found to be in error, corrected. If there are accounts or charges you did not authorize, immediately notify the appropriate credit bureau by telephone and in writing. Information that cannot be explained should also be reported to your local police or sheriff's office because it may signal criminal activity.

Security Freezes

You have the 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. The security 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 security 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 security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/freeze/center.html

TransUnion
P.O. Box 160
Woodlyn, PA 19094
1-888-909-8872
www.transunion.com/credit-freeze

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior 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.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

Fraud Alerts

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your 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 agencies listed below:

Experian
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax
P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
www.equifax.com/personal/credit-report-services

You can further educate yourself regarding identity theft prevention, 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.

Contact the Federal Trade Commission and Law Enforcement

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and 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.