

EXHIBIT 1

By providing this notice, American Bank Systems, Inc. (“ABS”), and its client, Royal Bancshares, Inc. (“Royal Bank”), do not waive any rights or defenses regarding the applicability of Maine law, the Maine data breach notification statute, or personal jurisdiction.

Nature of the Data Event

ABS provides banking software services as a service provider to several banks who are its clients. On October 22, 2020, ABS discovered suspicious activity impacting the operability of certain ABS systems that stored personal information of its banking clients. Upon discovering this activity, ABS immediately took systems offline and commenced an investigation to determine the nature and scope of the activity. Working with third party investigators, ABS determined that an unknown actor encrypted certain systems using malware. The investigation determined that certain personal information of banking clients may have been accessed or exfiltrated as a result of this event. ABS conducted a thorough review of the accessed or exfiltrated files, working to confirm the identities of the individual customers of its banking clients whose information may have been affected. On November 2, 2020, ABS began notifying certain banking clients that their individual customers’ information may have been impacted by this incident. Because the impacted data was identified on a rolling basis, ABS notified impacted banking clients on a rolling basis between November 2, 2020 and November 25, 2020. ABS notified Royal Bank on November 18, 2020. ABS provided Royal Bank and its other banking clients with lists of potentially impacted individual customers. Since that time, ABS has been working with the affected clients to confirm the contact information for these individuals who are customers of its banking clients.

ABS requested approval from its banking clients to notify the potentially impacted individual customers on the clients’ behalf. Once the clients granted approval, ABS developed a communications plan to issue written notice to impacted individual customers of those individual banks on the banks’ behalf.

The investigation determined that the following types of information belonging to Royal Bank customers may have been accessed or exfiltrated as a result of this event: name, address, date of birth, tax ID, and financial and/or loan account number(s). To date, the investigation has found no evidence of any actual or attempted misuse of personal information as a result of this event.

Notice to Maine Residents

On or around December 4, 2020, ABS began providing written notice of this incident to potentially affected individual customers of its banking clients, in accordance with the approval granted by those clients. Notice by ABS on behalf of Royal Bank to Royal Bank’s customers began on December 16, 2020 and includes twenty-one (21) Maine residents. Written notice is being provided in substantially the same form as the letter attached here as Exhibit A. The customer notifications provided to Royal Bank customers describe the additional steps that ABS and Royal Bank will take to help future incidents from occurring in the future, which are also detailed below.

Other Steps Taken and To Be Taken

Upon discovering the incident, ABS immediately launched an investigation to determine the nature and scope of this incident, as well as determine what data may potentially be affected. The investigation included working with an external forensic investigation firm.

ABS provided notice to all of its banking clients whose customer information was potentially affected by this event. With the clients' approval, ABS is also providing written notice to the individual banking customers whose information may have been affected. This notice includes an offer of complimentary access to 12 months of credit and identity monitoring services, including identity restoration services, through TransUnion for impacted individuals, and the contact information for a dedicated call center for potentially affected customers to contact with questions or concerns regarding this incident.

Additionally, ABS is providing potentially impacted individual customers with guidance on how to better protect against identity theft and fraud, including information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. At the direction of the impacted clients, ABS also may be providing notice of this event to other regulators pursuant to applicable state or federal laws.

To help prevent incidents like this from happening again, ABS began working with impacted institutions to ensure data entrusted to ABS is adequately protected with rigorous security procedures. Royal Bank has also reviewed its existing security policies and implemented advanced endpoint monitoring to further protect information in its care.

EXHIBIT A



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>>

<<Variable Heading>>

American Bank Systems (“ABS”) provides electronic data filing software to hundreds of financial institutions in the United States. This letter is to notify you that ABS recently discovered that an unauthorized party may have accessed information held by ABS for these institutions. The impacted data includes some Royal Bank customer and other consumer personal information that may affect you.

This incident does not involve any Royal Bank systems, which include those used to store and process customer funds, banking activities, online and mobile banking, cash management and debit/credit card account systems.

ABS has a 50-year history of support for financial institutions and takes the protection of your information very seriously. We have no evidence of identity theft or fraud as a result of this incident. This letter provides details of the incident, our response, and resources available to help protect your personal information from possible misuse, should you feel it is appropriate to do so.

What Happened? On October 22, 2020, ABS became aware that data stored within ABS’s environment was subject to unauthorized access or acquisition. On November 16, 2020 it was discovered this included information ABS held in order to upgrade software for Royal Bank. Some customer information was included in this data.

On November 18, 2020, ABS provided notice of the incident to impacted banks and worked to review the incident. We have now completed this review.

What Information Was Involved? Our investigation determined that the data impacted includes a backup database containing some Royal Bank customer and other consumer personal information. This may contain data about you, including address, date of birth, tax ID, and account number(s). In some cases, the accounts may no longer be open or active.

What We Are Doing. Upon discovering this incident, ABS immediately took steps to block the unauthorized access and mitigate the impact. ABS began working with impacted institutions to ensure data entrusted to us is adequately protected with rigorous security procedures. We also reviewed existing security policies and implemented advanced endpoint monitoring to further protect information in our care.

Although we are unaware of any identity theft or fraud as a result of this incident, we are offering you access to <<CM Length>> months of credit monitoring and identity theft protection services through TransUnion at no cost to you. The identity theft protection services include up to \$1,000,000 identity theft insurance as well as an identity restoration program in the event the individual’s identity is compromised. 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, 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 your local Royal Bank branch office. 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,

A handwritten signature in black ink, appearing to read "JB", is positioned above the typed name and title.

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 (*myTrueIdentity*) 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 *myTrueIdentity* 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.)

Special note for minors affected by this incident: The same services referred to above may not be available to affected minors. As an alternative, parents/legal guardians can check to see if your child may be a victim of identity theft by using TransUnion’s secure online form at www.transunion.com/childidentitytheft to submit your information so TransUnion can check their database for a credit file with your child’s Social Security Number. After TransUnion’s search is complete, they will respond to you at the email address you provide. If they locate a file in your child’s name, they will ask you for additional information in order to proceed with steps to protect your child from any impact associated with this fraudulent activity.

Monitor Accounts

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 and have information relating to fraudulent transactions deleted. 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.

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

As an alternative to a fraud alert, 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.

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. 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.

For District of Columbia residents, the Attorney General for the District of Columbia may be contacted at 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and <https://oag.dc.gov>.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-410-528-8662; 1-888-743-0023; or www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violators. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6000; or www.ncdoj.gov. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.