BAKER DONELSON
BEARMAN, CALDWELL & BERKOWITZ, PC

MONARCH PLAZA
SUITE 1500
3414 PEACHTREE ROAD N.E.
ATLANTA, GEORGIA 30326

PHONE: 404.577.6000
FAX: 404.221.6501

www.bakerdonelson.com

ALEXANDER F. KOSKEY, III, CIPP/US, CIPP/E, PCIP
Direct Dial: 404.443.6734
Email: akoskey@bakerdonelson.com

April 12, 2022

VIA U.S. MAIL

Consumer Protection Bureau
Office of the New Hampshire Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Notice of Data Incident*

To Whom It May Concern:

We represent IBKC Mortgage, a division of First Horizon Bank ("IBKC"). IBKC's principal place of business is located at 200 W. Congress St., Lafayette, LA 70501.[1] This correspondence is to notify you of a recent security incident reported by Technology Management Resources, Inc. ("TMR") in its lockbox application.

TMR is a third-party service provider of IBERIABANK, a division of First Horizon Bank. IBKC has a lockbox service with IBERIABANK for collecting and processing payments from its customers. TMR is a third-party service provider used to process payments and capture pertinent payment data for items received in the lockbox. On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. IBERIABANK determined that the activity was unauthorized. According to TMR, the unauthorized activity occurred between October 12, 2021 and October 14, 2021.[2] The incident did not affect IBKC's computer systems.

According to TMR's investigation, there may have been unauthorized access to bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes accessed by the threat actor were in binary format only as an encoded string and no actual images were viewed during the period of the unauthorized access.

[1] By providing this notice, IBKC does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

[2] IBERIABANK has notified law enforcement of this incident.

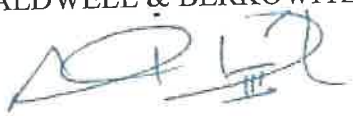
Although TMR's investigation did not reveal any evidence to confirm that the bytes accessed by the threat actor were converted into images, it could have been possible. Due to the risk that personally identifiable information may have been accessed, in an abundance of caution, a notification letter is being sent via U.S. Mail to 1 New Hampshire resident on or about April 12, 2022. The notification letter includes instructions for activating one (1) year of credit monitoring services at no cost to the residents. The PII that was potentially at risk included first and last names and financial account numbers. A sample notification letter is enclosed for your reference and includes:

- A description of the incident;
- Steps taken to investigate the incident;
- Steps taken to mitigate any potential harm to individuals;
- Instructions for activation of 1 year of free credit monitoring and identity theft protection services;
- Instructions on how to place a security freeze on the recipient's consumer credit report; and
- Instructions regarding how to obtain more information about this incident.

IBKC is fully committed to protecting consumer privacy and the confidentiality of personal information. Please contact me if you require any additional information regarding this incident.

Best regards,

BAKER, DONELSON, BEARMAN,
CALDWELL & BERKOWITZ, PC



Alexander F. Koskey, III

Exhibit 1: Sample notification letter to 1 resident

IBERIABANK

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>>

<<Date>>

RE: <<Variable Header>>

Dear <<Name 1>>:

IBKC Mortgage, a division of First Horizon Bank (the "Company"), is writing to notify you of a security incident. The Company has a lockbox service with IBERIABANK for collecting and processing payments from its customers. IBERIABANK uses Technology Management Resources, Inc. (TMR) as a third-party lockbox service provider to process payments and capture pertinent payment data for items received in the lockbox. You made a payment or submitted information to the Company's IBERIABANK lockbox. TMR alerted IBERIABANK of an incident that may have involved your personal information. This correspondence is intended to provide you with information regarding the incident and the resources available to you to help protect your information, should you feel it appropriate to do so.

What happened? On October 14, 2021, TMR identified unusual activity with a user account in its lockbox application. IBERIABANK determined that the activity was unauthorized, and the account was promptly disabled. TMR investigated the incident and reported that the unauthorized activity occurred between October 12, 2021, and October 14, 2021. According to TMR's investigation, the threat actor accessed bytes that were associated with certain images for lockbox payments and related documents. TMR has stated that the bytes (bits of computer data) accessed by the threat actor were in binary format only and as an encoded string (this means that the data was an encoded series of information stored in the form of ones and zeros). Technical manipulation of the bytes would be required to convert them into images. No actual images were viewed by the threat actor during the period of unauthorized access. The investigation determined that it is likely that these bytes were obtained by the threat actor based upon traffic to the IP address. However, the investigation has not revealed any evidence to confirm that the threat actor converted the bytes into images, although this could have been possible.

What information was involved? The encoded data was associated with certain check images and related documents within the third-party lockbox service application. These images generally consisted of information typically included on checks such as name, address, account numbers and bank routing number. This information is similar to that which appears on a check anytime an individual makes a purchase or pays a bill. Specifically, the information potentially involved may have included <<Breached Elements>>.

What is IBERIABANK doing in response? We take the protection and proper use of personal information very seriously. As part of our ongoing commitment to information privacy and the security of information, we are notifying you of this incident. Although we are not aware of any misuse of your information as a result of this incident, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection through TransUnion. These services will be available to you for <<Variable Data 3 – CM Length>> months at no cost to you in order to give you peace of mind. You must complete the enrollment steps listed in this letter to activate these services.

What you can do. As a best practice, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, and to monitor your credit reports for suspicious activity. This letter also includes additional information and resources to assist you in protecting your personal information, should you feel it appropriate to do so. You may also enroll in the complimentary credit monitoring and identity theft protection services we are making available to you as a professional courtesy and in an abundance of caution.

For more information. If you have additional questions about the 2021 lockbox service provider security incident or the protections available to you, please call 1-855-604-1755, toll-free, Monday through Friday, 9:00 a.m. – 9:00 p.m. Eastern Time. We apologize for any inconvenience this 2021 lockbox service provider security incident may have caused you.

Sincerely,

IBKC Mortgage, a division of First Horizon Bank

TransUnion

Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*my*TrueIdentity) for <<Var Data 3 – CM Lenth>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *my*TrueIdentity website at **www.mytrueidentity.com** and in the space referenced as "Enter Activation Code", enter the following unique 12-letter Activation Code **<<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 following 6-digit telephone pass code **<<Engagement Number>>** 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.

Once you are enrolled, you will be able to obtain <<Var Data 3 – CM Lenth>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. 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, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *my*TrueIdentity online 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 credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *my*TrueIdentity online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *my*TrueIdentity Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.

ADDITIONAL STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Monitor Your Accounts and Order Your Free Annual Credit Reports

In addition to enrolling in the complimentary credit monitoring services above, we encourage you to remain vigilant against incidents of identity theft and fraud, to review your financial account statements, debit/credit card statements, and other statements, and to monitor your credit reports for suspicious activity to detect errors. (For Oregon and Iowa residents: Report any suspected identity theft to law enforcement, the Federal Trade Commission and your State Attorney General). Under U.S. law, you are entitled to one free credit report annually from each of the three major credit bureaus. 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 to request a free copy of your report. (For Colorado, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico and Vermont residents: You may obtain additional copies of your credit report, free of charge. You must contact each of the three consumer reporting agencies directly to obtain such additional reports). Periodically review a copy of your credit report for discrepancies and identify any accounts you did not open or inquiries you did not authorize.

Freeze Your Credit File

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 a security freeze on your credit report. Note that a security freeze generally does not apply to an existing creditor or its agents or affiliates for certain types of account review, collection, fraud Control or similar activities. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian	**TransUnion**	**Equifax**
P.O. Box 9554 Allen, TX 75013	P.O. Box 160 Woodlyn, PA 19094	P.O. Box 105788 Atlanta, GA 30348
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com	www.transunion.com	www.equifax.com

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, II, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide 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, include a copy of either the police report, investigative report or complaint to a law enforcement agency concerning identity theft.

If you request a security freeze via toll-free telephone or other secure electronic means, the credit reporting agencies have one (1) business day after receiving the request to place the freeze. In the case of a request made by mail, the bureaus have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze. To lift the security freeze to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving a request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving the request to remove the freeze.

Place Fraud Alerts on Your Credit File

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 one-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 (7) years. Should you wish to place a fraud alert, please contact any one of the consumer reporting agencies listed above to activate an alert.

File or Obtain a Police Report

You have the right to file or obtain a police report if you experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide proof that you have been a victim. A police report is often required to dispute fraudulent items. You can generally report suspected incidents of identity theft to local law enforcement or to the Attorney General.

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, 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 (FTC) can be reached at 600 Pennsylvania Avenue NW, Washington, D.C. 20580, by phone at 1-877-ID-THEFT (1-877-438-4338), TTY: 1-866-653-4261, or by going to www.ftc.gov/idtheft. The FTC 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 a complaint through the above-referenced contact information.

You also have rights under the federal Fair Credit Reporting Act (FCRA), which promotes the accuracy, fairness and privacy of information in the files of consumer reporting agencies. These rights include the right to receive a copy of your credit report, the right to ask for a credit score, the right to dispute incomplete or inaccurate information, and the right to obtain corrections to your report or delete inaccurate, incomplete, unverifiable information. Consumer reporting agencies may not report outdated negative information. Access to your file is limited, and you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you receive based upon information in your credit report. You may have additional rights under the FCRA not summarized here. We recommend and encourage you to review your rights pursuant to the FCRA at https://files.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 Avenue N.W., Washington D.C., 20580.

For residents of North Carolina: The North Carolina Office of the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226, and www.ncdoj.com. You can obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.

For residents of Maryland: The Maryland Office of the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, and www.oag.state.md.us. You can obtain information from the Attorney General or Federal Trade Commission about preventing identity theft.

For residents of New Mexico: 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. Furthermore, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccuracies, 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 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 residents of New York: 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 residents of Rhode Island: The Rhode Island Office of the Attorney General can be contacted at: 150 South Main Street, Providence, RI 02903, 1-401-274-4400 and www.riag.ri.gov. Under Rhode Island law, you have the right to obtain any police report filed regarding this incident. There are <<RI #>> Rhode Island residents impacted by this incident.

For residents of the District of Columbia: The Attorney General may be contacted at: 400 6th Street NW, Washington, D.C. 20001, 1-(202) 727-3400 and https://oag.dc.gov/. You may obtain information from the Attorney General or the Federal Trade Commission about preventing identity theft.