Jeffrey J. Boogay
Office: 267-930-4784
Fax: 267-930-4771
Email: jboogay@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

March 27, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Security Incident

Dear Attorney General MacDonald:

We represent First Bank of Alabama (hereinafter referred to as "FBA"), where one of its primary offices is located at 120 North St. E, Talladega, Alabama 35160. We write to notify your office of an incident that may affect the security of some personal information relating to approximately one (1) New Hampshire resident. The investigation into this matter is ongoing, and this notice may be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, FBA 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.

Nature of the Data Event

On September 20, 2018, FBA became aware of unusual activity in an employee's email account. FBA immediately launched an investigation to determine what happened and what information may have been affected. With the assistance of computer forensics experts, FBA learned that a single FBA email account was accessed without authorization by an unknown party between September 6, 2018 and September 20, 2018.

FBA undertook a lengthy review of the email account to determine if any information was subject to unauthorized access. When the investigation could not rule out the possibility of such access, FBA engaged in a programmatic and manual review of the email account to determine if personal information existed in the account at the time of the incident. That review concluded on December 13, 2018. FBA then took steps to confirm address information for the potentially impacted individuals for purposes of providing notification to those individuals. FBA confirmed the email account contained personal information relating to approximately one (1) New Hampshire resident including name and Social Security number.

Notice to New Hampshire Resident

On or about March 27, 2019 FBA provided written notice of this incident to affected individuals, which includes one (1) New Hampshire resident. Written notice is being provided in substantially the same form as the letter attached here as ***Exhibit A***.

Other Steps Taken and To Be Taken

Upon discovering the event, FBA moved quickly to investigate and respond to the incident, assess the security of FBA's systems, and notify potentially affected individuals. FBA has strict security measures in place to protect information and upon learning of this incident, took additional steps relating to its employee email accounts. FBA reset passwords for FBA email accounts, implemented increased security measures for email account access, and are currently reviewing our policies and procedures relating to data security.

FBA is also providing access to identity and credit monitoring services for one (1) year, through Kroll, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, FBA is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. FBA is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, information on protecting against tax fraud, 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. FBA also provided relevant regulatory notices.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4784.

Very truly yours,

Jeffrey J. Boogay of
MULLEN COUGHLIN LLC

JJB/ajd
Enclosure

EXHIBIT A

First Bank OF ALABAMA

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

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

RE: Notice of Data Breach

Dear <<FirstName>> <<LastName>>,

First Bank of Alabama ("FBA") writes to notify you of a recent incident that may affect the security of some of your personal information. While there is currently no evidence that your information has been misused as a result of this incident, we are providing you with information on the event, steps we have taken since discovering the incident, and what you may do to better protect your personal information should you feel it appropriate to do so.

What Happened? On or about September 20, 2018, FBA became aware of unusual activity in an employee's email account. We immediately launched an investigation to determine what happened and what information may have been affected. With the assistance of computer forensics experts, we learned that a single FBA email account was accessed without authorization between September 6, 2018 – September 20, 2018.

FBA undertook a lengthy review of the email account to determine if it contained personal information, and determined on December 13, 2018 that information related to you was present in the account. We promptly launched a review of our files to ascertain address information for all impacted individuals. Although, to date, we are unaware of any actual or attempted misuse of this information, we are notifying you in an abundance of caution because your information was present in the impacted email account at the time of the incident.

What Information Was Involved? FBA cannot confirm if your information was actually viewed by the unauthorized individual. However, our investigation confirmed the information present in the impacted email account at the time of the incident includes your <<ClientDef1(name[, / and] data elements)>><<ClientDef2(data elements)>>.

What We Are Doing. Information privacy and security are among our highest priorities. FBA has strict security measures in place to protect information in our care. Upon learning of this incident, we took steps to confirm the security of our systems, including our employee email accounts. We reset passwords for FBA email accounts, implemented increased security measures for email account access, and are currently reviewing our policies and procedures relating to data security. Additionally, we notified relevant regulatory agencies.

While, to date, we have no evidence of actual or attempted misuse of information as a result of this incident, we are notifying potentially affected individuals, including you, so that you may take further steps to better protect your personal information should you feel it is appropriate to do so. We also secured the services of Kroll to provide identity monitoring services at no cost to you for one (1) year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **krollbreach.idMonitoringService.com** to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: **<<Member ID>>**

To receive credit services by mail instead of online, please call 1-866-337-8871. Additional information describing your services is included with this letter.

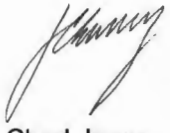
For more information on these services, please review the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud."

What You Can Do. You may review the information contained in the enclosed "Steps You Can Take to Protect Against Identity Theft and Fraud". You may also enroll to receive the identity monitoring services we are making available to you as we are unable to enroll in these services on your behalf.

For More Information. We understand you may have questions about this incident that are not addressed in this letter. To ensure your questions are answered in a timely manner, you can contact our toll-free dedicated assistance line at 1-866-337-8871, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time. You may also write to us at Attn: Legal Department, P.O. Box 797, Talladega, AL 35161.

FBA takes the privacy and security of the personal information in our care very seriously. We sincerely regret any inconvenience or concern this incident may cause you.

Sincerely,



Chad Jones
President and CEO
First Bank of Alabama

Steps You Can Take to Protect Against Identity Theft and Fraud

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 over the next 12-24 months. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting 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 directly to request a free copy of your credit report.

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	**TransUnion**	**Equifax**
PO Box 9554	P.O. Box 2000	PO Box 105788
Allen, TX 75013	Chester, PA 19016	Atlanta, GA 30348-5788
1-888-397-3742	1-888-909-8872	1-800-685-1111
www.experian.com/freeze/center.html	www.transunion.com/credit-freeze	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, 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.

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	**TransUnion**	**Equifax**
P.O. Box 2002	P.O. Box 2000	P.O. Box 105069
Allen, TX 75013	Chester, PA 19106	Atlanta, GA 30348
1-888-397-3742	1-800-680-7289	1-888-766-0008
www.experian.com/fraud/center.html	www.transunion.com/fraud-victim-resource/place-fraud-alert	www.equifax.com/personal/credit-report-services

Although we have no reason to believe that your personal information has been used to file fraudulent tax returns, you can contact the IRS at www.irs.gov/Individuals/Identity-Protection for helpful information and guidance on steps you can take to address a fraudulent tax return filed in your name and what to do if you become the victim of such fraud. You can also visit www.irs.gov/uac/Taxpayer-Guide-to-Identity-Theft for more information.

You can further educate yourself regarding identity theft, 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); 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 North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, 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 violator. 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 Rhode Island Residents: The Rhode Island Attorney General can be reached at: 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, 1-401-247-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are XXX Rhode Island residents impacted by this incident.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services[1] from Kroll:

Single Bureau Credit Monitoring. You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher. Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona. Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan. Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

$1 Million Identity Fraud Loss Reimbursement. Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation. You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration. If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

[1] Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.