Vincent F. Regan
Office: (267) 930-4842
Fax: (267) 930-4771
Email: vregan@mullen.law

309 Fellowship Road, Suite 200
Mt. Laurel, NJ 08054

September 3, 2024

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
E-mail: idtheft@oag.state.md.us

Re: Notice of Data Event

To Whom It May Concern:

We represent First Security Bank located at 312 Maple Street, Overbrook, Kansas, 66524 and are writing to notify your office of an incident that may affect the security of certain personal information relating to one (1) Maryland resident. By providing this notice, First Security Bank does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Data Event

On or about March 18, 2024, First Security Bank became aware of suspicious activity that was ultimately isolated to one (1) specific email account. Upon discovery, the First Security Bank team immediately secured the account and launched an investigation to determine the full nature and scope of the incident. Through this investigation, First Security Bank determined that the email account was subject to unauthorized access between February 9, 2024, and March 18, 2024. In response to the unauthorized access, First Security Bank undertook a comprehensive review of the contents of the potentially impacted account to determine what information was contained therein and to whom it related. Through the review, on or about July 16, 2024, it determined there was some sensitive information present in the email account at the time of the incident, and thus potentially accessed without authorization, though it has no evidence the information was taken or misused.

The information that could have been subject to unauthorized access includes name, account number, and account type.

Notice to Maryland Resident

On September 3, 2024, First Security Bank provided written notice of this incident to one (1) Maryland 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, First Security Bank moved quickly to investigate and respond to the incident, assess the security of First Security Bank systems, and identify potentially affected individuals. Further, First Security Bank notified federal law enforcement regarding the event, The Federal Deposit Insurance Corporation, Cybersecurity and Infrastructure Security Agency, and Office of the State Bank Commissioner of Kansas. First Security Bank is also working to implement additional safeguards and training to its employees. First Security Bank is providing access to credit monitoring services for twelve (12) months, through TransUnion, to individuals whose personal information was potentially affected by this incident, at no cost to these individuals.

Additionally, First Security Bank 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 bank. First Security Bank is providing individuals with 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.

First Security Bank is providing written notice of this incident to relevant state and federal regulators, as necessary, and to the three major credit reporting agencies, Equifax, Experian, and TransUnion.

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at (267) 930-4842.

Very truly yours,

Vincent F. Regan of
MULLEN COUGHLIN LLC

VFR:scs
Enclosure

EXHIBIT A

First Security Bank
c/o Cyberscout
555 Monster Rd SW
Renton, WA 98057
DB-09124

3_0000102

0000102

First Security Bank

September 3, 2024

NOTICE OF SECURITY INCIDENT

Dear

First Security Bank is writing to notify you of an isolated incident that may affect the privacy of some of your information. We know how important your personal information is and we take its protection very seriously and are providing details of the incident and the resources available to you to help protect your information from possible misuse, should you feel it is appropriate to do so. Though we determined there was some sensitive information potentially accessed without authorization, we have no evidence the information was taken or misused.

What Happened?

On or about March 18, 2024, First Security Bank became aware of suspicious activity that was ultimately isolated to one specific email account. Upon discovery, our team immediately secured the account and launched an investigation to determine the full nature and scope of the incident. Through this investigation, we determined that the email account was subject to unauthorized access between February 9, 2024, and March 18, 2024. In response to the unauthorized access, First Security Bank undertook a comprehensive review of the contents of the potentially impacted account to determine what information was contained therein and to whom it related. Through the review, on or about July 16, 2024, we determined there was some sensitive information present in the email account at the time of the incident, and thus potentially accessed without authorization, though we have no evidence the information was taken or misused.

What Information Was Involved?

While we have no evidence that your information has been subject to misuse, the following types of your information were present in the accessed account: your name and account number, date of birth, account type, routing number, institution name, full access credentials, medical information, and Health Insurance Information.

What We Are Doing.

Upon discovery of this incident, we immediately took steps to secure the account by changing the password and conducted a diligent investigation to confirm the incident was isolated to only an email account. As part of First Security Bank's ongoing commitment to the security of information, our policies and procedures regarding information security are being reviewed and enhanced, for any additional safeguards have been implemented and additional training is being conducted to reduce the likelihood of a similar event in the future. We also reported this incident to federal law enforcement and are cooperating with their investigation.

As an added precaution, we are also offering you complimentary access to twelve (12) months of credit monitoring and identity theft restoration services, through TransUnion. You will need to enroll yourself in these services if you wish to do so, as we are not able to activate them on your behalf. Please review the instructions contained in the attached *Steps You Can Take to Help Protect Your Personal Information* for additional information on these services.

What You Can Do.

We encourage you to remain vigilant against incidents of identity theft and fraud by reviewing your account statements, immediately reporting any suspicious activity to First Security Bank, and monitoring your free credit reports for suspicious activity and to detect errors over the next twelve (12) to twenty-four (24) months. You can find more information about how to obtain a free copy of your credit report, protect against potential identity theft and fraud, and place a fraud alert to put creditors on notice that you may be a victim of fraud, and other resources available to you in the enclosed *Steps You Can Take to Help Protect Your Information*. You may also enroll in the complimentary credit monitoring services available to you; detailed instructions for enrolling in these services are enclosed.

For More Information.

We understand that you may have questions about this incident that are not addressed in this letter. If you have additional questions, or need assistance, please call our dedicated assistance line at 1-800-405-6108 (toll-free), Monday through Friday, during the hours of 8:00 a.m. and 8:00 p.m. Eastern Standard Time (excluding U.S. national holidays).

Sincerely,

Michael L Needham
President
https://www.firstsecurityks.com/

Steps You Can Take to Help Protect Your Information

Enroll in Credit Monitoring Services

We are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for twelve (12) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://bfs.cyberscout.com/activate** and follow the instructions provided. When prompted please provide the following unique code to receive services:

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one (1) free credit report annually from each of the three (3) major credit reporting bureaus, Equifax, Experian, and TransUnion. To order a free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. Consumers may also directly contact the three (3) major credit reporting bureaus listed below to request a free copy of their credit report.

Consumers have the right to place an initial or extended "fraud alert" on a credit file at no cost. An initial fraud alert is a one (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 consumers are the victim of identity theft, they are entitled to an extended fraud alert, which is a fraud alert lasting seven (7) years. Should consumers wish to place a fraud alert, please contact any of the three (3) major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a "credit freeze" on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer's express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in a consumer's name without consent. However, consumers should be aware that using a credit freeze to take control over who gets access to the personal and financial information in their credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application they make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, consumers cannot be charged to place or lift a credit freeze on their credit report. To request a credit freeze, individuals may need to provide some or all of the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two (2) to five (5) 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, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if they are a victim of identity theft.

Should consumers wish to place a credit freeze or fraud alert, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
1-888-298-0045	1-888-397-3742	1-800-916-8800
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

Consumers may further educate themselves regarding identity theft, fraud alerts, credit freezes, and the steps they can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or their state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, D.C. 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, or have been the victim of identity theft, to promptly file a complaint with them and review the content on the Federal Trade Commission's website listed above. Consumers can obtain further information on how to file such a complaint by way of the contact information listed above. Consumers have the right to file a police report if they ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, consumers will likely need to provide some proof that they have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement, the relevant state Attorney General, and the Federal Trade Commission. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, D.C. 20001; (202) 442-9828; and oag.dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-410-576-6300 or 1-888-743-0023; and https://www.marylandattorneygeneral.gov/.

For those affected generally and New Mexico residents, consumers have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in their credit file has been used against them, the right to know what is in their credit file, the right to ask for their credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to consumers' files is limited; consumers must give consent for credit reports to be provided to employers; consumers may limit "prescreened" offers of credit and insurance based on information in their credit report; and consumers may seek damages from violators. Consumers 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 consumers to review their 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 New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or https://ag.ny.gov.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.