CONNELL FOLEY
A TRADITION OF LEGAL EXCELLENCE SINCE 1938

Connell Foley LLP
56 Livingston Avenue
Roseland, NJ 07068
P 973.535.0500 F 973.535.9217

April 21, 2023

VIA EMAIL - ATTORNEYGENERAL@DOJ.NH.GOV
Office of the Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301

Re: The Exchange Bank – Notice of Data Security Incident

Dear Attorney General Formella:

This firm represents The Exchange Bank ("Exchange Bank" or "Bank") relevant to the above referenced matter. We are writing to notify you of a data security incident involving the personal information of two (2) New Hampshire residents. By providing this notice, Exchange Bank does not waive any rights or defenses regarding the applicability of New Hampshire law, the New Hampshire data breach notification statute, or personal jurisdiction.

Exchange Bank maintains its headquarters at 300 W Rogers Blvd, Skiatook, OK 74070. On November 19, 2022, Exchange Bank encountered suspicious activity within its environment. The Bank immediately began an investigation with the assistance of forensic computer specialists. The Bank temporarily disconnected all systems from the Internet. Before resuming operations, Exchange Bank ensured all unauthorized access to its network was eradicated.

On December 9, 2022, the forensic investigation concluded that certain servers and workstations within the Exchange Bank environment had been infected with malware, and that data was accessed and/or exfiltrated by an unauthorized criminal actor. The Bank conducted a detailed review and analysis of the data impacted by this incident. On February 23, 2023, it was determined that the personal information of two (2) New Hampshire residents may have been impacted by this incident. The impacted information differed as to each individual, but included

.

At this time, Exchange Bank is unaware of any actual or attempted misuse of any personal information affected by this incident. Nevertheless, out of an abundance of caution, the Bank is sending a notification letter to all New Hampshire residents whose personal information may have been impacted. In furtherance of same, Exchange Bank has secured the services of Kroll Notification to provide credit monitoring and other identity theft monitoring services at no cost to these individuals for one (1) year. Attached for your reference is a template copy of the notification letter, which will be sent via U.S. mail on April 21, 2023.

Since the incident, Exchange Bank has implemented multiple network security improvements, including initiating system-wide password changes; installing Endpoint Detection & Response Software; moving its email environment to the cloud; using encryption when sending emails; and improving its data backup protocol.

Should you require any additional information, please do not hesitate to contact me.

Very truly yours,

CONNELL FOLEY LLP

KAREN PAINTER RANDALL

KPR/jam
Enclosure

EXCHANGE BANK

Your Community. Your Bank.

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

The Exchange Bank ("Exchange Bank" or "Bank") takes the protection and proper use of your information very seriously. For this reason, we are writing to tell you about a data security incident that may have impacted some of your personal information. We are contacting you directly to explain the circumstances of the incident.

Although we are unaware of any actual misuse of your information, we are providing notice to you and other potentially affected individuals about the incident, and providing tools you can use to help protect yourself against possible identity theft or fraud.

What happened?

On November 19, 2022, Exchange Bank encountered suspicious activity within its environment. Exchange Bank immediately began an investigation with the assistance of forensic computer specialists. The Bank temporarily disconnected all systems from the Internet and terminated the unauthorized access to its network.

The forensic investigation determined that certain servers and workstations within the Exchange Bank environment had been infected with malware. The investigation also found that that certain data was accessed and/or exfiltrated by an unauthorized criminal actor.

What information was involved?

After conducting a detailed review, Exchange Bank determined that the data which may have been accessed or exfiltrated contained the following information: your <<b2b_text_1(name, data elements)>>.

At this time, Exchange Bank is unaware of any actual or attempted misuse of any sensitive or personally identifiable information affected by this incident.

What we are doing.

Before resuming operations, Exchange Bank ensured all unauthorized access to its network was terminated. The Bank is unaware of any effect this incident had on customers' ability to access their funds or any Bank services.

Since the incident, Exchange Bank has implemented multiple network security improvements, including: initiating system-wide password changes; installing Endpoint Detection & Response Software; moving its email environment to the cloud; using encryption when sending emails; and improving its data backup protocol.

To help relieve concerns and restore confidence following this incident, Exchange Bank has secured the services of Kroll to provide identity monitoring at no cost to you for one 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, a Current Credit Report, Web Watcher, Public Persona, Quick Cash Scan, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.
*You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.*
Membership Number: **<<Membership Number s_n>>**

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter.

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For more information.

If you have questions, please call , Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays. Please have your membership number ready.

Protecting your information is important to us. We trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction.

Sincerely,

A.B. Bayouth Jr.
President

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

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 Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will have the option to call a Kroll fraud specialist, who will be able to help you determine if it is 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 will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will 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 will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.
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.