Appendix

On September 29, 2020, River City Bank (the "Bank"), discovered some unauthorized activity performed by a Bank employee. This individual downloaded customer data to a personal storage drive and later sent the information to a third party. In doing so, the employee exceeded their authorized access, which was limited to accessing the Bank's data for legitimate bank purposes. When the Bank first learned of this incident, it took immediate steps to restrict the employee's system access. It also reported the incident to law enforcement. A thorough investigation was conducted by a forensic investigation firm to determine what happened, who was impacted, and what information may have been affected. The Bank reviewed the entire contents of the database files that may have been affected and determined that it contained some personal information of one Maine resident, including name, Social Security number, and financial account number.

On November 20, 2020, the Bank began mailing written notifications to affected individuals, including the Maine resident who is being notified of the incident in writing in accordance with Me. Rev. Stat. Tit. 10, §1348.[1] A copy of the notification letter is attached. The Bank is offering the Maine resident a complimentary two-year membership in credit monitoring and identity theft protection services through Kroll. The Bank has also provided a telephone number for potentially affected individuals to call with any questions they may have.

To further protect against a similar incident from occurring in the future, the Bank is continuing to implement additional security measures and to train and educate its employees on information security and data protection.

[1] This notice is not, and does not constitute, a waiver of the Bank's objection that Maine lacks personal jurisdiction over it regarding any claims related to this data security incident

River City Bank

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

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

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

River City Bank ("the Bank") is committed to protecting the confidentiality and security of our customers' personal information. We are writing to inform you about an incident that may involve some of your information. This notice explains the data breach, measures we have taken, and some steps you can take in response.

What Happened

On September 29, 2020, we discovered some unauthorized activity performed by a Bank employee. This individual downloaded customer data, including yours, to a personal storage drive and later sent the information to a third party. In doing so, the employee exceeded their authorized access, which was limited to accessing the Bank's data for legitimate purposes. When we first learned of this incident, we took immediate steps to restrict the employee's system access. We also reported the incident to law enforcement. A thorough investigation was conducted by a forensic investigation firm to determine what happened, who was impacted, and what information may have been affected.

What Information Was Involved

We reviewed the entire contents of the database files that may have been affected. On November 4, 2020, we determined that it contained some of your personal information, including your <<b2b_text_1(Data Elements)>>.

What We Are Doing

Although to date we have no evidence that your information has been misused, as a precaution we are notifying you about the incident and we assure you that we take this incident very seriously. To help protect your identity and as a precaution, we are offering you complimentary identity monitoring services for two years through Kroll. Kroll is a leader in risk mitigation and response, and its team is experienced in helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **February 26, 2021** to activate your identity monitoring services.*

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

For additional information regarding the identity monitoring services being offered, please see the next section of this letter.

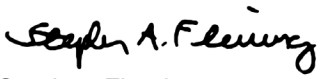
What You Can Do

We encourage you to take advantage of the identity monitoring services being offered. You should also always remain vigilant for incidents of fraud or identity theft by reviewing your free credit reports for any unauthorized activity. We also remind you to review your financial account statements closely and to report any unauthorized activity to your financial institution. Please see the pages that follow this notice for some additional steps you can take to help protect yourself.

For More Information

We sincerely regret that this occurred and apologize for any inconvenience or concern. To further protect against a similar incident from occurring in the future, we are continuing to implement additional security measures and to train and educate our employees on information security and data protection. **If you have any questions, please call 1-833-960-3572 between 8:00 am and 5:00 pm Pacific Time, Monday through Friday.** Please have your identity monitoring membership number, referenced above, ready.

Sincerely,



Stephen Fleming
President & CEO

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services 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 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.

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.

ADDITIONAL STEPS YOU CAN TAKE

Even if you choose not to take advantage of this free credit monitoring service, we remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity over the next 12 to 24 months. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax,* PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian,* PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion,* PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze,** PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze,** PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze,** PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information for residents of the following states:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office,* 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: The mailing address for River City Bank's headquarters is 2485 Natomas Park Dr. Ste 100, Sacramento, CA 95833 and the phone number is 916-567-2600. You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

Maryland: The mailing address for River City Bank's headquarters is 2485 Natomas Park Dr. Ste 100, Sacramento, CA 95833. You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office,* 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office,* 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.