FREEMAN MATHIS & GARY, LLP
Attorneys at Law

550 South Hope Street
Suite 2200
Los Angeles, CA 90071-2631

Tel: 213.615.7000

www.fmglaw.com

Zachariah E. Moura
Partner

Writer's Direct Access
213.615.7055

ZMoura@fmglaw.com

December 28, 2020

VIA EMAIL
Attorney General Gordon J. MacDonald
Office of New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301
DOJ-CPB@doj.nh.gov

RE: Notice of Breach in the Security of Personal Information

Dear Attorney General MacDonald:

We represent Carson Bank ("the Company"), which is a Kansas-based community banking institution. This letter is being provided pursuant to N.H. Rev. Stat. § 359-C:20, which requires that your office be notified in the event of a breach in the security of personal information affecting a resident of the state of New Hampshire.

The Company uses electronic account administration software provided by a company named American Bank Systems ("ABS"). On November 18, 2020, the Company was notified that, on October 22, 2020, ABS discovered it had been victimized by a cybercrime attack that infected some of its systems with malware and disrupted its operations. With the assistance of computer forensic specialists, ABS restored the functionality of its systems and investigated the incident. ABS then reported to the Company that its investigation found certain files stored on its network were accessed or acquired by the person or persons who committed the attack, and that some of these files contained personal information of the Company's customers.

The information on ABS's network believed to have been accessed or acquired by the unauthorized person or persons included the Company's clients' name, address, bank account name, account number, and Social Security number or tax identification number. At this time, neither the Company nor ABS are aware of any identity theft or fraud as a result of this incident or have any indication that any client's personal information has been misused. The Company believes this incident affected one resident of the state of New Hampshire.

Written notice will be mailed to all affected individuals on December 28, 2020. A sample copy of the notice letter is attached for your records.

As an added precaution, the Company is offering all affected New Hampshire residents 12 months of credit monitoring and fraud detection services, which includes a $1 million identity theft insurance policy and fully managed ID theft recovery services. The notice to the affected individuals includes instructions on the use of these services.

The Company has also taken additional steps in response to learning of this incident, including working closely with ABS to ensure that ABS thoroughly investigated the incident and has taken steps to prevent this from happening again. The Company has been assured that ABS immediately took steps to assess the security of its systems and mitigate the impact of this incident, including resetting their passwords. ABS also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information entrusted to it. The Company and ABS have also separately retained legal counsel to help respond to this incident.

I believe this provides you with all information necessary for your purposes and to comply with New Hampshire law. However, if you have any questions or need further information, please contact me.

Very truly yours,

FREEMAN MATHIS & GARY, LLP

ZACHARIAH E. MOURA

Encl.

cc: David A. Cole, Esq.

CARSON BANK
EST. 1886

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>>

Notice of Data Breach

Dear <<Name1>>:

At Carson Bank, we take our customers' privacy seriously. As part of that commitment, we are sending this letter to make you aware of a recent data security incident that may have affected your personal information. Please read this letter carefully.

What Happened

Carson Bank uses electronic account administration software provided by a company named American Bank Systems (ABS). ABS recently notified Carson Bank that, on October 22, 2020, ABS discovered it was victimized by a cybercrime attack that infected some of their systems with malware and disrupted its operations. With the assistance of computer forensic specialists, ABS restored the functionality of their systems and investigated the incident.

ABS then reported to us on November 18, 2020, that its investigation found certain files stored on their network were accessed or acquired by the person or persons who committed the attack, and that some of these files contained personal information of Carson Bank customers. Therefore, we are notifying all our potentially affected customers about this incident and providing them with the information and services described below to help protect their information from misuse.

What Information Was Involved

The information on ABS's network believed to have been accessed or acquired by the unauthorized person or persons included your name, address, bank account name and account number, and Social Security number or tax identification number. At this time, neither we nor ABS are aware of any identity theft or fraud as a result of this incident or have any indication that your personal information has been misused.

122 West Main
P.O. Box 158
Mulvane, Kansas 67110
P (316) 777-1171 F (316) 777-9015 TOLL FREE (888) 571-2233
carsonbank.com

What We Are Doing

We take the protection of our customers' information seriously and have worked closely with ABS to ensure that ABS thoroughly investigated the incident and has taken steps to prevent this from happening again. We have been assured that ABS immediately took steps to assess the security of its systems and mitigate the impact of this incident. ABS also reviewed existing security policies and implemented additional measures, including advanced endpoint monitoring, to further protect information entrusted to it.

As an added precaution to help protect your information from potential misuse, ABS is offering complimentary credit monitoring and identity theft restoration services through *my*TrueIdentity provided by TransUnion Interactive, a subsidiary of TransUnion®, at no cost to you. *my*TrueIdentity services include <<CM Length>> months of credit monitoring and alerts, a $1,000,000 insurance reimbursement policy, educational materials, and ID theft recovery services. *my*TrueIdentity will help reduce the risk of identity theft and also help you resolve issues in the event your identity is compromised. *(Please note, the *my*TrueIdentity services are not available to individuals under the age of 18. If you are under the age of 18, please instead refer to the note on the enclosed enrollment sheet pertaining to minors.)

To enroll in *my*TrueIdentity online or by telephone, please refer to the enclosed documentation containing your enrollment instructions and your personal activation code. Please note that you must complete enrollment by <<Enrollment Deadline>>.

What You Can Do

In light of this incident, we recommend that you remain vigilant against potential identity theft and fraud by reviewing and monitoring your account statements and credit reports for suspicious or unauthorized activity. If you find any suspicious or unauthorized activity, you should report it to your financial institutions and/or credit reporting agencies immediately. You also may file a report with law enforcement, your state attorney general, and/or the Federal Trade Commission. In addition, please refer to the enclosed *Recommended Steps to Help Protect Your Information* for additional steps you may take to protect your information from misuse, including some information that may be specific to your state of residence.

For More Information

We are very sorry for any inconvenience this incident has caused or may cause you, and we encourage you to take advantage of the *my*TrueIdentity services being offered. If you have any other questions that you would like to discuss, please contact the dedicated toll-free hotline at 855-914-4705 between 8:00 am and 8:00 pm Central Time, Monday through Friday.

Sincerely,

Frank L Carson IV
President and CEO

Recommended Steps to Help Protect Your Information

Review personal account statements and credit reports. We recommend that you remain vigilant by reviewing personal account statements and monitoring credit reports to detect any errors or unauthorized activity. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call (877) 322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months. If you discover any suspicious items, you should report any incorrect information on your report to the credit reporting agency. The names and contact information for the credit reporting agencies are:

Equifax	Experian	TransUnion
1-866-766-0008	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.equifax.com	www.experian.com	www.transunion.com

Report suspected fraud. You have the right to file a police report if you ever 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 some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You should report suspected incidents of identity theft to local law enforcement, your state's Attorney General, and/or the Federal Trade Commission.

Place Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. When you place a fraud alert, it will last one year. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. For more information, visit https://www.consumer.ftc.gov/articles/0275-place-fraud-alert.

Place a Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too. To place a security freeze, contact the nationwide credit reporting agencies by phone or online. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee. Also, do not confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock. For more information, visit https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs.

Place a security alert on ChexSystems. A security alert with ChexSystems may prevent accounts and services from being approved in your name without your consent. You can complete a security alert with ChexSystems by visiting https://www.chexsystems.com/web/chexsystems/consumerdebit/page/IdentityTheft/securityalert/ or you can call the toll-free number 888.478.6536, and answer the brief set of questions.

Change Online Account Credentials. If the information involved in this incident included credentials used to access any of your online accounts, such as a username, password, PIN, or an answer to a security question, you should to promptly change your username, password, PIN, security question and answer, or other access credentials and take other appropriate steps to protect all online accounts for which you use the same credentials.

Obtain additional information about the steps you can take to avoid identity theft from the following entities:

- **Arizona Residents**: Office of Attorney General, Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004, www.azag.gov/consumer/data-breach, (602)542-5025
- **Colorado Residents:** Office of Attorney General, Consumer Protection Section, 1300 Broadway, 7th Floor, Denver, CO 80203, www.stopfraudcolorado.gov/fraud-center/identity-theft.html
- **District of Columbia Residents:** Office of the Attorney General, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001; (202) 727-3400; and https://oag.dc.gov
- **Florida Residents:** Office of the Attorney General, State of Florida, PL-01 The Capitol, Tallahassee, FL 32399-1050, myfloridalegal.com, (850) 414-3990.
- **Georgia Residents:** Office of the Attorney General, Consumer Protection Division, 2 Martin Luther King Jr. Drive, Suite 356, Atlanta, Georgia 30334-9077, www.consumer.ga.gov, (800) 869-1123
- **Illinois Residents:** Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, www.illinoisattorneygeneral.gov/consumers/hotline.html, (800) 243-0618

- **Louisiana Residents:** Office of the Attorney General, Consumer Protection Section, 1885 North Third Street Baton Rouge, LA 70802, www.ag.state.la.us, (800) 351-4889
- **Maryland Residents:** Office of the Attorney General**,** Consumer Protection Division, 200 St. Paul Place Baltimore, MD 21202**,** www.oag.state.md.us/Consumer, (888) 743-0023.
- **Missouri Residents:** Office of Attorney General, Supreme Court Building, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov/civil-division/consumer/identity-theft-data-security, (573) 751-3321
- **New York Residents:** New York State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave Albany, NY 12231, www.dos.ny.gov/consumerprotection, (800) 697-1220
- **North Carolina Residents:** Office of the Attorney General of North Carolina**,** 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, (919) 716-6400.
- **Pennsylvania Residents:** Pennsylvania Office of Attorney General, Strawberry Square Harrisburg, PA 17120, www.attorneygeneral.gov (717) 787-3391
- **Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903; www.riag.ri.gov; (401) 274-4400. Under Rhode Island law, you have the right to obtain any police report filed about this incident. There are approximately [XX] Rhode Island residents whose information may have been affected by this incident.
- **Texas Residents:** Office of Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov/consumer-protection, (877) 877-9392
- **Virginia Residents:** Office of the Attorney General, Computer Crime Section, 202 North Ninth Street, Richmond, VA 23219, www.oag.state.va.us/CCSWeb2, (804) 786-4718
- **All US Residents:** Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.ftc.gov, 1-877-IDTHEFT (438-4338).

Know 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. You have certain rights under the FCRA, which you can read about by visiting https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf and https://www.consumer.ftc.gov/articles/0070-credit-and-your-consumer-rights. These rights include: (1) You must be told if information in your file has been used against you; (2) You have the right to know what is in your file (your "file disclosure"); (3) You have the right to ask for a credit score; (4) You have the right to dispute incomplete or inaccurate information; (5) Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; (6) Consumer reporting agencies may not report outdated negative information; (7) Access to your file is limited to people with a valid need; (8) You must give your consent for reports to be provided to employers; (8) You may limit "prescreened" offers of credit and insurance you get based on information in your credit report; (9) You may seek damages from violators; and (10) identity theft victims and active duty military personnel have additional rights. For more information, visit www.ftc.gov/credit. States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.

TransUnion

Activation Code: <<Activation Code>>

Enroll in Credit Monitoring

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

How to Enroll: You can sign up online or via U.S. mail delivery

- To enroll in this service, go to the *my*TrueIdentity website at **www.MyTrueIdentity.com** and, in the space referenced as "Enter Activation Code," enter the 12-letter Activation Code **<<Insert Unique 12-letter 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 six-digit telephone passcode **<<Insert static six- digit Telephone Pass Code>>** 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.

You can sign up for the online or offline credit monitoring service anytime between now and **<<Enrollment Deadline>>**. Due to privacy laws, neither we nor ABS can register you directly. Please note that credit monitoring services might not be available for individuals who do not have a credit file with TransUnion or an address in the United States (or its territories) and a valid Social Security number. Enrolling in this service will not affect your credit score.

ADDITIONAL DETAILS REGARDING YOUR COMPLIMENTARY CREDIT MONITORING SERVICE:

- Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and credit score.
- 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, changes of address, and more.
- The service also includes access to an identity restoration program that provides assistance in the event that your identity is compromised and up to $1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

*** Please note, the *my*TrueIdentity services are not available to individuals under the age of 18. If you are under the age of 18, please use TransUnion's secure Child Identity Theft Inquiry Form located at https://www.transunion.com/fraud-victim-resource/child-identity-theft to submit details about your concerns. You can also email childidtheft@transunion.com. Remember, do not email sensitive, identifying or account information.**