GODFREY & KAHN S.C.

833 EAST MICHIGAN STREET • SUITE 1800
MILWAUKEE, WISCONSIN 53202-5615

TEL • 414.273.3500 FAX • 414.273.5198

WWW • GKLAW.COM

Direct: 414-287-9450
ssargent@gklaw.com

November 16, 2021

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
SECURITY BREACH NOTIFICATION
6 State House Station
Augusta, ME 04333

RE: Data Incident Notification

Dear Attorney General Frey:

Our firm represents Horicon Bank ("Horicon"). Horicon hereby formally submits notification of a recent data incident pursuant to Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq. Horicon reserves the right to supplement this notice with any significant details learned subsequent to this submission. By providing this notice, Horicon does not waive any rights or defenses regarding the applicability of Maine law, including the applicability of Maine Rev. Stat. Tit. 10, Section 210-B-1346 et seq., the applicability of any other laws of this or any other state, or the existence of personal jurisdiction over Horicon.

Horicon discovered a security incident on September 20, 2021, involving an unauthorized third party accessing and encrypting some of Horicon's non-core banking systems (the "Incident"). That same day, Horicon retained forensic experts and outside counsel specializing in data security incidents and began investigating. Horicon also promptly notified its financial regulators and federal law enforcement of the Incident. On October 20, 2021, Horicon's investigation confirmed that unauthorized access to and acquisition of personal information, and more specifically, non-public personal information subject to the Gramm-Leach-Bliley Act, occurred during the Incident. In light of the foregoing, and out of an abundance of caution, Horicon has decided to notify your office (via this letter) and the one (1) Maine resident potentially affected by this Incident during the week of November 15, 2021. A sample notification letter to the affected resident is attached hereto as Exhibit A.

It is important to note that Horicon does not have any evidence of misuse of the personal information or any fraud or identity theft.

Horicon takes the security of personal information seriously and has already implemented additional security measures designed to prevent any similar attack in the future, including deploying further end point protection software on our systems, reviewing our security measures, and working with consultants to restore the affected systems. In addition, Horicon has retained Kroll, Inc., a leader in risk mitigation and identify theft services, to provide affected individuals

with identity theft services, and Experian to provide credit monitoring to impacted individuals. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,

GODFREY & KAHN, S.C.

Sarah A. Sargent

SAS

EXHIBIT A

Sample Notification Letter

HORICON BANK
The Natural Choice

<<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>>,

We are writing to notify you, as a precautionary measure, of a recent cybersecurity incident experienced by Horicon Bank, that may have involved some of your nonpublic personal information. Out of an abundance of caution, we are providing details to you about the nature of the incident because Horicon values the security and privacy of your personal information, is committed to ensuring you understand what happened, and wants to provide you with the tools to assist you with securing and protecting your personal information should you have ongoing concerns.

What happened?

On September 20, 2021, Horicon became aware that an unauthorized third party had gained access to and encrypted some of our internal systems. Immediately upon learning of the incident, Horicon retained forensic specialists and counsel, both of whom specialize in data security incidents, and immediately began investigating. On October 20, 2021, Horicon determined that some information on our systems, including your personal information, was accessed and/or acquired by the attacker during the incident. Horicon has been working with third-party forensic investigators to understand the nature and scope of the incident, what information may have been accessed and/or acquired, and who may have been impacted. While Horicon does not have any evidence of misuse of your personal information or any fraud or identity theft, we are nonetheless informing you of this incident because we greatly value our customers and take this matter seriously. This notice was not delayed due to an investigation by law enforcement.

At this time, we have no evidence that there was unauthorized access to your Horicon financial account(s).

What information was involved?

The personal information impacted may include some or all of the following personal information: your name, account number with your then-current account balance, address, phone number, and in some limited instances, transaction information related to past payments. Please note that the exact nature and extent of personal information impacted may vary by individual.

What we are doing.

We have reported this incident to the appropriate law enforcement authorities. In addition to fully investigating this incident and providing notice to you through this letter, we have deployed further end point protection software on our systems, are otherwise reviewing our security measures, and worked with consultants to restore the affected systems.

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorks℠ and have engaged Kroll to assist in answering your questions about this incident. Experian provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **<<b2b_text_6(ActivationDeadline)>>** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: https://www.experianidworks.com/3bcredit
- Provide your **activation code**: **<<Activation Code s_n>>**

If you have questions about the Experian product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 877-288-8057 by **<<b2b_text_6(ActivationDeadline)>>**. Be prepared to provide engagement number **<<b2b_text_1(Engagement#)>>** as proof of eligibility for the identity restoration services by Experian.

A credit card is **not** required for enrollment in Experian IdentityWorks. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please note that this Identity Restoration support is available to you for 12 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

What you can do.

To date, there has been no fraudulent activity on your Horicon financial account. However, if you are concerned about your account or personal information, please refer to the "Additional Resources" section included with this letter for steps you can take to protect your information. It includes 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.

While we trust that the services we are offering to you demonstrate our continued commitment to your security and satisfaction, we also sincerely apologize for any inconvenience and concern this incident may cause you.

If you have questions, please call 1-855-912-1519, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding major U.S. holidays.

Sincerely,

Mark Nelson

Mark Nelson
EVP – CIO/COO
Horicon Bank

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 California Residents: You may also wish to review the information provided by the California Attorney General at https://oag.ca.gov/idtheft.

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 at consumer@ag.iowa.gov, by calling (515) 281-5926, or writing to 1305 E. Walnut Street Des Moines, Iowa 50319-0106.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General at https://doj.state.or.us, by calling (877) 877-9392, or writing to Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096.