



May , 2024

Individual's Name
Address

Dear _____,

We at Icelandic Provisions, Inc. are writing to inform you of a recent security incident that we experienced that may have exposed your personal information. This notice is sent pursuant to M.G.L., Chapter 93H, sec. 3.

What Happened

In late December 2023, Icelandic Provisions learned of a cyberattack against its systems and engaged an outside cybersecurity consultant to investigate the cause and scope of this security incident. After a thorough forensics investigation, Icelandic Provisions learned that the attacker gained access to Icelandic Provisions' systems beginning on or around October 2023 and was active until around January 2024.

Now that the investigation has concluded, Icelandic Provisions has determined that the attacker may have had the ability to access your personal information through a compromised email account. **Your following personal information may have been exposed: Social Security Number, full name, date of birth, and address.** To be clear, there is no evidence that the attacker actually viewed or removed this information from Icelandic Provisions' systems. However, out of an abundance of caution, we are notifying you so that you can take measures to monitor your personal information.

What Are We Doing

Icelandic Provisions has taken steps to fully understand the scope of the security incident and what information may have been accessed. We take the protection of your personal information seriously and are contacting you directly to explain what occurred and the resources available to you.

What You Can Do

Icelandic Provisions is providing you with 18 months of complimentary identity monitoring services through Kroll. To take advantage of these free services, please follow the instructions in Attachment 1.

In addition to using these services, we urge you to remain vigilant to guard against the risk of fraud and identity theft by reviewing your financial account statements, contacting your financial institutions should you discover anything suspicious, and monitoring your free credit reports.

In the event you do not chose to take advantage of these free services through Kroll, you may choose to protect yourself with automatic credit monitoring by placing a fraud alert on your credit files.

- A fraud alert alerts any entity requesting your credit report that you suspect you were a victim of fraud. When you or someone else attempts to open a credit account in your name, the lender should take measures to verify that you have authorized the request.
- To place a fraud alert on your credit reports, contact one of the three major credit reporting agencies at the appropriate number listed below or via their website.

Equifax (888)766-0008 or www.fraudalert.equifax.com

Experian (888) 397-3742 or www.experian.com

TransUnion (800) 680-7289 or www.transunion.com

You may also considering placing a Security Freeze on your credit report. The instructions for placing a Security Freeze on your credit report are included in Attachment 2.

If you believe you have suffered identity theft or would like to obtain a statement about preventing identity theft, please contact the Federal Trade Commission at 1-877-FTC-HELP (1-877-382-4357), through the website www.identitytheft.gov, or at the mailing address 600 Pennsylvania Ave., NW, Washington, DC, 20580.

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

For More Information

If you have any further questions regarding this incident or would like to speak to anyone for further assistance, please contact me at tony.sciortino@icelandic-provisions.com.

Sincerely,

Tony Sciortino

Tony Sciortino
Icelandic Provisions, Inc.
134 West 25th St, 7th Floor
New York, NY 10001-7409

Attachment 1

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for 18 months. 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, Fraud Consultation, and Identity Theft Restoration.

Visit <<IDMonitoringURL>> to activate and take advantage of your identity monitoring services.

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

For more information about Kroll and your Identity Monitoring services, see below or visit info.krollmonitoring.com.



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'll 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.

Attachment 2

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you must send a written request to **each** of the three major consumer reporting agencies: Equifax (www.equifax.com); Experian (www.experian.com); and TransUnion (www.transunion.com) by regular, certified or overnight mail at the addresses below:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
(800) 685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
(888) 397-3742

Trans Union Security Freeze
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000
(888) 909-8872

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five 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, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.