



**Seyfarth Shaw LLP**  
233 South Wacker Drive  
Suite 8000  
Chicago, Illinois 60606-6448  
T (312) 460-5000  
F (312) 460-7000

[www.seyfarth.com](http://www.seyfarth.com)

Attorney General John Formella  
Office of the Attorney General  
NH Department of Justice  
33 Capitol Street  
Concord, NH 03301  
**VIA E-MAIL: [attorneygeneral@doj.nh.gov](mailto:attorneygeneral@doj.nh.gov)**

April 25, 2023

**Re: Notice of Data Incident**

Dear Attorney General Formella:

We represent InfoMart, Inc., (“InfoMart”) whose principal business office is located at 1582 Terrell Mill Rd., Marietta, GA 30067. We are writing to notify you on behalf of our clients of a data security incident involving 20 New Hampshire residents. This notice may be supplemented upon any further investigation. By providing this notice, InfoMart does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the relevant state statute, or personal jurisdiction.

**Background:** Our clients first became aware of a potential data incident involving a threat actor’s unauthorized access to a mailbox on InfoMart’s network on March 22, 2023. After conducting an investigation, InfoMart determined that the threat actor obtained unauthorized access through the use of stolen credentials and had access to the mailbox for a total of 14 hours. In that time, the threat actor used the mailbox to send out several phishing attempts. Upon discovery of the breach, InfoMart took immediate steps to secure its systems by forcing a password reset to a randomized password for affected the user’s account, and forcing a sign out of all active sessions. As part of the investigation, InfoMart identified the intruder’s IP address and login location and checked login activity for all users against those identifiers. No additional suspicious logins were found. On March 28, 2023, InfoMart discovered that 20 New Hampshire residents were affected. The personal information at issue for New Hampshire residents includes

In response to the breach, our clients have instituted a number of remedial measures, including the implementation of multi-factor authentication for all email and Microsoft 365 product access, and the configuration of geo-location filters to the InfoMart environment to prevent logins from any country outside of the United States and Canada. Additionally, InfoMart alerted its IT messaging service provider to the compromise and asked them to increase scrutiny for suspicious email and account login activity.

To further strengthen its security practices, InfoMart directed all employees to reset their passwords, and scheduled security refresher trainings to specifically address password complexity requirements, avoidance of password re-use, anti-phishing procedures, and security reporting procedures.

**Notice to New Hampshire Residents:** We have determined that the number of New Hampshire residents potentially affected by this security incident is 20. Written notice is being provided in substantially the same form the letter attached hereto as **Exhibit A**. InfoMart will begin mailing notice to impacted individuals subsequent to the transmittal of this letter, no later than April 27.

**Other Steps Taken and To Be Taken:** InfoMart is taking action to provide assistance to potentially affected individuals, even though it currently has no evidence of any misuse of or fraudulent activity relating to anyone's personal information as a result of this incident. Our clients are providing individuals whose personal information was potentially affected by this incident with access to credit monitoring services for 24 months through Experian at no cost to the individuals.

Additionally, InfoMart is providing impacted individuals with guidance on how to better protect against identity theft and fraud. These measures include advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Our clients are also providing individuals with information on how to place a fraud alert and security freeze on their credit file, information on protecting against fraud, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

**Contact Information:** Should you have any questions regarding this notification or other aspects of the data security incident, please contact us at

Very truly yours,

SEYFARTH SHAW LLP

Jason Priebe



[Insert Recipient's Name]  
[Insert Address]  
[Insert City, State, Zip]

[Date]

**RE: Notice of Data Breach**

Dear [First Name][Last Name]:

We are writing to notify you about an incident involving your personal information. This letter is to provide you with details of what happened, the measures we have taken in response, and to provide you with details on proactive steps you may consider to help protect your information.

InfoMart is a consumer reporting agency based in Atlanta, Georgia. Our services include pre-employment background checks, among other types of consent-based background checks. Your information is in our system because either your current or potential employer engaged us to conduct a background check within the last 21 months.

**What Happened:** On March 21, 2023, InfoMart Inc. ("InfoMart") discovered one of its user email boxes had been compromised by an unauthorized actor. Upon the discovery of the incident on March 22, 2023, we promptly removed the unauthorized actor's access and secured the mailbox content.

**What Information Was Involved:** Based on our investigation, we determined that messages in the mailbox accessed by the unauthorized actor may have contained some of your personal information, including :

Based on the circumstances of the incident, such as the time period during which the unauthorized actor had access to the mailbox, and our review of the unauthorized actor's activity within the mailbox, we have no reason at this time to conclude there is a likelihood of harm to your privacy or risk of further disclosure of your personal information.

**What You Can Do:** While we have no reason to believe there has been or will be any improper use or disclosure of your personal information, we encourage you to remain vigilant by reviewing your account statements and monitoring credit report information.

You can also obtain information about fraud alerts and security freezes from the FTC and the credit reporting agencies listed below:

1582 Terell Mill Road  
Marietta, GA 30067  
phone 770.984.2727  
fax 770.984.8997





Federal Trade Commission, <https://www.ftc.gov>, 600 Pennsylvania Avenue, NW, Washington, DC 20580 1-877-FTC-HELP

Nationwide Consumer Reporting Companies:

- **Equifax**, <https://www.equifax.com>, Equifax Credit Information Services, LLC, P.O. Box 740241, Atlanta, GA 30374, 1-800-525-6285
- **Experian**, <https://www.experian.com>, Experian National Consumer Assistance Center, P.O. Box 4500, Allen, TX 75013, 1-888-397-3742
- **TransUnion**, <https://www.transunion.com>, TransUnion Consumer Relations, P.O. Box 2000, Chester, PA 19016-2000, 1-800-680-7289

To the extent you desire to freeze your credit report, you must separately place a credit freeze on your credit file at each of the three credit reporting agencies. There is no charge associated with placing a credit freeze. The following information should be included when requesting a credit freeze:

- 1) Full name, with middle initial and any suffixes;
- 2) Social Security number;
- 3) Date of birth (month, day, and year);
- 4) Current address and previous addresses for the past five (5) years;
- 5) Proof of current address, such as a current utility bill or telephone bill;
- 6) Other personal information as required by the applicable credit reporting agency.

**What We Are Doing:** We regret that this incident occurred and take the security of our information very seriously. In addition to conducting a staff-wide training session across a variety of information security topics to minimize the likelihood that an incident like this will happen again, InfoMart has also implemented additional layers of multi-factor and authentication verifications, along with other system monitoring protection.

To help protect your identity, we are also offering complimentary access to Experian IdentityWorks<sup>SM</sup> for 24 months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for 24 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](http://www.ExperianIDWorks.com/restoration).

1582 Terell Mill Road  
Marietta, GA 30067  
phone 770.984.2727  
fax 770.984.8997





While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary 24-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you enroll by **[Enrollment End Date]** (Your code will not work after this date.)
- Visit the Experian IdentityWorks website to enroll: **[Enrollment URL]**
- Provide your activation code: **[Activation Code]**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **[Experian TFN]** by **[Enrollment End Date]**. Be prepared to provide engagement number **#####** as proof of eligibility for the Identity Restoration services by Experian.

#### **ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP**

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 file 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.
- **\$1 Million Identity Theft Insurance\*\*:** Provides coverage for certain costs and unauthorized electronic fund transfers.

**For More Information.** We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call **[Experian TFN]** toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number \_\_\_\_\_.

Sincerely,

Tim Gordon, Chief Compliance Officer

1582 Terell Mill Road  
Marietta, GA 30067  
phone 770.984.2727  
fax 770.984.8997