

Christopher L. Ingram  
Direct Dial (614) 464-5480  
Direct Fax (614) 719-4606  
Email [clingram@vorys.com](mailto:clingram@vorys.com)

December 3rd, 2021

**VIA E-MAIL**

Consumer Protection Bureau  
Office of the New Hampshire Attorney General  
33 Capitol Street  
Concord, NH 03302  
[DOJ-CPB@doj.nh.gov](mailto:DOJ-CPB@doj.nh.gov); [AttorneyGeneral@doj.nh.gov](mailto:AttorneyGeneral@doj.nh.gov)

Dear Office of the New Hampshire Attorney General:

We write to inform you of a recent data security incident involving our client, Reggio Register Company, LLC (“Reggio”), 31 Jytek Rd., Leominster, MA 01453.

On November 4, 2021, Reggio discovered that an unauthorized change had been made to its website. Upon investigation, Reggio learned that the change included code designed to collect information customers had entered on its website’s shopping cart page. The unauthorized code was immediately removed and the matter was reported to law enforcement.

Based on the information currently available, it is Reggio’s understanding that orders placed on its website between November 1, 2021 and November 4, 2021 may have been impacted by the unauthorized code. Reggio has determined that four (4) New Hampshire residents were impacted by this incident. Depending on the information these New Hampshire residents input into the shopping cart page, the unauthorized code may have collected the residents’ names, billing and shipping addresses, phone numbers, email addresses, the credit card or debit card numbers used to place their orders, those cards’ expiration dates, and card verification numbers (CVV2) for those cards. Since Reggio does not request PINs when debit cards are used, PINs were not subject to the collection.

Reggio immediately took steps to strengthen its website’s security. Among other things, Reggio reset certain passwords, enhanced access controls to its servers, and improved its endpoint detection and response security settings. Additionally, Reggio is implementing measures to improve its web application firewall settings to prevent this type of unauthorized activity in the future.

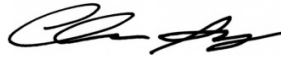
December 3rd, 2021

Page 2

More information regarding this matter is described in an enclosed sample notification letter. The letter will be sent via U.S. postal mail directly to the affected New Hampshire residents on or before December 3rd, 2021.

Please contact us with any questions or concerns.

Very truly yours,

A handwritten signature in black ink, appearing to read "Chris Ingram", written over a light gray rectangular background.

Christopher L. Ingram

CLI/vssp



December 3, 2021

«Name»  
«Street\_Address»  
«City», «State» «Zip»

### **Notice of Data Breach**

Dear «Name»,

We are writing to inform you of a data security incident involving Reggio Register Company, LLC's website. We want to make you aware of what happened, measures that have been taken in response to the incident, and recommended actions you may wish to take to protect your personal information.

#### **What happened?**

On November 4, 2021, we discovered that an unauthorized change had been made to our website. We immediately initiated an investigation and learned that the change included code designed to collect information customers entered on our website's shopping cart page. We immediately removed the unauthorized code and reported the matter to law enforcement. Based on the information currently available, we believe that orders placed by credit or debit cards between November 1, 2021 and November 4, 2021, may have been impacted by the unauthorized code.

#### **What information was involved?**

The unauthorized code was designed to collect information that customers submitted through the shopping cart page when completing an order, which may have included: name, billing and shipping addresses, phone number, email address, the credit card or debit card number used to place the order, the expiration date, and card verification number (CVV2) for that card. Since we do not request PINs when debit cards are used, PINs were not subject to collection. We are providing you with this notice because our records indicate that you placed an order between November 1, 2021 and November 4, 2021 «Last\_4»

#### **What we are doing.**

As soon as we learned of this situation, we immediately launched an investigation and retained a leading computer security firm. We removed the unauthorized code from our website and took steps to strengthen our website's security. Thus far, our investigation has found no evidence of any misuse of personal information or fraudulent activity as a result of this incident.

#### **What you can do.**

Although we do not have any evidence that your information has been misused, we recommend that you regularly review your statements related to the payment card referenced above, to remain vigilant for incidents of fraud on your payment card, and immediately report any suspicious activity to your card provider. Never provide personal information in a response to an electronic communication about a security event. Additionally, we encourage you to review the information provided in the enclosed "Further Information and Steps You Can Take." The enclosure identifies some steps you can take to guard against the misuse of your personal information.

**For more information.**

We sincerely regret and apologize for any inconvenience this may cause you. Please do not hesitate to email [customersecurity@reggio.com](mailto:customersecurity@reggio.com) or call 1-800-880-3090 if you have any questions or concerns.

Sincerely,

A handwritten signature in black ink, appearing to read "Marc Sieger". The signature is fluid and cursive, with the first name "Marc" and last name "Sieger" clearly distinguishable.

Marc Sieger  
CEO

Enclosure: Further Information and Steps You Can Take

## **Further Information and Steps You Can Take**

### **Filing a Police Report for Suspicious Activity**

We encourage you to remain vigilant of identity theft or fraud. You should review your account statements, explanation of benefits, and credit reports and report any suspicious activity or suspected identity theft. If you do find suspicious activity of identity theft or fraud, you should call your local police or sheriff's office and file a police report of identity theft or fraud. You are entitled to a copy of the police report. You may need to give copies of the police report to creditors to clear up your records. In addition, you should report identity theft to your state's Attorney General, to the Federal Trade Commission ("FTC"), and to us. This notice has not been delayed by law enforcement.

### **Obtaining a free credit report or placing a fraud alert or security freeze**

You may obtain a free copy of your credit report from each of the credit bureaus once a year by visiting [www.annualcreditreport.com](http://www.annualcreditreport.com), or calling 877-322-8228. Hearing impaired consumers can access TDD service at 877-730-4104. You may contact the nationwide credit bureaus at:

**Equifax**, 866-349-5191, P.O. Box 740241, Atlanta, GA 30374, [www.equifax.com/FCRA](http://www.equifax.com/FCRA)

**Experian**, 888-397-3742, P.O. Box 9701, Allen, TX 75013, [www.experian.com](http://www.experian.com)

**TransUnion**, 800-916-8800, P.O. Box 2000, Chester, PA 19022, [www.transunion.com](http://www.transunion.com)

You may also place a fraud alert or security freeze on your credit report at no cost. A fraud alert is a notice that can be placed on a consumer's credit report that alerts companies who may extend credit that the consumer may have been a victim of identity theft or fraud. When a fraud alert is displayed on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. There are two types of fraud alerts: an "initial" fraud alert that lasts for one year, and an "extended" fraud alert for victims of identity theft or fraud that lasts seven years. A fraud alert should not affect your ability to get a loan or credit, but it may cause some delay if you are applying for credit. To place a fraud alert, please contact one of the credit reporting agencies at:

**Equifax**, 888-836-6351, P.O. Box 105069, Atlanta, GA 30348, [www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**, 888-397-3742, P.O. Box 9554, Allen, TX 75013, [www.experian.com/fraud/center.html](http://www.experian.com/fraud/center.html)

**TransUnion**, 800-680-7289, P.O. Box 2000, Chester, PA 19016, [www.transunion.com/fraud-alerts](http://www.transunion.com/fraud-alerts)

Alternatively, you may place a security freeze on your file. Security freezes will prevent new credit from being opened in your name without the use of a personal identification number or password that will be issued by the credit reporting agencies after you initiate the freeze. In order to place a security freeze, you may be required to provide the credit reporting agencies with information that identifies you. A security freeze can make it more difficult for someone to get credit in your name, but it also may delay your ability to obtain credit. The credit reporting agencies may not charge a fee to place a freeze or remove a freeze. To place a security freeze, please contact one of the agencies at:

**Equifax**, 888-298-0045, P.O. Box 105788, Atlanta, GA 30348, [www.equifax.com/personal/credit-report-services](http://www.equifax.com/personal/credit-report-services)

**Experian**, 888-397-3742, P.O. Box 9554, Allen, TX 75013, [www.experian.com/freeze/center.html](http://www.experian.com/freeze/center.html)

**TransUnion**, 888-909-8872, P.O. Box 160, Woodlyn, PA 19094, [www.transunion.com/credit-freeze](http://www.transunion.com/credit-freeze)

### **Additional Information**

You may find additional information about fraud alerts, security freezes, and suggestions you can take to protect yourself from identity theft or fraud by contacting the FTC or your state Attorney General.

The FTC provides suggestions for actions you may take in the event of identity theft at [www.identitytheft.gov](http://www.identitytheft.gov). You may also call the FTC for more information at 1-877-ID-THEFT (438-4338) (TTY: 1-866-653-4261), or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

**For California Residents:** Visit the California Office of Privacy Protection at <https://oag.ca.gov/privacy> for additional information on protection against identity theft.

**For Connecticut Residents:** The Attorney General provides information about preventing identity theft at <https://portal.ct.gov/AG/Consumer-Issues/Identity-Theft/Identity-Theft>. You may also contact the Connecticut Attorney General by calling (860) 808-5318 and by mail at 165 Capitol Avenue, Hartford, CT 06106.

**For District of Columbia Residents:** The Attorney General provides information regarding identity theft at [www.oag.dc.gov](http://www.oag.dc.gov). You may also contact the Attorney General for the District of Columbia by calling (202)-727-3400, or by mail at 400 6th Street NW, Suite 1100 South, Washington, D.C. 20001.

**For Maryland Residents:** The Maryland Attorney General provides information regarding identity theft at [www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx](http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx). You may also contact the Identity Theft Unit at (410) 576-6491, by email at [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us), and by mail at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202.

**For New Mexico Residents:** You have rights under the federal Fair Credit Reporting Act (“FCRA”), such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Additionally, consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your credit file is limited; you must give your consent for your credit 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 the right to place a “security freeze” on your credit report, and you may seek damages from a violator of the FCRA. You may have additional rights under the FCRA not summarized here. Identity theft victims and active duty military personnel have specific additional rights under the FCRA. We encourage you to review your rights under the FCRA by visiting [www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf](http://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf), or by writing: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

**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; [www.ag.ny.gov](http://www.ag.ny.gov), or the Bureau of Internet and Technology at 28 Liberty Street, New York, New York 10005, (212) 416-8433, <https://ag.ny.gov/internet/resource-center>.

**For Oregon Residents:** The Oregon Attorney General provides information regarding identity theft at [www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/](http://www.doj.state.or.us/consumer-protection/id-theft-data-breaches/identity-theft/). You may also contact the Attorney General’s Consumer Hotline at 1-877-877-9392, by email at [help@oregonconsumer.gov](mailto:help@oregonconsumer.gov), and by mail at Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096.

**For Rhode Island Residents:** The Rhode Island Attorney General provides information about identity theft at <https://riag.ri.gov/what-we-do/civil-division/public-protection/consumer-protection/id-theft>. You may also contact the Consumer Protection Unit at (401) 274-4400, by email at [consumers@riag.ri.gov](mailto:consumers@riag.ri.gov), or by mail at 150 South Main Street, Providence RI 02903. At this time, we believe one Rhode Island resident was impacted by this incident.