From:
Sent: Thursday, June 15, 2023 10:05 PM
To: DOJ: Attorney General <attorneygeneral@doj.nh.gov>
Subject: notice of data breach affecting John and Kiras Chocolates

---

We are writing to inform you about an incident that occurred on our third-party e-commerce platform, CommerceV3, which may have impacted customer personal data.

CommerceV3 serves as the e-commerce platform we utilize to process payment card information when orders are placed on our website.

CommerceV3 notified us on June 6th that an unauthorized party had gained access to their systems and may have obtained the customer order. As soon as they became aware of this threat, CommerceV3 launched a comprehensive forensic investigation with the assistance of third-party cybersecurity experts. Throughout the investigation, CommerceV3 collaborated closely with major card brands and banks to assess the potential impact on cardholder data.

While the investigation was still ongoing, CommerceV3 implemented a series of additional security measures to protect customer information, including upgrades on johnandkiras.com and other stores that change how payment card data is processed when orders are placed online. The investigation has since confirmed that the threat has been eliminated, and they have also identified which customer information could have been affected as well as a date range when the information may have been accessed.

CommerceV3 has implemented additional security measures designed to protect the privacy of its valued customers. CommerceV3 analyzed the attack method used in the skimmer attack and modified the OSSEC service accordingly. This modification enables the service to monitor and block similar attacks effectively. Secondly, CommerceV3 has enhanced the monitoring and refreshing process of the affected service. This ensures that any similar attacks are detected, and if the OSSEC system fails, it will generate a report. To further strengthen security, CommerceV3 implemented an ICC upgrade that not only isolates data skimming capabilities but also provides tighter monitoring of any attempted data exfiltration from the networks. Lastly, CommerceV3 is in the process of transitioning all merchants to a fully tokenized infrastructure. This infrastructure eliminates PAN data from all networks, thereby significantly enhancing security measures.

Following their forensic investigation, CommerceV3 concluded on May 3, 2023, that there is a possibility that cardholder data collected on behalf of John & Kira's was accessed or acquired by the unauthorized party between November 24, 2021, and July 1, 2022. We were notified of customer names on June 12, 2023, and provided with a list of customers whose information may be involved, which is why we are contacting you now.

Personal information, including

.

The total number of customers affected was 9,328, with 72 being in the State of New Hampshire.

We are notifying them by electronic notice on June 19th, 2023, a sample copy of the notice attached

Thank you.

Christopher dal Piaz

Owner

John and Kira's

Subject: Important Notification Regarding Your Personal Information

June 15, 2023

Dear Valued Customer,

At John & Kira's, the privacy and security of your personal information is our utmost priority, rivaled only by our commitment to providing you with the highest quality chocolate. We deeply value the trust you place in us and want to inform you about an incident that occurred on our third-party e-commerce platform, CommerceV3, which may have impacted your personal data.

We are reaching out to provide you with information about what happened, what CommerceV3 has been doing to investigate the problem and eliminate the threat, and what steps you can take now to minimize any risks you may face if your personal information was among the affected data.

Why Does CommerceV3 Have My Information?

CommerceV3 serves as the e-commerce platform we utilize to process payment card information when orders are placed on our website. Your information was shared with CommerceV3 for this purpose.

What Happened?

CommerceV3 recently notified us to indicate that an unauthorized party had gained access to their systems and may have obtained the customer order information they process for stores like ours. As soon as they became aware of this threat, CommerceV3 launched a comprehensive forensic investigation with the assistance of third-party cybersecurity experts. Throughout the investigation, CommerceV3 collaborated closely with major card brands and banks to assess the potential impact on cardholder data.

While the investigation was still ongoing, CommerceV3 implemented a series of additional security measures to protect customer information, including upgrades on johnandkiras.com and other stores that change how payment card data is processed when orders are placed online. The investigation has since confirmed that the threat has been eliminated, and they have also identified which customer information could have been affected as well as a date range when the information may have been accessed.

How does this impact my Information and John & Kira's?

Following their forensic investigation, CommerceV3 concluded on May 3, 2023 that there is a possibility that cardholder data collected on behalf of John & Kira's was accessed or acquired by the unauthorized party between November 24, 2021, and July 1, 2022. We were notified of this on June 12, 2023 and provided with a list of customers whose information may be involved, which is why we are contacting you now. We are also reporting this incident as a data breach to various state and regulatory agencies across the country, as required by law.

What Personal Information Was Involved?

We regret to inform you that your personal information, including

. John & Kira's does not save or store any payment card information for orders placed through our website, but this information may have been intercepted by the attackers directly from CommerceV3 when the payment information was processed online, for orders placed between November 24, 2021, and July 1, 2022.

What You Can Do Now:

There are several measures you can take now to protect against misuse of your personal information. We encourage you to review your credit card statements and bank accounts for any suspicious transactions or unauthorized activity. If you do not regularly do so, you can obtain a free credit report from any of the major credit reporting bureaus to review for irregular or fraudulent activity. If you identify any such activity, please notify your financial institution immediately.

As an additional layer of security, you may also place a Fraud Alert and Security Freeze on your credit files. While many are familiar with the usual risks of unauthorized charges associated with stolen payment card information, online attackers can also use personal contact information from a data breach to target "phishing" scams. Be cautious of unsolicited emails, phone calls, or messages that may attempt to gather further personal or financial information from you. Do not click on suspicious links or provide sensitive details unless you are certain of the source's authenticity.

For More Information:

We are grateful for your past business and hope we can earn your continued trust and support in the future. We were extremely distressed to learn that our website was affected by the incident at CommerceV3, and we are incredibly sorry to be notifying you now that your personal information may have been accessed as a result.

We sincerely appreciate your patience and understanding as we continue to work alongside CommerceV3 to prioritize the security and privacy of your personal information, and we remain committed to protecting that information and delivering the highest standards of security.

If you have any further questions or concerns regarding this incident, please do not hesitate to contact us at

Sincerely,

Sarah Miller
Customer Service Admin
John & Kira's Chocolates

OTHER IMPORTANT INFORMATION

1. Placing a Fraud Alert on Your Credit File.

You may place an initial one-year "fraud alert" on your credit files, at no charge. A fraud alert tells creditors to contact you personally before they open any new accounts. To place a fraud alert, call any one of the three major credit bureaus at the numbers listed below. As soon as one credit bureau confirms your fraud alert, they will notify the others.

Equifax
P.O. Box 105069
Atlanta, GA 30348-5069
https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
(800) 525-6285

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

TransUnion
Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016-2000
https://www.transunion.com/fraud-alerts
(800) 680-7289

2. Placing a Security Freeze on Your Credit File.

If you are very concerned about becoming a victim of fraud or identity theft, you may request a "security freeze" be placed on your credit file, at no charge. A security freeze prohibits, with certain specific exceptions, the consumer reporting agencies from releasing your credit report or any information from it without your express authorization. You may place a security freeze on your credit report by contacting all three nationwide credit reporting companies at the numbers below and following the stated directions or by sending a request in writing, by mail, to all three credit reporting companies:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348
https://www.equifax.com/personal/credit-report-services/credit-freeze/
(800) 349-9960
(888) 298-0045

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
http://experian.com/freeze
(888) 397-3742

TransUnion Security Freeze
P.O. Box 160
Woodlyn, PA 19094
https://www.transunion.com/credit-freeze
(888) 909-8872

In order to place the security freeze, you'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

3. Obtaining a Free Credit Report.

Under federal law, you are entitled to one free credit report every 12 months from each of the above three major nationwide credit reporting companies. Call **1-877-322-8228** or request your free credit reports online at **www.annualcreditreport.com**. Once you receive your credit reports, review them for discrepancies. Identify any accounts you did not open or inquiries from creditors that you did not authorize. Verify all information is correct. If you have questions or notice incorrect information, contact the credit reporting company.

4. Additional Helpful Resources.

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Checking your credit report periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency and file a police report. Be sure to obtain a copy of the police report, as

many creditors will want the information it contains to absolve you of the fraudulent debts. You may also file a complaint with the FTC by contacting them on the web at www.ftc.gov/idtheft, by phone at 1-877-IDTHEFT (1-877-438-4338), or by mail at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for their investigations. In addition, you may obtain information from the FTC about fraud alerts and security freezes.

If this notice letter states that your financial account information and/or credit or debit card information was impacted, we recommend that you contact your financial institution to inquire about steps to take to protect your account, including whether you should close your account or obtain a new account number.

If your personal information has been used to file a false tax return, to open an account or to attempt to open an account in your name or to commit fraud or other crimes against you, you may file a police report in the city in which you currently reside.

Iowa Residents: You may contact law enforcement or the Iowa Attorney General's Office to report suspected incidents of identity Theft: Office of the Attorney General of Iowa, Consumer Protection Division, Hoover State Office Building, 1305 East Walnut Street, Des Moines, IA 50319, www.iowaattorneygeneral.gov, Telephone: 515-281-5164.

Maryland Residents: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office: Office of the Attorney General of Maryland, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 888-743-0023.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain a police report 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.

New York Residents: You may obtain information about preventing identity theft from the New York Attorney General's Office: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; https://ag.ny.gov/consumer-frauds-bureau/identity-theft; Telephone: 800-771-7755.

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office: Office of the Attorney General of North Carolina, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov/, Telephone: 877-566-7226 (Toll-free within North Carolina), 919-716-6000.

Oregon Residents: You may obtain information about preventing identity theft from the Oregon Attorney General's Office: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Washington D.C. Residents: You may obtain information about preventing identity theft from the Office of the Attorney General for the District of Columbia, 400 6th Street NW, Washington D.C. 20001, https://oag.dc.gov/consumer-protection, Telephone: 202-442-9828.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

In Addition, New Mexico Consumers Have the Right to Obtain a Security Freeze or Submit a Declaration of Removal

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, you will be provided with a personal identification number, password, or similar device to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report to a specific party or parties or for a specific period of time after the freeze is in place. To remove the freeze or to provide authorization for the temporary release of your credit report, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number, password, or similar device provided by the consumer reporting agency;
2. Proper identification to verify your identity; and
3. Information regarding the third party or parties who are to receive the credit report or the period of time for which the credit report may be released to users of the credit report.

A consumer reporting agency that receives a request from a consumer to lift temporarily a freeze on a credit report shall comply with the request no later than three business days after receiving the request. As of September 1, 2008, a consumer reporting agency shall comply with the request within fifteen minutes of receiving the request by a secure electronic method or by telephone.

A security freeze does not apply in all circumstances, such as where you have an existing account relationship and a copy of your credit report is requested by your existing creditor or its agents for certain types of account review, collection, fraud control, or similar activities; for use in setting or adjusting an insurance rate or claim or insurance underwriting; for certain governmental purposes; and for purposes of prescreening as defined in the federal Fair Credit Reporting Act.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze, either completely if you are shopping around or specifically for a certain creditor, with enough advance notice before you apply for new credit for the lifting to take effect. You should contact a consumer reporting agency and request it to lift the freeze at least three business days before applying. As of September 1, 2008, if you contact a consumer reporting agency by a secure electronic method or by telephone, the consumer reporting agency should lift the freeze within fifteen minutes. You have a right to bring a civil action against a consumer reporting agency that violates your rights under the Fair Credit Reporting and Identity Security Act.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. You may contact these agencies using the contact information provided above.

Rhode Island Residents: You may contact law enforcement, such as the Rhode Island Attorney General's Office, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. You can contact the Rhode Island Attorney General at: Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 401-274-4400.

As noted above, you may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You have a right to place a "security freeze" on your credit report pursuant to chapter 48 of title 6 of the Identity Theft Prevention Act of 2006.

The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. When you place a security freeze on your credit report, within five (5) business days you will be provided a personal identification number or password to use if you choose to remove the freeze on your credit report or to temporarily authorize the release of your credit report for a specific period of time after the freeze is in place. To provide that authorization, you must contact the consumer reporting agency and provide all of the following:

1. The unique personal identification number or password provided by the consumer reporting agency.
2. Proper identification to verify your identity.
3. The proper information regarding the period of time for which the report shall be available to users of the credit report.

A consumer reporting agency that receives a request from a consumer to temporarily lift a freeze on a credit report shall comply with the request no later than three (3) business days after receiving the request.

A security freeze does not apply to circumstances where you have an existing account relationship and a copy of your report is requested by your existing creditor or its agents or affiliates for certain types of an account review, collection, fraud control, or similar activities.

If you are actively seeking a new credit, loan, utility, telephone, or insurance account, you should understand that the procedures involved in lifting a security freeze may slow your own applications for credit. You should plan ahead and lift a freeze -- either completely, if you are shopping around, or specifically for a certain creditor -- with enough advance notice before you apply for new credit for the lifting to take effect.

You have a right to bring a civil action against someone who violates your rights under the credit reporting laws. The action can be brought against a consumer reporting agency or a user of your credit report.

To place a security freeze on your credit report, you must send a request to each of the three major consumer reporting agencies: Equifax, Experian, and TransUnion. These agencies can be contacted using the contact information provided above.

In order to request a security freeze, you may 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. Complete address;
5. Prior addresses;
6. Proof(s) of identification (state driver's license or ID card, military identification, birth certificate, etc.);
7. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

There were 48 Rhode Island residents impacted by this incident.