Fisher Broyles

January 12, 2023

Via First Class Mail

Attorney General John Formella
Office of the Attorney General
33 Capitol Street
Concord, NH 03302

Re: Data Security Incident

Dear Attorney General Formella:

FisherBroyles, LLP represents CORE Cashless ("CORE"), located at 9111 Barton St., Overland Park, KS 66214, with respect to a data security incident initially noticed to your office on September 13, 2022. CORE is a third-party agent of its merchant clients whose customers' personally identifiable information ("PII") was potentially compromised as a result of the incident. CORE requested that its potentially impacted clients provide information as to its online web portal customers for notification purposes. Please see the attached list of the CORE clients who provided this information and whose customers this notification is based upon (see **Exhibit A**). CORE takes the security and privacy of its clients' customer information seriously and has taken steps to prevent a similar incident from occurring in the future.

1. Description of the Incident.

Based in Overland Park, Kansas, CORE provides private debit card, payments and loyalty/membership systems for the entertainment industry, including amusement parks, waterparks, family entertainment facilities, arcades, events and attractions. On or about July 28, 2022, CORE was notified by the Secret Service that it had identified payment card numbers for sale on the dark web that had a common purchase point with CORE. Upon notice from the Secret Service, CORE immediately conducted an internal investigation of the incident and has since engaged third-party experts to conduct a forensic investigation to determine what occurred and what information was potentially impacted. Based upon the results of the forensic investigation, it is believed that on or about January 29, 2022, a SQL injection was used by an unauthorized individual ("threat actor") to activate a previously deactivated administrator user account and change the password. This permitted the threat actor to install backdoor access tools and implement "skimmers" that captured text inputted into online web payment portals of certain CORE clients. The potentially compromised data elements may include card holder names, billing addresses, email addresses, phone numbers and payment card data.

We note that despite the threat actor capturing such information, CORE does not collect, store or otherwise maintain customer data inputted into its clients' web portals but acts as a "passthrough" service. As such, CORE requested that its potentially impacted clients provide information as to its online web portal customers for notification purposes. Please see **Exhibit A**, containing a list of the CORE clients who provided this information to CORE and whose customers this notification is based upon.

2. Number of New Hampshire residents affected.

Based upon the information provided to CORE by its impacted customers, CORE discovered that the incident may have resulted in the unauthorized exposure of information pertaining to twenty-one (21) New Hampshire residents. Notification letters to these individuals were issued between December 2, 2022 and January 6, 2023. Sample copies of the notification letters are attached as **Exhibit B**.

3. Steps taken.

Upon understanding the scope of the incident, CORE took steps to secure its environment and the incident was contained on or before July 31, 2022. CORE is committed to ensuring the security of all information in its control and is taking steps to prevent a similar event from occurring in the future, including strengthening its security posture. Additionally, all notified New Hampshire residents were offered complimentary identity theft and credit monitoring services for twelve (12) months.

4. Contact information.

CORE remains dedicated to protecting the sensitive information of its clients' customers. If you have any questions or need additional information, please do not hesitate to contact me at

Very truly yours,

Richard Reiter, Partner

FisherBroyles, LLP

CORE Cashless, LLC

<<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 Incident

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

CORE Cashless, LLC recently experienced a data security incident which may have affected your personal information. We take the protection and proper use of your information seriously, and sincerely apologize for any inconvenience this incident may cause. This letter contains additional information about the incident, our response to this incident, and steps you can take to help safeguard your information.

What Happened

On or about July 28, 2022, CORE Cashless, LLC became aware of a compromise to its environment, which may have resulted in the inadvertent exposure of sensitive information of individuals who processed their payment card through the websites of certain CORE Cashless, LLC's clients, including <<b2b_text_1 (impacted merchant)>>. We have since worked diligently to determine what happened and what information was involved as a result of this incident.

What Information Was Involved

A forensic investigation determined that an unauthorized individual gained access to CORE Cashless, LLC's environment on January 29, 2022, which may have permitted the unauthorized individual to access information inputted into certain online payment portals, included that of <<b2b_text_1 (impacted merchant)>>, between February 2, 2022 and July 30, 2022. The elements of your personal information that may have been compromised included, and potentially were not limited to your: name, address, and payment card information.

What We Are Doing

We are working with cybersecurity counsel to determine the actions to take in response to the incident. Together, we continue to investigate and closely monitor the situation. Further, we are taking steps to strengthen our security posture to prevent a similar event from occurring again in the future.

In addition, we are providing you with access to identity monitoring services at no charge for 12 months (please find instructions below).

What You Can Do

Out of an abundance of caution, we have arranged for you to activate, at no cost to you, identity monitoring service for 12 months provided by Kroll. 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 credit and identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

How to Activate:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until <<b2b_text_6 (activation date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com.

Additional information describing your services is included with this letter. Activating this service will not affect your credit score.

We encourage you to remain vigilant, monitor your accounts, and immediately report any suspicious activity or suspected misuse of your personal information. We also recommend that you review the following page, which contains important additional information about steps you can take to help safeguard your personal information, such as the implementation of fraud alerts and security freezes.

For More Information

Please know that the protection of your personal information is a top priority, and we sincerely apologize for any concern or inconvenience that this matter may cause you. If you have any questions, please do not hesitate to call <<TFN>>, Monday – Friday, 8:00am to 5:30pm Central Time, excluding U.S. holidays.

Sincerely,

CORE Cashless, LLC

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, North Carolina, Vermont, Virginia, and Wyoming*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon, and West Virginia*: It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *New Mexico*: Individuals interacting with credit reporting agencies have rights under the Fair Credit Reporting Act. We encourage you to review your rights under the Fair Credit Reporting Act by visiting https://files.consumerfinance.gov/f/documents/bcfp_consumer-rights-summary_2018-09.pdf, or by requesting information in writing from the Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

For residents of *Vermont*: If you do not have internet access but would like to learn more about how to place a security freeze on your credit report, contact the Vermont Attorney General's Office at 802-656-3183 (800-649-2424 toll free in Vermont only).

For residents of *Washington D.C.*: You can obtain information about steps to take to avoid identity theft from the Office of the Attorney General for the District of Columbia at: 441 4th Street, NW, Washington, DC 20001; 202-727-3400; www.oag.dc.gov.

For residents of *Iowa*: State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*: State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Maryland, Rhode Island, Illinois, New York, and North Carolina: You can obtain information from the Maryland and North Carolina Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection, 150 South Main Street, Providence, RI 02903 1-401-274-4400 www.riag.ri.gov

North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com

Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft

New York Office of Attorney General Consumer Frauds & Protection, The Capitol, Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf); TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. 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 need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, 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 five 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, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion Security Freeze**
P.O. Box 105788	P.O. Box 9554	P.O. Box 160
Atlanta, GA 30348 equifax.com/personal/credit-report-services/	Allen, TX 75013 experian.com/freeze/center.html	Woodlyn, PA 19094 transunion.com/credit-freeze
1-800-349-9960	1-888-397-3742	1-888-909-8872

More information can also be obtained by contacting the Federal Trade Commission listed above.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

Please note that to activate monitoring services, you may be required to provide your name, date of birth, and Social Security number through Kroll's automated system. The services to be provided by Kroll include:

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.