Lindsay Nickle, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, TX 75270
LNickle@constangy.com
Mobile: 806.535.0274
Emergency:
BreachResponse@constangy.com
Hotline: 877-382-2724 (877-DTA-BRCH)

August 25, 2023

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey

Constangy, Brooks, Smith and Prophete LLP ("Constangy") represents SERRV International ("SERRV") in connection with a data security incident described in greater detail below. SERRV is a fair trade 501(c)(3) nonprofit with an online marketplace hosted by CommerceV3, an e-commerce platform which also processes payment card information on behalf of SERRV.

1. **Nature of Incident**

CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021 and December 14, 2022. Immediately upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to determine whether any cardholder data was compromised as a result of the incident. CommerceV3 also worked alongside the major card brands and banks during this investigation. On July 17, 2023, CommerceV3 notified SERRV that it had identified potentially impacted SERRV customers.

The potentially impacted information may have included customer names, email addresses, billing addresses, payment card number, payment card expiration date, and security code.

2. **Number of Maine residents affected**

SERRV notified 157 Maine residents of the incident via first class U.S. mail on August 25, 2023. A sample copy of the notification letter is included with this correspondence.

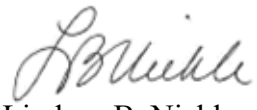
3. Steps taken relating to the incident

SERRV has received information from CommerceV3 that it has implemented additional security measures designed to protect the privacy of its customers. SERRV has also provided customers with information about steps they can take to help protect their personal information.

4. Contact information

SERRV takes the privacy and security of all information in its possession very seriously. If you have any questions or need additional information, please do not hesitate to contact me at 806.535.0274 or LNickle@constangy.com.

Sincerely yours,



Lindsay B. Nickle of
CONSTANGY, BROOKS, SMITH & PROPHETE LLP

Encl.: Sample Consumer Notification Letter

Return Mail to IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

August 25, 2023

Re: Notice of Data <<Variable Text: Breach or Security Incident>>

Dear <<FIRST NAME>> <<LAST NAME>>:

SERRV International ("SERRV") is writing to notify you of a data security incident that impacted our third-party e-commerce platform, CommerceV3, that may have involved your personal information, including your payment card information. SERRV takes the privacy and security of all information in its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

Who are SERRV and CommerceV3? SERRV is a fair trade 501(c)3 nonprofit with an online marketplace at https://serrv.org/ which provides a platform for empowering small-scale global artisans and farmers to sell their goods across the world. SERRV's online marketplace is hosted with CommerceV3, an e-commerce platform, who processes payment card information on behalf of SERRV when customers order through the website.

What Happened? CommerceV3 learned that an unauthorized party obtained access to its systems between November 24, 2021 and December 14, 2022. Immediately upon learning of this issue, CommerceV3 conducted a thorough forensic investigation alongside third-party cybersecurity experts to determine whether any cardholder data was compromised as a result of the incident. CommerceV3 also worked alongside the major card brands and banks during this investigation. On July 17, 2023, CommerceV3 notified SERRV that it had identified potentially impacted SERRV customers.

What Information was Involved? The potentially impacted information may include your name, email address, billing address, payment card number, and payment card expiration date and security code. The affected payment card is a <<CARDTYPE>> ending in <<LAST4>>.

What Are We Doing? We are providing you with this notification and information about steps you can take to help protect your personal information. In addition, SERRV has been told that CommerceV3 has implemented additional security measures designed to protect the privacy of its customers.

What You Can Do: You can follow the recommendations provided on the following page to help protect your personal information. SERRV also recommends that you review your current and past credit and debit card account statements for discrepancies or unusual activity. If you see anything that you do not understand or that looks suspicious, or if you suspect that any fraudulent transactions have taken place, you should call the bank that issued the credit or debit card immediately.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call IDX at 1-888-464-0015 from 9:00 A.M. to 9:00 P.M. Eastern Time, Monday through Friday (excluding holidays). Call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that SERRV takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

Kathleen Gscheidle Penn
Director of IT & Operations
SERRV International

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting https://www.annualcreditreport.com, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax
P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian
P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion
P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at https://www.annualcreditreport.com.

Put a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)
600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General
200 St. Paul Place
Baltimore, MD 21202
marylandattorneygeneral.gov
1-888-743-0023

New York Attorney General
Bureau of Internet and Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General
150 South Main Street
Providence, RI 02903
http://www.riag.ri.gov
1-401-274-4400

Washington D.C. Attorney General
441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.