manatt
manatt | phelps | phillips

Donna L. Wilson
Manatt, Phelps & Phillips, LLP
Direct Dial: (310) 312-4144
E-mail: DLWilson@manatt.com

October 25, 2018

Client-Matter: 48414-035

BY E-MAIL

Washington State Office of the Attorney General
securitybreach@atg.wa.gov

To the Office of the Attorney General:

We are writing to notify you that as a result of potential access by an unauthorized third party, the personal information of 2,384 customers of GS1 US, Inc. ("GS1 US") with addresses in Washington may have been accessed. We want to stress that these customers are business entities and not individuals, but we have decided to notify them out of an abundance of caution in the event that any personal information may have been associated with the online transactions.

While GS1 US's system does not store payment card information, the unauthorized third party may nonetheless have been able to access and acquire the information used to pay for purchases in GS1 US's online store. The potential incident was limited to the time period between approximately July 7, 2017 and October 2, 2018, and discovered on October 1, 2018.

The personal information that was involved in the incident may have included first and last name, company name, address, phone number, email address, and payment card information including account number, expiration date, and three-digit security code. Customers are receiving notifications only because they processed or attempted to process a payment card transaction during the potentially exposed time period; we cannot confirm that any individual customer's information was in fact involved in the potential incident. Notification was not delayed due to law enforcement investigation, and credit monitoring or identity theft protection services have not been offered.

GS1 US takes this matter very seriously and apologizes for any inconvenience caused. Upon learning of the incident, GS1 US took immediate measures to contain and neutralize the vulnerability and immediately began a forensic investigation to determine the extent of the third party criminal conduct. GS1 US has also deployed, and will continue to deploy, additional security procedures to prevent future attacks.

We have attached an anonymized draft of the notice letter to be sent by mail on October 25, 2018 to the Washington business entities that may have had personal information compromised as a result of this incident.

Best regards,

Donna L. Wilson
Brandon P. Reilly
Counsel for GS1 US, Inc.

cc: GS1 US, Inc.

Enclosure

GS1 US
Processing Center ● P.O. BOX 141578 ● Austin, TX 78714

00001
R829503

JOHN
1234 MAIN STREET
ANYTOWN US 12345-6789

October 25, 2018

NOTICE OF DATA BREACH

Dear John:

We are writing to notify you that as a result of the potential access by an unauthorized third party, your personal information may have been compromised. We are providing this notice out of an abundance of caution and to inform you of steps you can take to help protect your company and any other individuals whose information may be involved. You may have received another letter from 1WorldSync. Please note that both letters arise from the same or similar string of events.

What Happened

Specifically, we have learned that an unauthorized third party may have obtained access to your personal information. While our system does not store payment card information, the unauthorized third party may nonetheless have been able to access and acquire the information used to pay for purchases in our online store. The potential incident was limited to the time period between approximately July 7, 2017 and October 2, 2018, and was discovered on October 1, 2018. This notification was not delayed as a result of a law enforcement investigation.

What Information Was Involved

The personal information that was involved in the incident may have included first and last name, company name, address, phone number, email address, and payment card information including account number, expiration date, and three-digit security code. Please note that you are receiving this notification only because your business processed or attempted to process a payment card transaction during the potentially exposed time period; we cannot confirm your information was in fact involved in the potential incident.

Please also note that, in the event an individual used her or his personal credit card, rather than a corporate card, to make purchases from our online store on behalf of your company during the period above, it is possible that his or her personal information may be compromised and that individual should be notified. If a personal card was used to make the purchase in our store on your company's behalf, please let us know.

What We Are Doing

We take this matter very seriously and apologize for any inconvenience caused. Upon learning of the incident, we took immediate measures to contain and neutralize the vulnerability and immediately began a forensic investigation to determine the extent of the third party criminal conduct. We have also deployed, and will continue to deploy, additional security procedures to prevent future attacks.

What You Can Do

There are certain other steps you can take to protect against potential fraudulent activity. You are entitled to obtain a copy of your credit report, free of charge. A credit report contains information about your credit history and the status of your credit accounts. Your credit report could alert you to fraudulent activity being carried on in your name by an identity thief. Please remain vigilant for incidents of fraud and identity theft by reviewing all of your account statements and monitoring your free credit reports by contacting any one of the national consumer reporting agencies set forth below.

The agencies can also provide you with information on how to place a fraud alert or security freeze on your account. A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing, or other services. If you have been the victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to $5.00 each to place, temporarily lift, or permanently remove a security freeze. In order to request a security freeze, you will need to provide the following information: Full name, Social Security number, date of birth, addresses of residence for the past five years, proof of current address, legible photocopy of a government-issued identification card, copy of police report or other law enforcement complaint or report (if the victim of identity theft), and payment by check, money order, or credit card (if not a victim of identity theft). You can obtain information from the following agencies about fraud alerts and security freezes.

Equifax	**Experian**	**TransUnion**	**Federal Trade Commission**
P.O. Box 740241	P.O. Box 4500	P.O. Box 2000	600 Pennsylvania Ave. NW
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016-2000	Washington, D.C. 20580
1-888-766-0008	1-888-397-3742	1-888-909-8872	202-326-2222
www.equifax.com	www.experian.com	www.transunion.com	www.ftc.gov

For More Information

We have established a confidential assistance line so you can contact us should you have any questions regarding the incident or the contents of this letter. This confidential assistance line is staffed with professionals familiar with the incident and is operational Monday through Saturday, 8:00 a.m. to 8:00 p.m. Central Time. Please call, toll-free, 1-855-865-6900.

Other Important Information

RESIDENTS OF IOWA: State law advises you to report any suspected incidents of identity theft to local law enforcement or the attorney general.

RESIDENTS OF MARYLAND: You can obtain information from the Federal Trade Commission and the Office of the Attorney General about steps you can take to avoid 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

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
202-326-2222
www.ftc.gov

RESIDENTS OF NEW MEXICO: You have rights pursuant to the Fair Credit Reporting Act in order to ensure the accuracy, fairness, and privacy of the information contained in your credit report.

RESIDENTS OF NORTH CAROLINA: You can obtain information from the North Carolina Office of the Attorney General and the Federal Trade Commission about preventing identity theft.

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

Federal Trade Commission
600 Pennsylvania Ave. NW
Washington, D.C. 20580
202-326-2222
www.ftc.gov

RESIDENTS OF OREGON: State law advises you to report any suspected identity theft to law enforcement, including the Attorney General and the Federal Trade Commission.

RESIDENCE OF RHODE ISLAND: State law advises you that the state Attorney General can be contacted at:

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

We remain committed to protecting your personal information. We again sincerely apologize for any inconvenience caused by this incident. We are undertaking measures to further secure your personal information, and are continuously monitoring our processes to prevent similar incidents in the future.

Sincerely,

GS1 US, Inc.