DLA Piper LLP (US)
401 B Street
Suite 1700
San Diego, California 92101-1147

Justine Phillips
(619) 699-2795
Justine.Phillips@us.dlapiper.com

September 28, 2022

VIA U.S. MAIL

OCT 03 2022

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

Dear Attorney General Formelia:

We are writing on behalf of Swissport North America, Inc. ("Swissport") pursuant to N.H. RSA § 359-C:20, regarding an incident involving 1 New Hampshire resident.

On February 3, 2022, Swissport detected suspicious activity that resulted in the encryption of several Swissport networks and servers (the "Incident"). The internal security team worked diligently to quickly take affected servers offline, reset account credentials, and deploy additional network monitoring solutions. Upon discovery, Swissport immediately launched a comprehensive investigation with the assistance of cybersecurity experts and engaged appropriate law enforcement authorities.

Swissport's in-depth investigation of the Incident determined that an unauthorized user gained access to certain systems between February 1 through February 3, 2022, that resulted in the encryption of several Swissport networks and servers. With the assistance of cybersecurity experts and out of an abundance of caution, affected servers were immediately taken offline and analyzed. Swissport worked diligently to recover and restore the impacted data accessed by the unauthorized user so it could analyze its contents and identify any affected individuals. During Swissport's comprehensive investigation of the Incident, Swissport identified impacted data originating from three Swissport employee email accounts. On August 26, 2022, the results of the final data mining report were made available and revealed that individuals in New Hampshire were impacted.

The information affected varies by individual but includes one or more of the following types of personal information: Name, Social Security Number, Driver's License Number, Passport Number, financial account/payment card account number, and medical or health insurance information. The notification letter sent to impacted New Hampshire residents will identify the specific data elements impacted for each individual receiving notice.

The monitoring and security systems Swissport had in place enabled it to quickly identify and respond to the Incident. Since this Incident, Swissport has implemented additional security technologies and processes to bolster overall security and harden Internet-facing systems, strengthen its multi-factor authentication process, enhance email security, and block suspicious Internet traffic. Swissport continues to monitor the Internet for potential misuses of New Hampshire residents' data, and there is no indication to suggest the impacted data is being misused. Swissport has also engaged and continues to work with law enforcement agencies on their investigation of this Incident.

On September 29, 2022, Swissport will mail notice to the affected New Hampshire residents, offering a 12-month subscription for credit monitoring and identity protection through Experian IdentityWorks. Affected residents may enroll in the services at no cost by using a promotional code and instructions provided to them in the notification letter.

A sample notification letter is enclosed.

Should you have any questions regarding this matter or if we can be of any further assistance to the New Hampshire residents affected by this Incident, please contact me at (619) 699-2795 or Justine.Phillips@us.dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

Justine Phillips
Counsel for Swissport North America, Inc.

Enclosure: Sample Notification Letter

swissport

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

September 29, 2022

i3555-L01-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L01
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

Notice of Data Breach

Dear Sample A. Sample:

Swissport North America, Inc. ("Swissport") is writing to inform you of an event that may impact the privacy of some of your personal information. While we are unaware of any attempted or actual misuse of your information, we are providing you with information about the event, our response, and information related to what you may do to better protect your information, should you feel it necessary to do so. Swissport takes this incident and the security of your personal information very seriously and we sincerely regret any inconvenience this incident may cause.

What Happened? On February 3, 2022, Swissport became aware of suspicious activity related to its systems and immediately launched a comprehensive investigation with the assistance of cybersecurity experts to determine the nature and scope of the activity. Swissport also engaged with law enforcement. At the same time, we took proactive measures to remove the unauthorized individual and ensure the security of our systems.

Our in-depth investigation determined that an unauthorized individual gained access to certain Swissport systems between February 1 through February 3, 2022, that resulted in the encryption of some of our networks and servers. With the assistance of cybersecurity experts and out of an abundance of caution, affected servers were immediately taken offline and analyzed. We then proceeded to conduct a thorough and time-intensive review of the impacted information to ensure we identified all individuals with information potentially impacted. During our comprehensive review of the systems and data potentially impacted, we discovered some of your personal information.

What Information Was Involved? Our investigation determined that the following types of your personal information was included in the impacted data: [Extra2].

What We Are Doing. Please know that protecting your personal information is something that Swissport takes very seriously. We conducted a diligent investigation to confirm the nature and scope of the incident. We also took steps to further secure our systems to prevent an incident like this in the future, and we continue to make additional improvements that strengthen our cybersecurity protections. We continue to monitor for any unauthorized uses of your personal information, and while we are unaware of any attempted or actual misuse of your information, we are sending you this letter so that you can take steps to protect yourself.

Although we have no evidence to suggest that your personal information has been fraudulently used, we are nevertheless offering you a **complimentary** ## month membership of Experian's IdentityWorks. This service helps detect possible misuse of your personal information and provides you with identity protection support. To enroll in this service, please follow the instructions below in the "**What You Can Do**" section by December 31, 2022.

What You Can Do. To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for ## months.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to you for ## months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

While identity restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorks as a complimentary ##-month membership. This product provides you with superior identity detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by** December 31, 2022 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: https://www.experianidworks.com/credit
- Provide your **activation code**:

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident, or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at (888) 397-0030 by December 31, 2022. Be prepared to provide engagement number ENGAGE# as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ##-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks. You can contact Experian immediately regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup**: See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE[TM]:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Please review the enclosed Information about Identity Theft Protection for additional information on how to protect against identity theft and fraud. You may also take advantage of the complimentary identity protection services being offered.

For More Information. We sincerely regret any inconvenience or concern caused by this incident. If you have further questions or concerns, or would like an alternative to enrolling online, please call (888) 397-0030 toll-free Monday through Friday from 8 am – 10 pm Central, or Saturday and Sunday from 10 am – 7 pm Central (excluding major U.S. holidays). Be prepared to provide your engagement number ENGAGE#.

Sincerely,

Todd Lindamood
Senior Vice President, Human Resources
Swissport North America Inc.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Information about Identity Theft Protection

Monitor Your Accounts

We recommend that you regularly review statements from your accounts and periodically obtain your credit report from one or more of the national credit reporting companies. You may obtain a free copy of your credit report online at www.annualcreditreport.com, by calling toll-free 1-877-322-8228, or by mailing an Annual Credit Report Request Form (available at www.annualcreditreport.com) to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281. You may also purchase a copy of your credit report by contacting one or more of the three national credit reporting agencies listed below.

Equifax®
P.O. Box 740241
Atlanta, GA 30374-0241
1-800-685-1111
www.equifax.com

Experian
P.O. Box 9701
Allen, TX 75013-9701
1-888-397-3742
www.experian.com

TransUnion®
P.O. Box 1000
Chester, PA 19016-1000
1-800-888-4213
www.transunion.com

When you receive your credit reports, review them carefully. Look for accounts or creditor inquiries that you did not initiate or do not recognize. Look for information, such as home address and Social Security number that is not accurate. If you see anything you do not understand, call the credit reporting agency at the telephone number on the report.

Credit Freeze

You have the right to put a security freeze, also known as a credit freeze, on your credit file, so that no new credit can be opened in your name without the use of a Personal Identification Number (PIN) that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to access your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. Should you wish to place a credit freeze, please contact all three major consumer reporting agencies listed below.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
www.equifax.com/personal/
credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/
freeze/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-888-909-8872
www.transunion.com/
credit-freeze

You must separately place a credit freeze on your credit file at each credit reporting agency. The following information should be included when requesting a credit freeze:

1) Full name, with middle initial and any suffixes;
2) Social Security number;
3) Date of birth (month, day, and year);
4) Current address and previous addresses for the past five (5) years;
5) Proof of current address, such as a current utility bill or telephone bill;
6) Other personal information as required by the applicable credit reporting agency;

If you request a credit freeze online or by phone, then the credit reporting agencies have one (1) business day after receiving your request to place a credit freeze on your credit file report. If you request a lift of the credit freeze online or by phone, then the credit reporting agency must lift the freeze within one (1) hour. If you request a credit freeze or lift of a credit freeze by mail, then the credit agency must place or lift the credit freeze no later than three (3) business days after getting your request.

Fraud Alerts

You also have the right to place an initial or extended fraud alert on your file at no cost. An initial fraud alert lasts 1-year and is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7

years. Should you wish to place a fraud alert, please contact any one of the agencies listed below. The agency you contact will then contact the other two credit agencies.

Equifax
P.O. Box 105788
Atlanta, GA 30348-5788
1-888-766-0008
www.equifax.com/personal/credit-report-services

Experian
P.O. Box 9554
Allen, TX 75013-9554
1-888-397-3742
www.experian.com/fraud/center.html

TransUnion
P.O. Box 2000
Chester, PA 19016-2000
1-800-680-7289
www.transunion.com/fraud-victim-resource/place-fraud-alert

Additional Information

You can further educate yourself regarding identity theft and the steps you can take to protect yourself, by contacting your state Attorney General or the Federal Trade Commission. Instances of known or suspected identity theft should be reported to law enforcement, your Attorney General, and the FTC.

The Federal Trade Commission
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-ID-THEFT (1-877-438-4338)
TTY: 1-866-653-4261
www.ftc.gov/idtheft

District of Columbia Residents: You may obtain information about preventing and avoiding identity theft from the Office of the Attorney General for the District of Columbia at:

Office of the Attorney General for the District of Columbia
400 6th Street, NW
Washington, D.C. 20001
(202) 727-3400
Email: oag@dc.gov
https://oag.dc.gov/Consumer

Iowa Residents: You may obtain information about preventing and avoiding identify theft, or reporting suspected incidents of identity theft from the following Iowa agencies:

Office of the Attorney General of Iowa
Consumer Protection Division
1305 E. Walnut Street
Des Moines, Iowa 50319-0106
Telephone: 515-281-5926; or
888-777-4590 (outside of the Des Moines metro area)
Email: consumer@ag.iowa.gov

Office of the Attorney General
Crime Victim Assistance Division
Lucas State Office Building
321 East 12th Street
Des Moines, IA 50319
Telephone: 515-281-5044
Toll-Free: 800-73-5044

Maryland Residents: You may obtain information from the Maryland Office of the Attorney General about steps you can take to avoid identity theft at:

Office of the Attorney General of Maryland
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
Telephone: 1-888-743-0023
https://www.ag.md/IdentityTheft

New York Residents: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General
Consumer Frauds & Protection Bureau
The Capitol
Albany, NY 12224-0341
(800) 771-7755
https://ag.ny.gov/consumer-frauds-bureau

New York Department of State
Division of Consumer Protection
99 Washington Avenue, Suite 650
Albany, NY 12231
(800) 697-1220
www.dos.ny.gov

North Carolina Residents: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office at:

Office of the Attorney General of North Carolina
114 West Edenton Street
Raleigh, NC 27699-9001
Telephone: 1-919-716-6400
www.ncdoj.gov

Oregon Residents: You may obtain information about reporting suspected identity theft from the following Oregon agencies:

Office of the Attorney General
Oregon Department of Justice
1162 Court St. NE
Salem, OR 97301-4096
Email: AttorneyGeneral@doj.state.or.us

Office of Attorney General
Consumer Protection
Toll-Free: 1-877-877-9392
https://justice.oregon.gov/consumercomplaints/

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.