Freshfields Bruckhaus Deringer US LLP

BROCK DAHL

Washington
700 13th Street, NW, 10th Floor
Washington, DC 20005
T +1 (202) 777-4500 (Switchboard)
+1 (202) 777-4538 (Direct)
E brock.dahl@freshfields.com
freshfields.us

By E-Mail

Office of the Attorney General
Idtheft@oag.state.md.us

April 22, 2022

To Attorney General Frosh:

We write pursuant to Md. Code Ann., Com. Law § 14-3504 to inform you that Silversea Cruises Ltd. (***Silversea***) will be sending notices to Maryland residents advising them of a data incident. On August 24, 2021, Silversea identified indications of potential unauthorized access to and attempts to encrypt certain of its information technology systems. A subsequent prioritized review of the contents of those systems that may have been accessible identified personal data potentially giving rise to a notification obligation under Maryland law. At this time, Silversea has identified 24 such records for which the corresponding person appears to be a Maryland resident. By providing this notice, Silversea does not waive any rights or defenses regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Although the personal information identified for this population varies from individual to individual, in general such information may include names; dates of birth; gender; nationality; contact information; government identification numbers, including social security numbers, other tax identification numbers, or passport numbers; or financial account numbers. For Silversea employees, the information may include data such as position title and voyages on which crewmembers served. For Silversea guests, the information may include data about the guest's vacations with Silversea, such as destinations visited.

We are not currently aware of any financial harm to any Maryland residents whose data was involved in this incident. Silversea interrupted the attempts to encrypt its systems, and to date, Silversea has not been contacted by the malicious actor.

Starting on April 27, formal notices of the incident will be sent by U.S. mail to individuals for whom we have identified a Maryland mailing address. A copy of the anticipated notice is attached. Silversea is providing two years of complimentary credit monitoring services to affected state residents.

Silversea takes the security of information on guests, employees, and others seriously. Silversea continues to evolve its cyber security practices in line with its reliance on technology and the changing external threat landscape. Since this event, Silversea has taken additional steps to strengthen the security and monitoring that protects its systems.

Please contact me if you have any questions.

Sincerely,

Brock Dahl

Brock Dahl

Enclosures (1)

SILVERSEA

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Dear Sir or Madam:

We are writing to let you know about an incident in which a third party may have gained unauthorized access to your personal information. Below is a summary of what happened, what personal data was involved, what we are doing, what you can do, and where you can obtain more information.

Notice of Data Breach	
What happened?	At some time between August 18, 2021, and August 25, 2021, certain of your personal data may have been accessed by a third party who gained unauthorized remote access to a limited number of our company systems. Following discovery, we implemented measures to contain the incident, remove the third party access and secure our network. We also began an investigation and arranged resources to start identifying, informing, and assisting persons whose personal information may have been involved. During our review, we identified certain of your information as having potentially been accessed, although we are not aware of any attempt to exploit this information in any way.
What personal data was involved?	In addition to your name and information about your relationship with Silversea Cruises, the personal data that may have been accessed includes some or all of the following: your date of birth; gender; nationality; contact information; passport number; driver's license or other government identification number; social security number; financial account number; credit or debit card number; a username and password for an online account; or health information.
What are we doing?	We are taking this incident very seriously and have taken steps to strengthen the security and monitoring that protects our systems. We have not identified any further unauthorized activity since the breach was identified and contained in August 2021. We will continue to closely monitor and take further steps as appropriate to safeguard your personal data.
What can you do?	Although we are not aware of any attempts to exploit this information, as a precautionary measure, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for 24 months. This service is provided by Equifax. You can find information about the service and how to enroll in Appendix A to this letter. In addition to enrolling in Equifax's complimentary online credit monitoring service, you can protect yourself by monitoring your financial accounts and your account statements for unusual or unauthorized activity over the next 12 to 24 months and promptly report any suspected identity theft to the police. You should be vigilant against possible "phishing" communications and emails that appear to be (but are not) sent from Silversea brand email addresses.

For more information	We are sorry that this occurred. You can find more information about steps that you can take in Appendix B to this letter. If you have any questions, please call 855-520-1219 between 9:00 a.m. and 9:00 p.m. Eastern Time, Monday through Friday.

Yours sincerely,

Roberto Martinoli
President and CEO

Appendix A

EQUIFAX®

<<Name 1>>
Enter your Activation Code: <<Activation Code>>
Enrollment Deadline: <<Enrollment Deadline>>

<u>Equifax Credit Watch™ Gold</u>

*Note: You must be over age 18 with a credit file to take advantage of the product

<u>Key Features</u>

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

<u>Enrollment Instructions</u>

Go to ***www.equifax.com/activate***

Enter your unique Activation Code of <<Activation Code>> then click "Submit" and follow these 4 steps:

1. **<u>Register</u>:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header.
   Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **<u>Create Account</u>:**
   Enter your email address, create a password, and accept the terms of use.
3. **<u>Verify Identity</u>:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **<u>Checkout</u>**:
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

<u>You're done</u>!
The confirmation page shows your completed enrollment.
Click "View My Product" to access the product features.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

APPENDIX B

MEASURES THAT YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

1. prevent you from getting your free annual credit report;
2. keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;
3. prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

EQUIFAX
Fraud Alerts

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
888-836-6351 (automated service line)
800-525-6285 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Security Freezes

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
888-298-0045 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Credit Reports

Equifax Information Services LLC
P.O. Box 740241
Atlanta, GA 30374-0241
866-349-5191
https://www.annualcreditreport.com/index.action

EXPERIAN
Fraud Alerts

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.experian.com/fraud/center.html

Security Freezes

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013 (regular mail)
Experian
711 Experian Parkway
Allen, TX 75013 (overnight mail)
1-888-397-3742
https://www.experian.com/freeze/center.html

Credit Reports

Experian
P.O. Box 4500
Allen, TX 75013
1-888-397-3742
https://www.annualcreditreport.com/index.action

TransUnion

Fraud Alerts

TransUnion Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://fraud.transunion.com

Security Freezes

TransUnion LLC
P.O. Box 2000
Chester, PA 19016
888-909-8872
https://freeze.transunion.com/

Credit Reports

Annual Credit Report Request Service
P.O. Box 105281
Atlanta, GA 30348-5281
800-888-4213
https://www.annualcreditreport.com/index.action

INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC by mail at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.*

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

In addition, as of September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. *See www.ftc.gov/credit for additional information.*

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures.*

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit.*

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).*

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active duty military personnel have additional rights. *For more information, visit www.ftc.gov/credit.*

Source: https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.

IF YOU ARE A RESIDENT OF CERTAIN STATES, YOU HAVE ADDITIONAL RIGHTS:

Massachusetts

Under Massachusetts state law, you have the right to obtain any police report filed 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.

Oregon

You can reach the Attorney General of the State of Oregon at 1-877-877-9392 or by mail at help@oregonconsumer.gov.

Rhode Island

You can reach the Attorney General of the State of Rhode Island by phone at (401) 274-4400 or online at www.riag.ri.gov.

Maryland

You may also wish to review information provided by the Maryland Attorney General on how to avoid identity theft at http://www.oag.state.md.us/idtheft, or by sending an email to idtheft@oag.statemd.us, or calling 1-410-576-6491. The Identity Theft Unit can give you step-by-step advice on how to protect yourself from identity thieves using, or continuing to use, your personal information. You may also reach the Maryland Attorney General by mail at:

Identity Theft Unit
Office of the Attorney General
200 St. Paul Place
25th Floor
Baltimore, MD 21202

North Carolina
You can reach the Attorney General of the State of North Carolina by mail at:
9001 Mail Service Center
Raleigh, NC 27699-9001
+1 (919) 716-6400
http://www.ncdoj.gov

District of Columbia
You can reach the Attorney General of the District of Columbia at:
400 6th Street NW
Washington, D.C. 20001
Phone: (202) 727-3400
https://oag.dc.gov/