

COVINGTON

BEIJING BOSTON BRUSSELS DUBAI FRANKFURT
JOHANNESBURG LONDON LOS ANGELES NEW YORK
PALO ALTO SAN FRANCISCO SEOUL SHANGHAI WASHINGTON

Ashden Fein

Covington & Burling LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001-4956
T +1 202 662 5116
afein@cov.com

By Electronic Mail

August 29, 2024

Anthony G. Brown
Office of the Maryland Attorney General
Attn: Notice of Breach
200 St. Paul Place
Baltimore, MD 21202
IDTheft@oag.state.md.us

Re: Legal Notice of Information Security Breach Pursuant to Md. Code Ann., Com. Law § 14-3501(h)(1)

To Whom it May Concern:

In accordance with the above-referenced provision of Maryland law, I write on behalf of Magical Cruise Co. Limited, dba Disney Cruise Line, an affiliate of The Walt Disney Company, and certain other Disney affiliates (collectively, our “client” and “Disney”) to inform you of an information security breach affecting residents of Maryland.

On July 11, 2024, an employee made Disney aware of a security incident involving a bad actor accessing an employee’s Disney Slack account. Upon discovering this incident, Disney promptly took steps to secure the impacted account. It also initiated an ongoing investigation in close consultation with cybersecurity experts and started working with law enforcement. Additionally, Disney is enhancing its security controls to help prevent a similar incident in the future.

Disney determined that between around May 14, 2024, and July 11, 2024, a bad actor accessed an employee’s Disney Slack account by leveraging stolen account credentials and manipulating the employee into accepting a multifactor authentication request (“MFA”). The bad actor then copied certain information from Slack, a communication platform for corporate teams, that was accessible to the employee and posted that information on the dark web. Based on Disney’s investigation to date, there is no evidence that the incident impacted other systems.

Disney’s ongoing investigation also determined that the information may have included current or former employees’ names along with passport number and other personal identifiers, such as name, date and place of birth and contact details, among other types of information. Disney has no indications of this data being misused.

On August 27, 2024, Disney determined that the impacted current and former employees included residents of Maryland. Currently, our client intends to notify 20 potentially affected individuals who are residents of Maryland. Enclosed is a version of the notification letters that

COVINGTON

August 29, 2024
Page 2

our client will send to affected individuals. Affected individuals will be sent this letter via first-class mail starting around September 6, 2024.

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by our client to protect personal information from further unauthorized access; (3) our client's address and a toll-free phone number to call for further information and assistance; (4) information on how the individual may enroll in free credit monitoring and other complimentary services arranged by our client; (5) information about how to place a fraud alert or security freeze on a credit report; (6) the toll-free numbers and addresses for the major consumer reporting agencies; (7) the toll-free number, address, and website for the Federal Trade Commission and the Office of the Attorney General of Maryland, and a statement that individuals can obtain information on identity theft from these sources; (8) advice that directs the individual to remain vigilant by reviewing account(s) for unusual activity and monitoring free credit reports.

If you have any questions or need further information regarding this incident, please contact the undersigned at afein@cov.com or (202) 662-5116.

Respectfully submitted,

A handwritten signature in black ink, appearing to be 'A' followed by a long horizontal stroke.

Ashden Fein

Enclosure:
Sample Notification Letter



3 Queen Caroline Street
Hammersmith, London, W6 9PE

[Date]

[Insert Recipient's name]

[Insert Address]

[Insert City, State, Zip]

NOTICE OF DATA BREACH

Dear [Insert Customer Name],

We, Magical Cruise Co. Limited, dba Disney Cruise Line, an affiliate of The Walt Disney Company, and certain other Disney affiliates, are writing to inform you of a security incident that involved certain of your personal information. We wanted to provide you details of the incident, our response, and steps you may take to protect against possible misuse of your personal information.

What Happened?

On July 11, 2024, we became aware of a security incident involving a bad actor accessing an employee's Disney Slack account. Upon learning of the incident, we immediately initiated an investigation and determined that between around May 14, 2024 and July 11, 2024, a bad actor leveraged stolen account credentials to copy certain information from Slack, a communication platform for corporate teams, accessible to the employee and posted that information on the dark web. Based on our investigation to date, we have no evidence that the incident impacted other systems.

What Information Was Involved?

Although our analysis of the impacted data is ongoing, we determined on August 27, 2024 that the impacted personal information may include your passport number and other personal identifiers, such as name, date and place of birth and contact details, among other types of information. To date, we have no indications that the data included your financial account information or national identity number (e.g., Social Security number). Additionally, we have no indications of your data being misused.

What We Are Doing.

Upon discovering this incident, we promptly took steps to secure the impacted account. We also initiated an ongoing investigation in close consultation with cybersecurity experts and started working with law enforcement. This notice was not delayed as a result of law enforcement notification. Additionally, we are enhancing our security controls to help prevent a similar incident in the future.

To help protect your identity, we are offering a complimentary 12-month membership of Experian's® IdentityWorksSM for credit monitoring and identity theft protection. This product



provides you with superior identity detection and resolution of identity theft. Instructions on how you can take advantage of these services is provided in the enclosed **Attachment A**.

What You Can Do.

Regardless of whether you elect to enroll in IdentityWorksSM, we recommend that you remain vigilant for unsolicited or suspicious communications and incidents of fraud and identity theft, including by regularly reviewing and monitoring your credit history and credit reports to guard against any unauthorized transactions or activity. We also recommend that you closely monitor your account statements and notify your financial institution if you suspect any unauthorized activity. **Attachment B** to this letter contains more information about steps you can take to protect yourself against potential fraud and identity theft.

For More Information.

Please be assured that we are taking steps to address the incident and to protect the security of your data. If you have any questions about this notice or the incident, please feel free to contact us at [\[customer service number\]](#).

Sincerely,

Yvonne Sweeney
Vice President, DSE Human Resources



ATTACHMENT A

To activate your IdentityWorks membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: December 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [\[URL\]](#)
- Provide your **activation code: [code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at [\[customer service number\]](#) by **December 31, 2024**. Be prepared to provide engagement number [\[engagement #\]](#) as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-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 agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at [\[customer service number\]](#). 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 (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 this Identity Restoration support is available to you for 16 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. You will also find self-help tips and information about identity protection at this site.

* 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.



ATTACHMENT B

Additional Information

To protect against possible fraud, identity theft, or other financial loss, we encourage you to remain vigilant, to review your account statements, and to monitor your credit reports. Provided below are the names and contact information for the three major U.S. credit bureaus and additional information about steps you can take to obtain a free credit report, and place a fraud alert or security freeze on your credit report. If you believe you are a victim of fraud or identity theft you should consider contacting your local law enforcement agency, your state's Attorney General, or the U.S. Federal Trade Commission ("FTC").

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT, CREDIT FREEZE, OR CREDIT LOCK

To place a fraud alert, credit freeze, or credit lock on your credit report, you must contact the three consumer reporting agencies below:

Equifax:
Equifax Information
Services LLC
P.O. Box 105788
Atlanta, GA 30348
1-888-298-0045
www.equifax.com

Experian:
Credit Fraud Center
P.O. Box 9554
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion:
Fraud Victim Assistance
Department
P.O. Box 2000
Chester, PA 19022-2000
1-800-680-7289
www.transunion.com

Fraud Alert: Consider contacting the three major consumer reporting agencies at the addresses above to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

To place a fraud alert, contact any of the three major consumer reporting agencies listed above and request that a fraud alert be put on your file. The agency that you contacted must notify the other two agencies. A fraud alert is free and lasts 90 days, but can be renewed.

Credit Freeze: A credit freeze prohibits a consumer reporting agency from releasing any information from a consumer's credit report until the freeze is lifted. When a credit freeze is in place, no one—including you—can open a new account. As a result, 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.

Placing a credit freeze is free. To place a credit freeze, contact all three consumer reporting agencies listed above and provide the personal information required by each agency to place a freeze, which may include:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.); and
7. If you are a victim of identity theft, a copy of either a police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

When you place a credit freeze, you will be provided a PIN to lift temporarily or remove the credit freeze. A credit freeze generally lasts until you lift or remove it, although in some jurisdictions it will expire after seven years.

Credit Lock: Like a credit freeze, a credit lock restricts access to your credit report and prevents anyone from opening an account until unlocked. Unlike credit freezes, your credit can typically be unlocked online without delay. To lock your credit, contact all three consumer reporting agencies listed above and complete a credit lock agreement. The cost of a credit lock varies by agency, which typically charges monthly fees.

You may also contact the FTC for further information on fraud alerts, credit freezes, credit locks, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone 1-877-382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state Attorney General may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state Attorney General, or the FTC.

District of Columbia Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or <https://oag.dc.gov/>. You have the right to obtain a security freeze free of charge pursuant to 15 U.S.C. § 1681c-1.



Maryland Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, MD 21202; (888) 743-0023; or <http://www.oag.state.md.us>.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the 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.

North Carolina Residents: The Attorney General can provide information about steps to take to avoid identity theft and can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or <http://www.ncdoj.gov>.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act ("FCRA"), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

New York Residents: The Attorney General can be contacted at 1-800-771-7755 or <https://ag.ny.gov/>. The Department of State Division of Consumer Protection can be contacted at 1 (800) 697-1220 or <https://dos.ny.gov/>.

Rhode Island Residents: The Attorney General can be contacted at (401) 274-4400 or <http://www.riag.ri.gov/>. You may also file or obtain a police report by contacting local or state law enforcement agencies.