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 September 20, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

Re: Legal Notice of Information Security Breach Pursuant to Md. Code Ann., Com. Law § 14-3501 *et seq*.

To Whom it May Concern:

In accordance with the above-referenced provision of Maryland law, I write to inform you of an information security breach affecting residents of Maryland.

On June 1, 2023, Aristocrat Technologies, Inc. and its affiliates ("Aristocrat") became aware of a cyber incident involving a previously-unknown vulnerability in an external file transfer software named MOVEit Transfer, which is a tool used by governments, companies, and other organizations to share files securely. According to law enforcement, an international group of cyber criminals exploited a zero-day vulnerability in the MOVEit Transfer software to steal electronic files from hundreds of organizations globally.

Upon learning of this vulnerability, Aristocrat immediately removed the impacted server from the network, launched an investigation and fixed the relevant software vulnerability. Aristocrat also notified law enforcement and, where required, relevant supervisory authorities and regulators, and have been working closely with law enforcement since. After a thorough investigation, Aristocrat determined that, between May 29 and May 31, 2023, a criminal group exploited the vulnerability to extract information from an Aristocrat server, including certain personal data belonging to some individuals. Aristocrat has found no indications that any of its other systems (or data from those systems) were impacted.

On August 18, 2023, with the assistance of external experts that Aristocrat engaged to assist with the investigation, Aristocrat determined that the extracted information may have included Social Security numbers, drivers' license numbers, passport numbers and dates of birth. Beginning around September 21, 2023, Aristocrat plans to notify 10 potentially affected individuals who are residents of Maryland. In addition, Aristocrat is providing 24-months of identity monitoring services to all individuals affected. Enclosed is the baseline version of notification letter that Aristocrat plans to send to affected individuals.

The notification to individuals includes (1) a description of the incident and the type of personal information at issue; (2) the actions taken by Aristocrat to protect personal information from further unauthorized access; (3) Aristocrat's addresses and toll-free phone numbers 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 a statement that individuals can obtain information on identity theft from this source; (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 (202) 662-5116 or afein@cov.com.

Respectfully submitted,

Ashden Fein

Enclosure

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

September 21, 2023

K0309-L1A-0000001 T00001 P001 ********SCH 5-DIGIT 12345
SAMPLE A SAMPLE - L1A ADULT RED
APT ABC
123 ANY STREET
ANYTOWN, FC 1A2 B3C
COUNTRY

NOTICE OF DATA BREACH

Dear Sample A. Sample:

We are writing to provide information relating to a cyber incident that involved some of your personal information. Please know, we take the privacy and security of the personal data we hold about you seriously. Below we have outlined the steps that we have taken, and measures that you can take, to help further protect your data.

What Happened?

On 1 June 2023, Aristocrat became aware of a cyber incident involving a previously-unknown vulnerability in an external file transfer software named MOVEit Transfer, which is a tool used by governments, companies, and other organisations to share files securely. This incident has impacted hundreds of organizations globally, including Aristocrat.

After a thorough investigation, we determined that, between 29-31 May 2023, a criminal group exploited the vulnerability to extract information from an Aristocrat server, including certain personal data belonging to some individuals. We have found no indications that any of our other systems (or data from those systems) were impacted.

What Information Was Involved?

On 18 August, 2023, with the assistance of external experts that we engaged to assist with the investigation, we determined that the extracted information may have included your Social Security number, national identifier, government-issued identification number, or date of birth, among other types of information.

What We Are Doing.

Upon learning of this vulnerability, we immediately removed the impacted server from the network, launched an investigation and fixed the relevant software vulnerability. We also notified law enforcement and, where required, relevant supervisory authorities and regulators, and have been working closely with them since.

We are also offering 24 months of complimentary credit monitoring and identity theft protection services to you, and all individuals impacted by this incident, where the service is available. You may sign up for this service by following the instructions included in Attachment A.

ARISTOCRAT

What You Can Do.

Regardless of whether you elect to enroll in the identity-theft protection service, we strongly recommend that you remain vigilant and regularly review and monitor all of your credit history (if available) 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 unauthorised activity. Attachment B contains more information about steps you can take to protect yourself against fraud and identity theft.

For More Information.

We will continue to work hard to protect your information and that of our organisation. If you have any questions about this notice or the incident, please feel free to call **833-575-2853** 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 **B105059**. Alternatively, you can email AskAristocrat@aristocrat.com for assistance.

Sincerely,

Tanya Madison
Global Chief Privacy Officer

ARISTOCRAT

ATTACHMENT A

To help protect your identity, we are offering complimentary access to Experian IdentityWorks[SM] for 24 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 24 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 24-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, 2023 (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: [Extra2]
- Provide your **activation code**: **ABCDEFGHI**

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 **833-575-2853** by December 31, 2023. Be prepared to provide engagement number **B105059** as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-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, Equifax and Transunion files 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.

* 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 Federal Trade Commission.

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 below 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 U.S. Federal Trade Commission ("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 be contacted at the Office of the Attorney General, 441 4th Street NW, Washington, DC 20001; (202) 727-3400; or https://oag.dc.gov/.

Maryland Residents: The Attorney General 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.

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/articles/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/.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; (919) 716-6400; or http://www.ncdoj.gov.

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