

June 7, 2024

Via Email

ldtheft@oag.state.md.us

Re: Legal Notice of Data Security Incident

Dear Sir or Madam:

I am writing on behalf of my client Christie's Inc. ("Christie's") to inform you of a cybersecurity incident.

On May 9, 2024, Christie's discovered that it was the victim of a cybersecurity incident that impacted some of its systems. As soon as Christie's became aware of this incident, it promptly took steps to secure its environment, launched an investigation, and engaged external cybersecurity experts to assist. It also notified law enforcement and continues supporting their investigation.

The investigation revealed an unauthorized actor accessed some of Christie's systems and certain files stored therein between May 8, 2024, and May 9, 2024, and some files were copied from those systems on May 9, 2024. Christie's conducted a robust review of the files to identify individuals whose information may have been impacted and worked to obtain addresses and notify them as quickly as possible after completing the review on May 30, 2024. Christie's determined that the data contained personal information for eight hundred thirty-five (835) Maryland residents including name, Driver's License number, electoral card information, foreign identification card number, national identification card number, and/or passport number.

Today, June 7, 2024, Christie's will begin mailing notification letters to individuals, which include the eight hundred thirty-five (835) Maryland residents, and will be offering the Maryland residents twelve months of complimentary credit monitoring and fraud protection services. A copy of the notice letter is attached. Christie's is also providing a telephone number for the recipients to call with questions regarding the incident.

To help prevent something like this from happening again, Christie's has implemented and will continue to adopt additional safeguards and technical security measures to further protect and monitor its systems.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.



Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3446
dan.pepper@nortonrosefulbright.com

Tel +1 212 318 3000
Fax +1 212 318 3400

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

June 7, 2024
Page 2

^NORTON ROSE FULBRIGHT

Respectfully submitted,

Daniel Pepper

Dan Pepper
Enclosure

CHRISTIE'S

Secure Processing Center
25 Route 111, P.O. Box 1048
Smithtown, NY 11787

Postal Endorsement Line

<<Full Name>>

<<Address 1>>

<<Address 2>>

<<Address 3>>

<<City>>, <<State>> <<Zip>>

<<Country>>

***Postal IMB Barcode

<<Date>>

RE: NOTICE OF DATA BREACH

Dear <Full Name>,

We are writing to inform you of a data security incident we recently experienced that involved some of your information. This letter explains the incident, our response, and resources you may use to help protect your data from possible misuse should you feel it is appropriate to do so. We are not aware of any attempts to misuse your information as a result of this incident.

What Happened?

On May 9, 2024, we discovered that we were the victim of a cybersecurity incident that impacted some of our systems. As soon as we became aware of this event, we promptly took steps to secure our environment, launched an investigation, and engaged external cybersecurity experts to assist. We also notified law enforcement and continue supporting their investigation.

The investigation revealed an unauthorized actor accessed some of our systems and certain files stored therein between May 8, 2024, and May 9, 2024, and some files were copied from those systems on May 9, 2024. We conducted a robust review of the files to identify individuals whose information may have been impacted and worked to obtain addresses and notify them as quickly as possible after completing the review on May 30, 2024.

What Information Was Involved?

Our review determined the files involved in this incident contained your name and the following: <<Impacted Data Elements >.

What We Are Doing

As a precaution, we have arranged for you to receive a complimentary twelve-month subscription to CyEx Identity Defense Total. This identity theft and fraud monitoring service will notify you of changes to your Experian, Equifax, and TransUnion credit files, which allows you to identify any potential fraudulent activity on your credit reports.

We took additional steps to secure our systems and continue to evaluate technical and organizational measures to avoid the reoccurrence of a similar incident.

What You Can Do

For more information on CyEx Identity Defense Total, including instructions on activating your complimentary twelve-month membership and additional information on steps you can take in response to this incident, please see the pages that follow this letter.

We also encourage you to remain vigilant against incidents of identity theft and fraud by engaging in the following best practices:

- Change your passwords regularly and make sure they are secure. Do not use the same passwords for work and personal accounts.
- Be careful when sharing your personal information unsolicited, whether by phone, email, or on a website.
- Avoid clicking on links or downloading attachments in suspicious emails.

For More Information

The privacy and protection of personal information is a top priority at Christie's, and we deeply regret any inconvenience or concern this incident may cause. Should you have further questions, please call 212-641-3620 Monday through Friday between 9 am and 5 pm EST (excluding major U.S. holidays).

Sincerely,

A handwritten signature in black ink that reads "Ben Gore". The signature is written in a cursive, flowing style.

Ben Gore
Chief Operating Officer

ATTACHMENT A

Identity Defense Total

Key Features

- 3-Bureau Credit Monitoring
- Monthly Credit Score and Tracker (VantageScore 3.0)
- Real-Time Authentication Alerts
- High-Risk Transaction Monitoring
- Address Change Monitoring
- Dark Web Monitoring
- Wallet Protection
- Security Freeze Assist
- \$1 Million Identity Theft Insurance**

Enrollment Instructions

To enroll in Identity Defense, visit app.identitydefense.com/enrollment/activate/chrs

1. Enter your unique Activation Code: <<Activation Code>>

Enter your Activation Code and click 'Redeem Code'.

2. Create Your Account

Enter your email address, create your password, and click 'Create Account'.

3. Register

Enter your legal name, home address, phone number, date of birth, Social Security Number, and click 'Complete Account'.

4. Complete Activation

Click 'Continue to Dashboard' to finish enrolling.

The deadline to enroll is <<Enrollment Deadline>>. After <<Enrollment Deadline>>, the enrollment process will close, and your Identity Defense code will no longer be active. If you do not enroll by <<Enrollment Deadline>>, you will not be able to take advantage of Identity Defense, so please enroll before the deadline.

If you need assistance with the enrollment process or have questions regarding Identity Defense, please call Identity Defense directly at **1.866.622.9303**.

ADDITIONAL STEPS YOU CAN TAKE

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit <https://www.annualcreditreport.com/index.action> or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at <https://consumer.ftc.gov/>) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Contact information for the three nationwide credit reporting companies is as follows:

<u>Equifax</u>	<u>Experian</u>	<u>TransUnion</u>
<u>Phone: 1-800-685-1111</u>	<u>Phone: 1-888-397-3742</u>	<u>Phone: 1-888-909-8872</u>
<u>P.O. Box 740256</u>	<u>P.O. Box 9554</u>	<u>P.O. Box 2000</u>
<u>Atlanta, Georgia 30348</u>	<u>Allen, Texas 75013</u>	<u>Chester, PA 19016</u>
<u>https://www.equifax.com/</u>	<u>https://www.experian.com/</u>	<u>www.transunion.com</u>

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible and display your name, current mailing address, and the date of issue. You may obtain information from the credit reporting agencies and the FTC about security freezes.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on

your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report. You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, ct.gov/ag, 860-808-5318.

For District of Columbia residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, oag.dc.gov, 202-442-9828.

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 888-743-0023.

For New York residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, dos.ny.gov/consumerprotection, 518-474-8583 / 800-697-1220; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, ag.ny.gov, 800-771-7755.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, ncdoj.gov, 877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, riag.ri.gov, 401-274-4400.

For Washington residents: You may contact the Washington State Office of the Attorney General, 1125 Washington St SE, PO Box 40100, Olympia, WA 98504, <https://www.atg.wa.gov/>, 1-800-551-4636 (in Washington only) or 1-206-464-6684.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon Residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident.