STATE OF NH
DEPT OF JUSTICE
2017 MAR 28 AM 11: 22

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2732
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

March 24, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Christie's Inc. ("Christie's"), to inform you of a security incident involving personal information that affected approximately four New Hampshire residents. Christie's has notified these individuals and outlined some steps they may take to help protect themselves.

Christie's recently discovered that it was victimized by a targeted e-mail phishing scam in which an unknown individual was able to obtain and use the e-mail login credentials for three Christie's employees. The dates of the potential unauthorized access to the email accounts vary, but were generally in the first half of 2016. At this point, Christie's does not have evidence that any particular email containing individuals' personal information was actually accessed or acquired by the unauthorized actors, though Christie's cannot rule it out. Nor is Christie's aware of any fraud or misuse of any individuals' personal information as a result of this incident.

E-mails in the affected mailboxes included certain information individuals provided to Christie's, such as name, personal or business address(es), personal or business phone number(s), credit or debit card number, date of birth, or government-issued identification number. Social Security Numbers of New Hampshire residents were not involved in this incident.

Christie's takes the privacy and security of its clients' personal information very seriously. It retained a top computer forensics firm to help it conduct a thorough investigation of the incident and performed an extensive review of the relevant email boxes for potentially impacted personal information. To help prevent a similar type of incident from occurring in the future, Christie's has implemented additional security measures designed to protect Christie's email accounts and personal information, including two-factor authentication for remote access to its email system. Christie's has also undertaken an employee education initiative to inform employees about

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.

phishing scams and how to guard against them and will continue to deliver additional employee training about email safety and recognizing phishing emails. Christie's has also reported the incident to law enforcement and will continue to cooperate with any investigation.

Affected individuals were notified via written letter, including an offer for one year of complimentary identity protection and fraud resolution services, on or around March 15, 2017, with a follow-up notice sent on March 24, 2017. A form copy of the notice sent to affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2732 or david.navetta@nortonrosefulbright.com.

Very truly yours,

David Navetta
Partner
Co-Chair, Data Protection, Privacy & Access to Information

DJN/smm
Enclosure

STATE OF NH
DEPT OF JUSTICE
2017 MAR 28 AM 11: 22

NORTON ROSE FULBRIGHT

Norton Rose Fulbright US LLP
Tabor Center
1200 17th Street, Suite 1000
Denver, Colorado 80202-5835
United States

Direct line +1 303 801 2732
david.navetta@nortonrosefulbright.com

Tel +1 303 801 2700
Fax +1 303 801 2777
nortonrosefulbright.com

March 24, 2017

By Certified Mail
Return Receipt Requested

Office of the New Hampshire Attorney General
Consumer Protection & Antitrust Bureau
33 Capitol Street
Concord, NH 03301

Re: Legal Notice of Information Security Incident

Dear Sirs or Madams:

I write on behalf of my client, Christie's Inc. ("Christie's"), to inform you of a security incident involving personal information that affected approximately four New Hampshire residents. Christie's has notified these individuals and outlined some steps they may take to help protect themselves.

Christie's recently discovered that it was victimized by a targeted e-mail phishing scam in which an unknown individual was able to obtain and use the e-mail login credentials for three Christie's employees. The dates of the potential unauthorized access to the email accounts vary, but were generally in the first half of 2016. At this point, Christie's does not have evidence that any particular email containing individuals' personal information was actually accessed or acquired by the unauthorized actors, though Christie's cannot rule it out. Nor is Christie's aware of any fraud or misuse of any individuals' personal information as a result of this incident.

E-mails in the affected mailboxes included certain information individuals provided to Christie's, such as name, personal or business address(es), personal or business phone number(s), credit or debit card number, date of birth, or government-issued identification number. Social Security Numbers of New Hampshire residents were not involved in this incident.

Christie's takes the privacy and security of its clients' personal information very seriously. It retained a top computer forensics firm to help it conduct a thorough investigation of the incident and performed an extensive review of the relevant email boxes for potentially impacted personal information. To help prevent a similar type of incident from occurring in the future, Christie's has implemented additional security measures designed to protect Christie's email accounts and personal information, including two-factor authentication for remote access to its email system. Christie's has also undertaken an employee education initiative to inform employees about

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.

phishing scams and how to guard against them and will continue to deliver additional employee training about email safety and recognizing phishing emails. Christie's has also reported the incident to law enforcement and will continue to cooperate with any investigation.

Affected individuals were notified via written letter, including an offer for one year of complimentary identity protection and fraud resolution services, on or around March 15, 2017, with a follow-up notice sent on March 24, 2017. A form copy of the notice sent to affected New Hampshire residents is included for your reference.

If you have any questions or need further information regarding this incident, please contact me at (303) 801-2732 or david.navetta@nortonrosefulbright.com.

Very truly yours,

David Navetta
Partner
Co-Chair, Data Protection, Privacy & Access to Information

DJN/smm
Enclosure

A

STATE OF NH
DEPT OF JUSTICE
2017 MAR 28 AM 11:22

CHRISTIE'S

<<Date>>

<<First Name>> <<Middle Name>> <<Last Name>>
<<Address Line 1>>
<<Address Line 2>>
<<City>>, <<State>> <<ZIP>>

Dear <<First Name>>,

Notice of Data Breach

We are writing to inform you of a security incident that may have affected certain personal information you provided to Christie's and, as a precaution, to call your attention to steps you can take to help protect your information. We sincerely regret any concern this incident may cause.

What Happened

We recently discovered that Christie's was victimized by a targeted e-mail phishing scam in which an unknown individual was able to obtain and use the e-mail login credentials for three Christie's employees. The dates of the potential unauthorized access to the email accounts vary, but were generally in the first half of 2016. At this point, we do not have evidence that any particular email containing your personal information was actually accessed or acquired by the unauthorized actors, though we cannot rule it out. Nor are we aware of any fraud or misuse of any of your personal information as a result of this incident.

What Information Was Involved

E-mails in the affected mailboxes included certain information you provided to Christie's, such as your:

Name
Personal or business contact information
<<Social Security Number>>
<<Bank account number>>
<<Payment card information>>
<<Driver's license or government issued identification number>>
<<Date of birth>>
<<Username and password>>

What We Are Doing

Christie's takes the privacy and security of your personal information very seriously. We retained a top computer forensics firm to help us conduct a thorough investigation of the incident. To help prevent a similar type of incident from occurring in the future, we have implemented additional security measures designed to protect Christie's email accounts and your information, including two-factor authentication for remote access to our email system. We have also undertaken an employee education initiative to inform employees about phishing scams and how to guard against them and will continue to deliver additional employee training about email safety and recognizing phishing emails. We have also reported the incident to law enforcement and will continue to cooperate with any investigation.

Christie's
20 Rockefeller Plaza, New York, NY 10020
212.636.2000
www.christies.com

CHRISTIE'S

What You Can Do

As a precaution, there are several steps listed below that may help to guard against fraud or identity theft:

- **Enrollment in Identity Protection Services**. We have engaged Experian® to offer you complimentary fraud resolution and identity protection services for one year. These services help detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. To enroll, please follow these steps:
    - Visit www.experianidworks.com/3bcreditone to enroll
    - Provide the following activation code: **<<Experian Code>>**
    - Enroll by **March 20, 2018** (your code will not work after this date)
    - You may also enroll over the phone by calling 877-890-9332 between the hours of 9:00 AM and 9:00 PM (Eastern Time), Monday through Friday and 11:00 AM and 8:00 PM Saturday (excluding holidays). Please provide the following engagement number as proof of eligibility: **XXXXXXX**.

  Please see the attached guide for further information about the complimentary Experian services we have arranged for you.

- **Review of Financial Accounts and Credit Reports**. You can carefully review your account statements and credit reports for suspicious activity, accounts you did not open, or inquiries from creditors you did not initiate. You should remain vigilant and continue to monitor your statements for unusual activity going forward. If you see anything you do not understand on your credit report, call the credit agency immediately. If you find any suspicious activity on your statements or credit reports, call your local police or sheriff's office, file a police report for identity theft and get a copy of it. You may need to give copies of the police report to creditors to clear up your records.

- **Information About Identity Theft Protection Guide**. Please review the "Information About Identity Theft Protection" reference guide, enclosed here, which describes additional steps you may take to help protect yourself, including recommendations from the Federal Trade Commission regarding identity theft protection and details regarding placing a fraud alert or a security freeze on your credit file.

For More Information

We understand that you may be concerned about this matter, and we sincerely regret that this incident occurred. For more information, or if you have questions or need additional information, please contact our dedicated Client Services team at **XXX-XXX-XXXX**.

Sincerely,

<<SIGNATURE>>

Richard Entrup
Chief Information Officer

CHRISTIE'S

INFORMATION ABOUT IDENTITY THEFT PROTECTION

Experian IdentityWorks℠ Membership: Christie's has arranged one year of complimentary membership in Experian's IdentityWorks℠ as an accommodation to you after this incident. You can contact Experian **immediately** in the event you experience any fraud, 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™:** 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.

While Identity Restoration assistance is immediately available to you, we also encourage you to activate the fraud detection tools available through Experian IdentityWorksSM. To start monitoring your personal information please follow the steps below:

- Visit www.experianidworks.com/3bcreditone to enroll
- Provide the activation code included in the letter you received regarding this incident
- Enroll by March 20, 2018 (your code will not work after this date)

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 877-890-9332 by March 20, 2018. Be prepared to provide engagement number **XXXXXXX** as proof of eligibility for the identity restoration services.

A credit card is **not** required for enrollment in Experian IdentityWorks. 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.

Review of Accounts and Credit Reports: As a precaution you may 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 at the end of this guide.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft. There may be similar resources available at the state level, and you may contact your state department of revenue directly for more information.

For residents of Maryland: You may also obtain information about preventing and avoiding identity theft from the Maryland Office of the Attorney General: Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For residents of North Carolina: You may also obtain information about preventing and avoiding identity theft from North Carolina Attorney General's Office: North Carolina Attorney General's Office, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-5-NO-SCAM, www.ncdoj.gov.

For residents of Rhode Island: You may also obtain information about preventing and avoiding identity theft from the Rhode Island Office of the Attorney General: Rhode Island Office of the Attorney General, Consumer Protection Unit, 150 South Main Street, Providence, RI 02903, 401-274-4400, http://www.riag.ri.gov.

Fraud Alerts: There are also two types of fraud alerts that you can place on your credit report to put creditors on notice that you may be a victim of fraud: an initial alert and an extended alert. You may request an initial fraud alert if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may request an extended fraud alert 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed below.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number 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 get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

NATIONAL CREDIT REPORTING AGENCIES CONTACT INFORMATION

Equifax (www.equifax.com)
P.O. Box 740241
Atlanta, GA 30374
800-685-1111

Fraud Alerts:
https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp
Credit Freezes:
https://www.freeze.equifax.com

Experian (www.experian.com)
P.O. Box 2002
Allen, TX 75013
888-397-3742

Fraud Alerts:
https://www.experian.com/fraud/center.html
Credit Freezes:
https://www.experian.com/consumer/security_freeze.html

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

Fraud Alerts:
http://www.transunion.com/personal-credit/credit-disputes/fraud-alerts.page
Credit Freezes:
http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page