BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

May 24, 2019

VIA E-MAIL (SECURITYBREACH@ATG.WA.GOV)

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave., Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, Drury Hotels Company, LLC ("Drury"), to notify your office of a security incident involving Washington residents.

On March 26, 2019, Drury was notified by a vendor that collects data from reservations made through third-party booking websites and enters it into hotel property management systems for Drury and other hotel companies ("Vendor") that Vendor was conducting an investigation to determine if there had been unauthorized access to its network. Vendor reported that it had hired a cybersecurity firm to conduct an investigation. Since then Drury has worked closely with Vendor to get updates on its investigation. Over time, Vendor learned that there had been unauthorized access to some, but not all, of the payment card transaction records it collected from reservations made through third-party booking websites. Vendor informed Drury that it was working with the third-party booking websites to identify the specific transaction records involved. Vendor ultimately advised Drury that there had been unauthorized access to payment card transaction records in Vendor's network between December 29, 2017 and March 13, 2019. Drury received a list of the specific transaction records that were involved on May 15, 2019. The information in the transaction records consisted of name, address, payment card number, expiration date, and the card's external verification code.

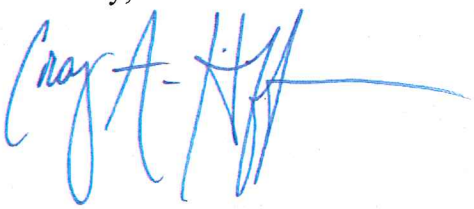
Beginning on May 30, 2019, Drury will mail notification letters via United States Postal Service First-Class Mail to the Washington residents for whom it has a mailing address, in

accordance with RCW § 19.255.010. Drury will provide a supplemental notice that includes a copy of the notification letter and identifies the number of residents to whom it is mailing letters.

Drury does not have a mailing address for every individual whose information may have been involved in this incident. Drury, therefore, is unable to identify the total number of Washington residents whose information may have been subject to unauthorized access. Beginning on May 24, 2019, under RCW § 19.255.010, Drury will provide substitute notification to potentially involved Washington residents by issuing a press release and posting a statement on its website. Copies of the press release and website statement are attached. Drury also has established a dedicated call center that individuals may call with related questions.

To help prevent a similar incident from occurring in the future, Drury will continue to work with Vendor to identify the security enhancements it is implementing. Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Craig A. Hoffman
Partner

Attachments

May 24, 2019

Notice of Data Breach

Drury Hotels values the relationship we have with our guests and understands the importance of protecting their information. We are providing notification regarding a security incident that occurred on the network of one of our service providers. This notice explains the incident, the measures we have taken in response, and some steps you may consider taking in response.

What Happened?
For most hotels, there are two ways to make a reservation – directly with the hotel or indirectly through third party online booking websites (websites run by other companies that compare rooms and rates at different hotels). For reservations that are made through online booking websites, many hotels use a technology service provider to collect the reservation data from the online booking company and enter it into the hotel's property management system. On March 26, 2019, we were notified by the company that provides that service to us and other hotel companies that it was conducting an investigation to determine if there had been unauthorized access to its network. The service provider reported that it had hired a cybersecurity firm to conduct an investigation. Since then Drury Hotels has worked closely with the service provider to get updates on its investigation.

The service provider later advised us that the unauthorized access to transaction records related to reservations in its network began on December 29, 2017 and ended on March 13, 2019. We received a list of the specific transaction records that were involved on May 15, 2019.

What Information Was Involved?
The information in the transaction records that were involved included name, payment card number, expiration date, and the card's external verification code. Some transaction records also included mailing addresses or email addresses. Specific details regarding the reservation itself were not involved. Only transaction records from some third party online booking websites were involved. And only some, not all, of the transaction records from those third party online booking sites were involved.

Reservations that were made directly with Drury Hotels (by calling Drury Hotels or using our website or mobile app) were not involved in this incident.

What You Can Do.
We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information on additional steps you can take can be found below.

What We Are Doing.
We regret that this incident occurred and apologize for any inconvenience. We have been in frequent communication with the service provider since it notified us of the matter and have received confirmation that it has undertaken measures to prevent something like this from happening again. We will continue to work with the service provider to identify the security enhancements it is implementing.

For More Information.
If you have any questions about this matter, please call (800) 382-6291, Monday to Friday, from 8:00 a.m. to 8:00 p.m., Eastern Time. The call center is also open on Saturday, May 25, from 10 a.m. to 6 p.m., Eastern Time.

ADDITIONAL STEPS YOU CAN TAKE

We remind you 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. 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 www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, Massachusetts, North Carolina, or Rhode Island, you may contact and obtain information from your state attorney general at:

- *Connecticut Attorney General's Office*, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

- *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

- *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

- *North Carolina Attorney General's Office*, 9001 Mail Service Center, Raleigh, NC 27699, 1-919-716-6400 / 1-877-566-7226, www.ncdoj.gov

- *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov

If you are a resident of Massachusetts or Rhode Island, note that pursuant to Massachusetts or Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze.

If you are a resident of West Virginia, you have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described below. You also have a right to place a security freeze on your credit report, as described below.

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report 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 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. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, so that no new credit can be opened in your name without the use of a PIN that is issued to you when you initiate a freeze. A security freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a security 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 security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

To request a security freeze, you will need to provide the following information:

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 years, provide 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.)
7. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, or to lift a security freeze for a specified period of time, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to the credit reporting agencies and include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have one business day after receiving your request by toll-free telephone or secure electronic means, or

three business days after receiving your request by mail, to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must submit a request through a toll-free telephone number, a secure electronic means maintained by a credit reporting agency, or by sending a written request via regular, certified, or overnight mail to each of the three credit bureaus and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have one business day after receiving your request by toll-free telephone or secure electronic means, or three business days after receiving your request by mail, to remove the security freeze.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal 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 of your major rights under FCRA. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

Press Release – May 24, 2019

Drury Hotels Announces Third Party Service Provider Security Incident

ST. LOUIS, MO – May 24, 2019 - Drury Hotels has taken measures to address a security incident experienced by a third party technology service provider. The service provider, a company that Drury Hotels (and other hotel companies) uses to collect reservations made by guests on third party online booking websites and enter them into its system, notified Drury that it was investigating unauthorized access to the service provider's network. The service provider later advised us that certain transaction records from some third party online booking sites were accessed during the incident from December 29, 2017 to March 13, 2019. **Reservations that were made directly with Drury Hotels (by calling Drury Hotels or using our website or mobile app) were not involved in this incident.**

What Happened?

For most hotels, there are two ways to make a reservation – directly with the hotel or indirectly through third party online booking websites (websites run by other companies that compare rooms and rates at different hotels). For reservations that are made through online booking websites, many hotels use a technology service provider to collect the reservation data from the online booking company and enter it into the hotel's property management system. On March 26, 2019, we were notified by the company that provides that service to us and other hotel companies that it was conducting an investigation to determine if there had been unauthorized access to its network. The service provider reported that it had hired a cybersecurity firm to conduct an investigation.

What Information Was Involved?

The information in the transaction records that were involved included name, payment card number, expiration date, and the card's external verification code. Some transaction records also included mailing addresses or email addresses. Specific details regarding the reservation itself were not involved. Only transaction records from some third party online booking websites were involved. And only some, not all, of the transaction records from those third party online booking sites were involved.

What You Can Do.

We encourage you to closely review your payment card statements for any unauthorized charges. You should immediately report any such charges to the bank that issued your card. If reported timely, payment card network rules generally provide that cardholders are not responsible for unauthorized charges. Information about this incident and additional steps you can take can be found on the dedicated website Drury Hotels established regarding this incident - https://ide.myidcare.com/druryhotels.

What We Are Doing.

We regret that this incident occurred and apologize for any inconvenience. Since then Drury Hotels has worked closely with the service provider to get updates on its investigation. We received a list of the specific transaction records that were involved on May 15, 2019. For the transaction records that contained a mailing address, Drury Hotels is mailing letters to those individuals. For transaction records without an address that contained an email address, Drury Hotels is sending email notifications to those individuals. And Drury Hotels issued this press release and posted a notification on its website to provide notification to others involved. If you do not receive a notification letter or email, either your information was not involved in this incident or the list from the service provider did not contain your mailing address or email address.

Drury Hotels received confirmation from the service provider that it has undertaken measures to prevent something like this from happening again. We will continue to work with the service provider to identify the security enhancements it is implementing.

For More Information.

If you have any questions about this matter, please call (800) 382-6291, Monday to Friday, from 8:00 a.m. to 8:00 p.m., Eastern Time. The call center is also open on Saturday, May 25, from 10 a.m. to 6 p.m., Eastern Time.

About Drury Hotels Company

Drury Hotels Company is a Missouri-based, family-owned and operated hotel system with more than 150 hotels in 25 states. Drury Hotels' brands include Drury Inn & Suites®, Drury Inn®, Drury Plaza Hotel ®, Drury Suites®, Pear Tree Inn by Drury®, as well as other hotels in the mid-priced hotel segment.