

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

February 24, 2017

VIA EMAIL: SECURITYBREACH@ATG.WA.GOV

Attorney General Bob Ferguson
Washington Office of the Attorney General
1125 Washington St., N.E.
P.O. Box 40100
Olympia, WA 98504

Re: Incident Notification

Dear Attorney General Ferguson:

We are writing on behalf of our client, BENCHMARK, a global hospitality company, to notify you of a security incident that may have involved the payment card information of Washington residents.

After being alerted to a potential security incident at one of the properties Benchmark manages, Benchmark initiated an investigation at that property and identified an unauthorized file designed to capture payment card information as it is routed through its payment processing system. Benchmark immediately hired a leading cybersecurity firm to assist with its investigation across all of its properties. Findings from the investigation show that the malware – which searched for track data including cardholder name, payment card account number, card expiration date, and verification code – was installed on certain devices that process payment card transactions at certain Benchmark managed properties.

Payment cards used at six affected properties from October 23, 2016 to January 1, 2017 may have been affected. The six affected properties (and affected category) along with the specific time frames for each (times vary by location) are identified in the following table.

Atlanta	Chicago	Cincinnati	Cleveland	Columbus	Costa Mesa	Denver
Houston	Los Angeles	New York	Orlando	Philadelphia	Seattle	Washington, DC

Property Name	Location	Category	Time
Doral Arrowwood	Rye Brook, NY	Hotel Front Desk	10/23/16 - 12/30/16
Eaglewood	Itasca, IL	Hotel Front Desk	10/23/16 - 12/31/16
The Chattanooga	Chattanooga, TN	Food & Beverage	10/23/16 - 1/1/17
Willows Lodge	Woodinville, WA	Food & Beverage	10/28/16 - 1/1/17
Turtle Bay Resort	Kahuku-Oahu, HI	Food & Beverage	10/23/16 - 12/22/16
Santa Barbara	Porta Blancu, Nieuwport, Curacao	Hotel Front Desk	10/27/16 - 12/30/16

Benchmark continues to take significant steps to resolve this issue and strengthen the security of its network environment, including resetting all administrator passwords, removing the malware from the network, increasing its firewall security, applying two factor authentication for remote network connections and complete the implementation of point to point encryption and installation of EMV readers at its properties. In addition, the payment card networks have been notified so that they can work with the banks that issued payment cards used during the at-risk time period. Lastly, Benchmark has established a dedicated call center that potentially affected individuals can call with questions regarding the incident.

Benchmark is able to identify a mailing address or email address for some, but not all, potentially affected cardholders. Accordingly, Benchmark is not able to identify the total number of potentially affected Washington residents. Consequently, pursuant to Wash. Rev. Code Ann. §19.255.010, Benchmark is providing substitute notification today to Washington residents who used their payment cards at a food and beverage, or front desk location in an affected property during that property's at risk time frame by posting a statement on its website and issuing a press release. The substitute notification and press release are enclosed. Benchmark believes it will be able to identify the mailing address of some Washington residents who used their payment cards at the front desk of an affected hotel. In accordance with Wash. Rev. Code Ann. §19.255.010, Benchmark will be mailing a letter to these individuals. A copy of the notification letter is enclosed. Notification is being provided in the most expedient time possible and without unreasonable delay following the completion of an investigation by Benchmark to determine the scope of the incident. *See* Wash. Rev. Code Ann. §19.255.010.

Please do not hesitate to contact me if you have any questions regarding this matter.

Attorney General Bob Ferguson
February 24, 2017
Page 3

Sincerely,

A handwritten signature in blue ink, appearing to read "Craig A. Hoffman", with a long horizontal flourish extending to the right.

Craig A. Hoffman
Partner

Enclosures

Benchmark Notifies Customers of Payment Card Incident

February 24, 2017

California residents please click [here](#)

BENCHMARK, a global hospitality company, understands the importance of protecting payment card data. As the management company for the property owners of the Santa Barbara, Doral Arrowwood, Eaglewood Resort & Spa, the Chattanooga, Willows Lodge and Turtle Bay Resort properties, Benchmark is writing on their behalf to notify you of an incident that may involve your payment card information.

After being alerted to a potential security incident at one of the properties we manage, Benchmark initiated an investigation at that property and identified an unauthorized file designed to capture payment card information as it is routed through our payment processing system. We immediately hired a leading cybersecurity firm to assist with our investigation across all of our properties. Findings from the investigation show that the malware – which searched for track data including cardholder name, payment card account number, card expiration date, and verification code – was installed on certain devices that process payment card transactions at certain Benchmark managed properties.

Payment cards used at six affected properties from October 23, 2016 to January 1, 2017 may have been affected. The six affected properties (and affected category) along with the specific time frames for each (times vary by location) are identified in the following table.

Property Name	Location	Category	Time
Doral Arrowwood	Rye Brook, NY	Hotel Front Desk	10/23/16 – 12/30/16
Eaglewood	Itasca, IL	Hotel Front Desk	10/23/16 – 12/31/16
The Chattanooga	Chattanooga, TN	Food & Beverage	10/23/16 – 1/1/17
Willows Lodge	Woodinville, WA	Food & Beverage	10/28/16 – 1/1/17
Turtle Bay Resort	Kahuku-Oahu, HI	Food & Beverage	10/23/16 – 12/22/16
Santa Barbara	Porta Blancu, Nieuwport, Curacao	Hotel Front Desk	10/27/16 – 12/30/16

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

Benchmark has taken measures to contain this incident and eradicate the malware. We continue to work with the cybersecurity firm to further strengthen our security measures including completing the implementation of point to point encryption and installation of EMV readers at our properties. We are also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

We regret any inconvenience this may have caused. If you have questions, please call 844-734-6819 from 9:00 a.m. to 6:00 p.m. Eastern, Monday to Friday.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain 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

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 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.

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

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland) (410) 576-6300 (for calls originating outside Maryland)

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

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

If you are a resident of Massachusetts, note that pursuant to Massachusetts law, you have the right to file and obtain a copy of any police report.

Massachusetts law also allows consumers to request a security freeze. A security freeze prohibits a credit reporting agency from releasing any information from your credit report without written authorization. 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.

The fee for placing a security freeze on a credit report is \$5.00. If you are a victim of identity theft and submit a valid investigative report or complaint with a law enforcement agency, the fee will be waived. In all other instances, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. If you have not been a victim of identity theft, you will need to include payment to the credit reporting agency to place, lift, or remove a security freeze by check, money order, or credit card.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

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

In order 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 (5) 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 three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) 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, you must call or send a written request to the credit reporting agencies by mail 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 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 three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail 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 three (3) business days after receiving your request to remove the security freeze.

FOR IMMEDIATE RELEASE

Benchmark Notifies Customers of Payment Card Incident

The Woodlands, TX– February 24, 2017 – BENCHMARK, a global hospitality company, is providing notice of a payment card incident that may have affected guests of the individually owned Santa Barbara, Doral Arrowwood, Eaglewood Resort & Spa, the Chattanooga, Willows Lodge and Turtle Bay Resort properties that Benchmark manages.

After being alerted to a potential security incident at one of its managed properties, Benchmark initiated an investigation at that property and identified an unauthorized file designed to capture payment card information as it is routed through its payment processing system. Benchmark immediately hired a leading cybersecurity firm to assist with its investigation across all its properties. Findings from the investigation show that the malware – which searched for track data including cardholder name, payment card account number, card expiration date, and verification code – was installed on certain devices that process payment card transactions at certain Benchmark managed properties. A list of the specific time frames, and affected locations at each affected property is located at http://www.benchmarkglobalhospitality.com/protecting_our_guests/?fullsite=false. The website also contains more information on steps guests may take to protect their information.

Guests who used their card at an affected property location during an affected time frame are advised to remain vigilant to the possibility of fraud by reviewing their payment card statements for any unauthorized activity. Guests should immediately report any unauthorized charges to their card issuer because payment card rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of the payment card.

Benchmark has taken measures to contain this incident and eradicate the malware. Benchmark continues to work with the cybersecurity firm to further strengthen its security measures including completing the implementation of point to point encryption and installation of EMV readers at its properties. Benchmark is also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

Benchmark understands the importance of protecting payment card data and regrets any inconvenience this may cause its guests. Guests with questions may call 844-734-6819 from 9:00 a.m. to 6:00 p.m. Eastern, Monday to Friday.

About BENCHMARK, a global hospitality company: Benchmark is a recognized global leader in the management and marketing of resorts, hotels and conference centers. The company's two distinctive portfolios of properties, Benchmark Resorts & Hotels and Gemstone Collection, represent the finest in guest-dedicated hospitality in desirable destinations across the United States, in the Caribbean and Japan.

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and 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 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 9554, 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

[Benchmark letterhead]

[DATE]

[first name][last name]

[address]

[city][state][zip]

Dear [first name][last name]:

BENCHMARK, a global hospitality company, understands the importance of protecting payment card data. As the management company for the property owners of the Santa Barbara, Doral Arrowwood, Eaglewood Resort & Spa, the Chattanooga, Willows Lodge and Turtle Bay Resort properties, Benchmark is writing on their behalf to notify you of an incident that may involve your payment card information.

After being alerted to a potential security incident at one of the properties we manage, Benchmark initiated an investigation at that property and identified an unauthorized file designed to capture payment card information as it is routed through our payment processing system. We immediately hired a leading cybersecurity firm to assist with our investigation across all of our properties. Findings from the investigation show that the malware – which searched for track data including cardholder name, payment card account number, card expiration date, and verification code – was installed on certain devices that process payment card transactions at certain Benchmark managed properties.

Payment cards used at six affected properties from October 23, 2016 to January 1, 2017 may have been affected. The six affected properties (and affected category) along with the specific time frames for each (times vary by location) are identified in the following table.

Property Name	Location	Category	Time
Doral Arrowwood	Rye Brook, NY	Hotel Front Desk	10/23/16 – 12/30/16
Eaglewood	Itasca, IL	Hotel Front Desk	10/23/16 – 12/31/16
The Chattanooga	Chattanooga, TN	Food & Beverage	10/23/16 – 1/1/17
Willows Lodge	Woodinville, WA	Food & Beverage	10/28/16 – 1/1/17
Turtle Bay Resort	Kahuku-Oahu, HI	Food & Beverage	10/23/16 – 12/22/16
Santa Barbara	Porta Blancu, Nieuwport, Curacao	Hotel Front Desk	10/27/16 – 12/30/16

It is always advisable to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized activity. You should immediately report any unauthorized charges to your card issuer because payment card rules generally provide

that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the section that follows this notice for additional steps you may take to protect your information.

Benchmark has taken measures to contain this incident and eradicate the malware. Benchmark continues to work with the cybersecurity firm to further strengthen its security measures including completing the implementation of point to point encryption and installation of EMV readers at its properties. Benchmark is also working with the payment card networks so that the banks that issue payment cards can be made aware and initiate heightened monitoring on the affected cards.

We regret any inconvenience this may have caused. If you have questions, please call 844-734-6819 from 9:00 a.m. to 6:00 p.m. Eastern, Monday to Friday.

Kirk Jones
Chief Financial Officer
BENCHMARK, a global hospitality company

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant by reviewing your account statements and 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 740256, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 9554, 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