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

August 31, 2016

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, Kimpton Hotels & Restaurants, to notify you of a security incident that may have involved the payment card information of Washington residents.

Kimpton received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at one of its hotels. Kimpton immediately began to investigate the report and hired leading cyber security firms to examine its payment card processing system. Findings from the investigation show that malware was installed on servers that processed payment cards used at the restaurants and front desks of certain Kimpton properties.

The malware was designed to search for track data read from the magnetic stripe of a payment card as it was being routed through the affected server. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in a small number of instances it may have found the track that also contains the cardholder name.

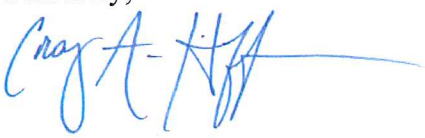
This incident involved cards used at certain restaurants and hotel front desks during the window of February 16, 2016 to July 7, 2016. A list of the affected hotel front desks and restaurants, along with the specific time frames for each (times vary by location) is located at www.kimptonhotels.com/protectingourguests.

Kimpton has taken significant steps to resolve this issue and strengthen the security of its network environment. Measures taken to stop the attack included resetting all enterprise passwords, segmentation efforts, blocking certain network communication attempts and removing affected systems from the network. Law enforcement was notified. 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, Kimpton has established a dedicated call center that potentially affected individuals can call with questions regarding the incident.

For cards used in its restaurants, Kimpton is not able to identify a mailing address or email address for potentially affected cardholders, nor is Kimpton able to identify a mailing address or email address for all individuals who used their card at a front desk. Accordingly, Kimpton is not able to identify the total number of potentially affected Washington residents. Consequently, pursuant to Wash. Rev. Code Ann. §19.255.010, Kimpton Hotels & Restaurants is providing substitute notification today to Washington residents who used their payment cards at a restaurant or hotel front desk in an affected Kimpton location during that location'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. Kimpton 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, Kimpton 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 Kimpton 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.

Sincerely,



Craig A. Hoffman
Partner

Enclosures

Kimpton Hotels & Restaurants Notifies Customers of Payment Card Incident

August 31, 2016

California residents please click here

Kimpton Hotels & Restaurants values the relationship we have with our guests and understands the importance of protecting personal information. We are notifying you of an incident that may involve your payment card information.

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant in one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that malware was installed on servers that processed payment cards used at the restaurants and front desks of some of our hotels. The malware searched for track data read from the magnetic stripe of a payment card as it was being routed through the affected server. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in a small number of instances it may have found the track that also contains the cardholder name.

This incident involved cards used at certain restaurants and hotel front desks from February 16, 2016 to July 7, 2016. A list of the affected hotel front desks and restaurants, along with the specific time frames for each (times vary by location) is located here. We do not have information available to identify the name and address of restaurant guests. We will be mailing letters to those guests who used their card at a front desk during an at risk time frame for whom we have a mailing address.

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.

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and 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 (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, 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.

-more-

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

-more-

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

Kimpton Hotels & Restaurants Notifies Customers of Payment Card Incident

San Francisco, CA – August 31, 2016 – Kimpton Hotels & Restaurants has completed its investigation of the previously announced payment card security incident.

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant in one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that malware was installed on servers that processed payment cards used at the restaurants and front desks of some of our hotels. The malware searched for track data read from the magnetic stripe of a payment card as it was being routed through the affected server. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in a small number of instances it may have found the track that also contains the cardholder name.

This incident involved cards used at certain restaurants and and hotel front desks from February 16, 2016 to July 7, 2016. A list of the affected hotel front desks and restaurants, along with the specific time frames for each (times vary by location) is located at www.kimptonhotels.com/protectingourguests. The site also contains more information on steps guests may take to protect their information. Kimpton Hotels & Restaurants does not have information available to identify the name and address of restaurant guests. We will be mailing letters to those guests who used their card at a front desk during an at risk time frame for whom we have a mailing address.

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.

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and 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 (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

[Kimpton Hotels & Restaurants letterhead]

[DATE]

[first name][last name]
[address]
[city][state][zip]

Dear [first name][last name]:

Kimpton Hotels & Restaurants values the relationship we have with our guests and understands the importance of protecting personal information. We are writing to notify you of an incident that may involve your payment card information.

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant of one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that an unauthorized person installed malware on certain servers that processed payment cards used at some of our hotels. The malware searched for track data read from the magnetic stripe of payment cards as it was being routed through the affected servers. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in some instances it found the track that also contains the cardholder name. We are notifying you because you used your payment card at the front desk of the [affected Kimpton Hotel] between February 16, 2016 and July 7, 2016.

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.

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and 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 (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

Sincerely,

Mike DeFrino
CEO
Kimpton Hotels & Restaurants

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

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

September 16, 2016

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

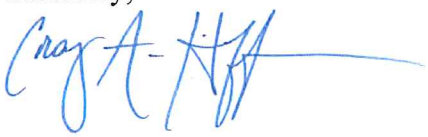
Re: Incident Notification Follow Up

Dear Attorney General Ferguson:

In our letter to you on August 31, 2016 we informed you that our client, Kimpton Hotels & Restaurants, would be providing substitute notification of a payment card incident to Washington residents who used their payment cards at certain restaurants and hotel front desks between February 16, 2016 and July 7, 2016. We further indicated that Kimpton was working to identify the mailing address of certain Washington residents who used their payment cards at the front desk of an affected hotel so that Kimpton could mail notification letters to those individuals in accordance with *Wash. Rev. Code Ann. §19.255.010*. Kimpton has identified 5428 such residents of Washington and notification letters were mailed to those individuals beginning September 9, 2016, in substantially the same form as the attached.

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

Sincerely,



Craig A. Hoffman
Partner

Enclosures

KIMPTON®

HOTELS & RESTAURANTS

September 6, 2016

Kimpton Hotels & Restaurants values the relationship we have with our guests and understands the importance of protecting personal information. We are writing to notify you of an incident that may involve your payment card information.

Kimpton Hotels & Restaurants received a report on July 15, 2016 of unauthorized charges occurring on payment cards after they had been used by guests at the restaurant of one of our hotels. We immediately began to investigate the report and hired leading cyber security firms to examine our payment card processing system. Findings from the investigation show that an unauthorized person installed malware on certain servers that processed payment cards used at some of our hotels. The malware searched for track data read from the magnetic stripe of payment cards as it was being routed through the affected servers. The malware primarily found track data that contained the card number, expiration date, and internal verification code, but in some instances it found the track that also contains the cardholder name. We are notifying you because you used your payment card at the front desk of the Hotel Lumen between February 16, 2016 and July 7, 2016.

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.

We have resolved the issue and continue to work with the cyber security firms to further strengthen our existing security measures. We notified law enforcement and 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 (888) 339-3142 from 9:00 a.m. to 8:00 p.m. EST, Monday to Friday.

Sincerely,

Mike DeFrino
CEO
Kimpton Hotels & Restaurants

KIMPTON®

HOTELS & RESTAURANTS

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