

Noble House Hotels & Resorts Notifies Guests of Payment Card Security Incident

California residents, please [click here for security incident information](#).

Noble House Hotels and Resorts (Noble House) values the relationship it has with its guests and understands the importance of protecting your personal information. Regrettably, an incident occurred that may involve some of your information.

Noble House Hotels & Resorts began an investigation after it was notified by the Secret Service about possible fraudulent activity on the payment card system at one of its properties. It engaged a computer security firm to examine the payment systems at all of the properties it manages for any signs of an issue. Through its investigation, it learned that malware may have been installed on payment processing systems that potentially affected cards swiped at the following hotels, restaurants, and bars during the periods identified:

- Kona Kai Resort & Spa, San Diego, CA, including the Vessel restaurant and the Tiki Bar, from April 25, 2016 - August 3, 2016;
- Little Palm Island Resort & Spa, Florida Keys, FL, including the Little Palm Island Dining Room, from April 25, 2016 - June 8, 2016;
- The Portofino Hotel & Marina, Redondo Beach, CA, including the Baleen Kitchen & Lounge restaurant and the Living Room Bar, from April 26, 2016 - June 8, 2016;
- The Edgewater, Seattle, WA, including the Six Seven restaurant, from April 26, 2016 - August 3, 2016;
- River Terrace Inn, Napa, CA, including the Terrace Café & Wine Bar, from April 25, 2016 - June 8, 2016;
- LaPlaya Beach & Golf Resort, Naples, FL, including the Baleen restaurant and the Tiki Bar, from April 26, 2016 - August 3, 2016;
- Mountain Lodge at Telluride, Telluride, CO, including The View restaurant, from April 26, 2016 - August 5, 2016;
- Hotel Deca, Seattle, WA, from April 25, 2016 - June 8, 2016;
- Blue Mermaid restaurant, San Francisco, CA from April 26, 2016 – August 3, 2016;
- Pescatore restaurant, San Francisco, CA from April 26, 2016 – August 3, 2016..
- Ocean Key Resort, Key West, FL including the Hot Tin Roof Restaurant, Liquid Pool Bar, and Sunset Pier Bar, from April 26, 2016 – June 8, 2016
- Hotel Terra, Teton Village, WY from September 5th, 2016 – September 6th, 2016.
- Teton Mountain Lodge & Spa, Teton Village, WY from September 5th, 2016 – September 6th, 2016.

The information potentially compromised involved data found in the magnetic stripe on payment cards, including payment card number, payment card expiration date, CVV number, and may have included the payment cardholder's name. We have no evidence that any cards used at these hotels, restaurants, or bars outside of the periods identified were affected.

The information potentially compromised by the attack involved Track 1 and Track 2 data found in the magnetic stripe on payment cards. Track 1 data includes name, payment card number, payment card expiration date, and CVV number. Track 2 data does not generally include the payment cardholder name. Unfortunately, because Noble House does not retain this information, it is unable to determine whether Track 1 or Track 2 data was exposed for individual guests.

As soon as our investigation yielded sufficient accurate and reliable information, we started the process of notifying potentially affected guests and providing information about this incident.

If you used a payment card at one of the affected hotels, restaurants, or bars during the dates listed above, we recommend you review your account statements for any unauthorized activity. You should immediately report any unauthorized charges to your financial institution because the major credit card companies generally will not require you to pay fraudulent charges that are reported in a timely manner. If you incurred costs that your financial institution declined to reimburse related to fraudulent charges on a payment card you used at one of the affected hotels, restaurants, and bars, please contact us at the number below. We will reimburse you for any such reasonable, documented costs that your financial institution declined to pay. You may also review the "More Information About Ways to Protect Yourself" below.

We regret any inconvenience or concern this may have caused. If you have any questions, or you need further assistance, please call (866) 877-7528, Monday through Friday between the hours of 9 am and 5 pm EST.

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.