

Sandy B. Garfinkel  
412.566.6868  
sgarfinkel@eckertseamans.com

April 2, 2019

**VIA FIRST CLASS MAIL and FACSIMILE (603-271-2110)**

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

Re: Notice of Data Security Incident

To Whom It May Concern:

My firm represents Key West Hotels, LLC, the current owner of The Key Ambassador Resort Inn (the "Hotel"). I write to inform you of an incident involving a breach of personal information.

On December 13, 2018, the Hotel noticed some unusual activity in its front desk computer system. The Hotel promptly began investigating, retaining a well-known global cyber security firm to perform an assessment of the computer system. Ultimately the Hotel learned that on approximately February 7, 2018, many months prior to Key West Hotels, LLC's purchase of the Hotel, an unauthorized person had gained access to the Hotel's front desk computer system while the Hotel was being operated by a prior owner. Using malware, the intruder was able to gain access to and view guest reservation information. The malware was quickly removed and the system restored so that it could be used safely.

An investigation by a forensic technology expert was conducted for the purpose of determining the scope of the unauthorized activity. On March 8, 2019 it was confirmed that the intruder, using malware, had the ability to view files containing certain guest information during the period of approximately February 7, 2018 through December 13, 2018 (when the suspicious activity was first observed). Although it is unlikely that all guest information contained in the front desk computer system during that period was viewed by the intruder, out of an abundance of caution we are notifying every guest who booked reservations at the Hotel during that period.

The intruder may have viewed computer files that contain guest names, addresses, phone numbers, frequent guest account numbers and partial credit or debit card numbers. In some cases the expiration date of the credit card may have also been included.

As previously noted, upon learning of the incident, the Hotel promptly retained a reputable global cybersecurity firm to examine the system and remove all malware. Improvements and

STATE OF NH  
DEPT OF JUSTICE  
2019 APR -5 PM 12:25

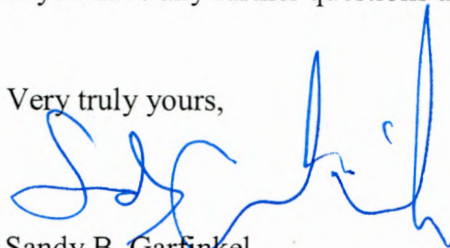
technical safeguards to system security have been implemented. The Hotel also notified federal law enforcement officials of the incident. In addition, the Hotel is upgrading its system security and providing employee training to reinforce vigilance against cyber threats of this type.

The Hotel does not have contact information for approximately 60% of the total number of affected individuals. The Hotel will provide direct notification by letter to affected individuals that are known to reside in New Hampshire and will undertake to provide substitute notification within New Hampshire as well.

Enclosed is a copy of a form of notification letter which will be sent to all of the affected individuals, including the individual residing in New Hampshire on or about April 2, 2019. We have also enclosed the text of the substitute notification which will be posted on the Hotel's website and sent to state-wide media contemporaneously with the mailing of the letters.

If you have any further questions about the incident, do not hesitate to contact me.

Very truly yours,



Sandy B. Garfinkel

*Enclosures*

Key Ambassador Resort Inn  
Key West, FL

<<Date>> (Format: Month Day, Year)

<<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>  
<<Address1>>  
<<Address2>>  
<<City>>, <<State>> <<Zip>>

## NOTICE OF DATA SECURITY INCIDENT

Dear <<FirstName>> <<LastName>>,

Key West Hotels, LLC, the current owner of the **Key Ambassador Resort Inn** (the "Hotel") is writing to inform you of an incident that may affect the security of your personal information. We are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so.

The privacy and protection of our guests' information is a matter we take extremely seriously. We apologize for any concern or inconvenience that may be caused by this incident and we recommend that you closely review this letter for steps that you may take to further protect yourself against any potential misuse of your information.

### What Happened?

On December 13, 2018, the Hotel noticed some unusual activity on its front desk computer system. The Hotel promptly began investigating, retaining a well-known global cyber security firm to perform an assessment of the computer system. Ultimately the Hotel learned that on approximately February 7, 2018, many months prior to Key West Hotels, LLC's purchase of the Hotel, an unauthorized person had gained access to the Hotel's front desk computer system while the Hotel was being operated by a prior owner. Using malware, the intruder was able to gain access to and view guest reservation information. The malware was quickly removed, and the system was restored so that it could be used safely.

An investigation by a forensic technology expert was conducted for the purpose of determining the scope of the unauthorized activity. In early March 2019, it was confirmed that the intruder, using malware, had the ability to view files containing certain guest information during the period of approximately February 7, 2018, through December 13, 2018 (when the suspicious activity was first observed). Although it is unlikely that all guest information contained in the front desk computer system during that period was viewed by the intruder, out of an abundance of caution, we are notifying every guest who booked reservations at the Hotel during that period.

### What Information Was Involved?

The intruder may have viewed computer files that contain guest names, addresses, phone numbers, frequent guest account numbers and partial credit or debit card numbers. In some cases, the expiration date of the credit card may have also been included.

### What Are We Doing?

As previously noted, upon learning of the incident, the Hotel promptly retained a reputable global cybersecurity firm to examine the system and remove all malware. Improvements and technical safeguards to system security have been implemented. The Hotel also notified federal law enforcement officials of the incident.

**What Can You Do?**

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring your free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges if they are reported in a timely fashion.

**For More Information**

We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline to assist you with questions regarding this incident and steps you can take to protect yourself against identity theft and fraud. We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please call 1-866-656-0426, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Jacqueline Loring, General Manager  
Key Ambassador Resort Inn, Key West, Florida

## ADDITIONAL RESOURCES

### Contact information for the three nationwide credit reporting agencies is:

**Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19022, [www.transunion.com](http://www.transunion.com), 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

### **For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:**

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alert.** You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

**Security Freeze.** You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**For Maryland residents:** You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), 1-888-743-0023.

**For North Carolina residents:** You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), 1-919-716-6400.

**For California Residents:** Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

**For Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**For Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**For Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400

**For New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**Reporting of identity theft and obtaining a police report.**

**For Iowa residents:** You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

**For Massachusetts residents:** You have the right to obtain a police report if you are a victim of identity theft.

**For Oregon residents:** You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

## NOTICE OF DATA SECURITY INCIDENT

Key West Hotels, LLC, the current owner of *The Key Ambassador Resort Inn* (the “Hotel”) wishes to inform you of an incident that may affect the security of your personal information. We are providing you with information and access to resources so that you can better protect against the possibility of misuse of your personal information, should you feel it appropriate to do so.

The privacy and protection of our guests’ information is a matter we take extremely seriously. We apologize for any concern or inconvenience that may be caused by this incident and we recommend that you closely review this letter for steps that you may take to further protect yourself against any potential misuse of your information

### **What Happened?**

On December 13, 2018, the Hotel noticed some unusual activity in its front desk computer system. The Hotel promptly began investigating, retaining a well-known global cyber security firm to perform an assessment of the computer system. Ultimately the Hotel learned that on approximately February 7, 2018, many months prior to Key West Hotels, LLC’s purchase of the Hotel, an unauthorized person had gained access to the Hotel’s front desk computer system while the Hotel was being operated by a prior owner. Using malware, the intruder was able to gain access to and view guest reservation information. The malware was quickly removed and the system restored so that it could be used safely.

An investigation by a forensic technology expert was conducted for the purpose of determining the scope of the unauthorized activity. In early March of 2019 it was confirmed that the intruder, using malware, had the ability to view files containing certain guest information during the period of approximately February 7, 2018 through December 13, 2018 (when the suspicious activity was first observed). Although it is unlikely that all guest information contained in the front desk computer system during that period was viewed by the intruder, out of an abundance of caution, we are notifying every guest who booked reservations at the Hotel during that period.

### **What Information Was Involved?**

The intruder may have viewed computer files that contain guest names, addresses, phone numbers, frequent guest account numbers and partial credit or debit card numbers. In some cases the expiration date of the credit card may have also been included.

### **What Are We Doing?**

As previously noted, upon learning of the incident, the Hotel promptly retained a reputable global cybersecurity firm to examine the system and remove all malware. Improvements and technical safeguards to system security have been implemented. The Hotel also notified federal law enforcement officials of the incident.

### **What Can You Do?**

You should remain vigilant for incidents of fraud and identity theft by regularly reviewing your account statements and monitoring free credit reports for any unauthorized activity. If you discover any suspicious or unusual activity on your accounts, be sure to report it immediately to your financial institutions, as major credit card companies have rules that restrict them from requiring you to pay for fraudulent charges if they are reported in a timely fashion.

### **For More Information**

We understand that you may have questions about this incident that are not addressed in this letter. We have established a confidential, toll-free hotline to assist you with questions regarding this incident, the free services we are making available, and steps you can take to protect yourself against identity theft and fraud. We apologize for any inconvenience caused by this incident. If you have any questions regarding this incident or if you desire further information or assistance, please contact our call center at 1-866-656-0426.

---

### **ADDITIONAL RESOURCES**

#### **Contact information for the three nationwide credit reporting agencies is:**

**Equifax**, PO Box 740241, Atlanta, GA 30374, [www.equifax.com](http://www.equifax.com), 1-800-685-1111

**Experian**, PO Box 2104, Allen, TX 75013, [www.experian.com](http://www.experian.com), 1-888-397-3742

**TransUnion**, PO Box 2000, Chester, PA 19022, [www.transunion.com](http://www.transunion.com), 1-800-888-4213

**Free Credit Report.** It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit [www.annualcreditreport.com](http://www.annualcreditreport.com) or call toll free at 1-877-322-8228.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at [www.consumer.ftc.gov](http://www.consumer.ftc.gov)) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

**For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents:** You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

**Fraud Alert.** You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. A fraud alert tells creditors to follow certain procedures, including contacting you before they open any new accounts or change your existing accounts.



For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit.

**Security Freeze.** You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue.

**Federal Trade Commission and State Attorneys General Offices.** 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, [www.ftc.gov/bcp/edu/microsites/idtheft/](http://www.ftc.gov/bcp/edu/microsites/idtheft/), 1-877-IDTHEFT (438-4338).

**California Residents:** Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

**Kentucky Residents:** Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, [www.ag.ky.gov](http://www.ag.ky.gov), Telephone: 1-502-696-5300.

**Maryland Residents:** Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, [www.oag.state.md.us/Consumer](http://www.oag.state.md.us/Consumer), Telephone: 1-888-743-0023.

**New Mexico Residents:** You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under

the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting [www.consumerfinance.gov/f/201504\\_cfpb\\_summary\\_your-rights-under-fcra.pdf](http://www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf), or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

**North Carolina Residents:** Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, [www.ncdoj.gov](http://www.ncdoj.gov), Telephone: 1-919-716-6400.

**Oregon Residents:** Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, [www.doj.state.or.us/](http://www.doj.state.or.us/), Telephone: 877-877-9392

**Rhode Island Residents:** Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, [www.riag.ri.gov](http://www.riag.ri.gov), Telephone: 401-274-4400