

Best American Hospitality Corp.'s Notification Regarding Stolen Payment Cards at Some Restaurants it Manages (Some Shoney's® Corporate-Owned Restaurants)

Best American Hospitality Corp. commenced an investigation after receiving a report that some payment card numbers that were used at restaurant locations it manages and operates (some of Shoney's corporate affiliated restaurants) had been stolen. Best American Hospitality Corp. hired Kroll Cyber Security, LLC, a leading cyber security investigation firm, to examine the payment card processing systems for all restaurants on its network.

Kroll's findings show that malware was installed remotely on point of sale equipment that processed payment cards used at some of the restaurants. The malware searched for track data (cardholder name, card number, expiration date, and internal verification code) read from the magnetic stripe of a payment card as it was being routed through the affected computer.

Based on the investigation, Kroll determined that some of the restaurants were subject to initial data breach from December 27, 2016 (the date of first breach varies by location), until the malware was contained on March 6, 2017. In some instances, the malware appears to have identified data from the card's magnetic stripe that included the cardholder name and number and in other instances the card data identified by the malware did not appear to include the cardholder name. It is possible that not every cardholder name was identified.

A list of the affected restaurants, along with the earliest date of first breach for each restaurant is below.

Earliest Date	Address	City	State	ZIP
2016-12-27	1307 North Main Street	Summerville	SC	29483
2016-12-27	407 Thompson Lane	Nashville	TN	37211
2016-12-27	791 North Second Street	Clarksville	TN	37040
2017-01-11	2225 Carmack Blvd	Columbia	TN	38401
2017-01-11	880 South Jefferson Ave.	Cookeville	TN	38501
2016-12-27	420 Westbank Expressway	Gretna	LA	70053
2016-12-27	110 Interstate Drive	Nashville	TN	37206
2016-12-27	365 White Bridge Pike	Nashville	TN	37209
2016-12-27	1306 Hwy 96 East	Franklin	TN	37064
2016-12-27	2003 Memorial Blvd	Springfield	TN	37172
2016-12-27	546 Donelson Pike	Nashville	TN	37214
2017-01-11	1950 S. Church Street	Murfreesboro	TN	37130
2017-01-11	1302 West Walnut Avenue	Dalton	GA	30720
2017-01-11	2227 Woodward Avenue	Muscle Shoals	AL	35661
2016-12-27	6121 Highway 49	Hattiesburg	MS	39401
2017-01-11	3313 Pemberton Square Blvd	Vicksburg	MS	39180
2016-12-27	312 S. 16th Avenue	Laurel	MS	39440
2016-12-27	2645 McGavock Pike	Nashville	TN	37214
2017-01-11	2124 North Locust Avenue	Lawrenceburg	TN	38464
2016-12-27	307 Long Hollow Pike	Goodlettsville	TN	37072
2016-12-27	3083 Wilma Rudolph Blvd.	Clarksville	TN	37040
2016-12-27	105 Kimball Crossing Dr	Kimball	TN	37347

2016-12-27	2673 Lee Highway	Troutville	VA	24175
2016-12-27	26 Sergeant Prentiss Drive	Natchez	MS	39120
2017-01-11	500 Springridge Road.	Clinton	MS	39056
2016-12-27	415 W Interstate Drive	Jennings	LA	70546
2016-12-27	1950 West Hwy 76	Branson	MO	65616
2016-12-31	101 Bluefish Dr Suite 105	Panama City Beach	FL	32413
2016-12-30	1805 North Kings Highway	Myrtle Beach	SC	29577
2016-12-28	1206 South Kings Highway	Myrtle Beach	SC	29577
2016-12-27	2318 Shallowford Village Dr	Chattanooga	TN	37421
2017-01-11	222 W. Service Rd	West Memphis	AR	72301
2017-01-11	5829 Highway 70 (Summer Ave)	Memphis	TN	38134
2017-01-11	3081 Covington Pike	Memphis	TN	38128
2017-01-09	2771 Highway 82 East	Greenville	MS	38703
2017-01-11	1526 Sunset Drive	Grenada	MS	38901
2017-01-11	12204 S. Apopka Vineland Rd	Orlando	FL	32836

Best American Hospitality Corp. has been working with Kroll Cyber Security, LLC to review its security measures, confirm that this issue has been remediated, and evaluate ways to enhance Best American Hospitality Corp.'s security measures. Best American Hospitality Corp. is 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.

The following are some steps guests may take to protect their information.

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. 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.

It is also advisable to check your credit report with credit bureaus including Equifax, Transunion and Experian, which offer free credit reports annually. You can also obtain a free credit report at <https://www.annualcreditreport.com>.

Equifax
 Phone: 800-685-1111
 P.O. Box 740256
 Atlanta, Georgia 30348
www.equifax.com

Experian
 Phone: 888-397-3742
 P.O. Box 9554
 Allen, Texas 75013
www.experian.com

Transunion
 Phone: 888-909-8872
 P.O. Box 105281
 Atlanta, GA 30348-5281
www.transunion.com

Even if you do not find any suspicious activity on your initial credit reports, the Federal Trade Commission (FTC) recommends that you check your credit reports periodically. Thieves may hold stolen information to use at different times. Checking your credit reports periodically can help you spot problems and address them quickly. If you find suspicious activity on your credit reports or have reason to believe your information is being misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. 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.

You can place a fraud alert on your credit file. A fraud alert tells creditors to contact you before they open any new accounts or change your existing accounts. Call any one of the three major credit bureaus. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts. The initial fraud alert stays on your credit report for 90 days. You can renew it after 90 days.

You also may want to consider contacting the major credit bureaus to place a credit freeze on your credit file. A credit freeze means potential creditors cannot get your credit report. That makes it less likely that an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law.

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.

Find your state Attorney General's office at www.naag.org.

If you should have any questions regarding this notice, please contact us at info@bestamericanhospitality.com.