

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) AND OVERNIGHT MAIL

Attorney General Bob Ferguson
Office of the Washington Attorney General
Consumer Protection Division
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

Re: Incident Notification

Dear Attorney General Ferguson:

Our client, Roberts Hawaii, submits this notice after learning of a security incident that may have involved personal information for Washington residents. Roberts Hawaii received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on its website. Roberts Hawaii immediately initiated an investigation and engaged a leading cyber security firm to examine their website network.

The investigation determined that an unauthorized person gained access to the web server for two of Roberts Hawaii's sites (robertshawaii.com, airportwaikikishuttle.com) and installed code that was designed to copy information entered during the checkout process, including, name, address, email address, phone number, payment card number, expiration date and card security code. Information from purchases made between July 30, 2015 and December 14, 2016 may have been affected.

Roberts Hawaii provided written notification via U.S. Mail on February 24, 2017, to 1178 Washington residents in accordance with Wash. Rev. Code § 19.255.010 in substantially the same form as the letter attached hereto.¹ Notice is being provided as expeditiously as practicable and without unreasonable delay. Roberts Hawaii has established a dedicated call center that potentially affected individuals can contact with questions. Roberts Hawaii is also

¹ This report is not, and does not constitute, a waiver of personal jurisdiction.

Attorney General Bob Ferguson

February 24, 2017

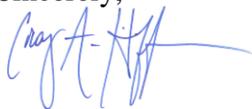
Page 2

recommending that potentially affected individuals remain vigilant to the possibility of fraud by reviewing their account statements and credit reports for unauthorized activity.

Roberts Hawaii has stopped the incident, removed the unauthorized code, and is taking steps to further strengthen the security of its websites to help prevent a similar incident from happening in the future.

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

Sincerely,



Craig A. Hoffman

Enclosure



Return Mail Processing
P.O. Box 399
Claysburg, PA 16625-0399



123456

##C5920-L01-0123456

TO THE ESTATE OF
SAMPLE A SAMPLE
APT ABC

123456



123 ANY ST
ANYTOWN US 12345-6789

February XX, 2017

Dear To the Estate of Sample A Sample,

Roberts Hawaii values the relationship we have with our customers and understands the importance of protecting payment card information. We are writing to inform you about an incident that may involve some of that information.

Roberts Hawaii received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on our website. We immediately initiated an investigation and engaged a leading cyber security firm to examine our website network. The investigation determined that an unauthorized person gained access to the web server for robertshawaii.com and airportwaikikishuttle.com and installed code that was designed to copy information entered during the checkout process, including, name, address, email address, phone number, payment card number, expiration date and card security code. Information from purchases made between July 30, 2015 and December 14, 2016 may have been affected. You are being notified because you placed an order through one of these websites (robertshawaii.com, airportwaikikishuttle.com) using the payment card ending in XXXX during this time period.

Caring for our customers is a top priority for Roberts Hawaii, and we worked swiftly to address this situation. We have stopped the incident, removed the unauthorized code, and are taking steps to further strengthen the security of our website to help prevent this from happening in the future. We encourage you to remain vigilant for incidents of fraud and identity theft. You should review your payment card account statements closely and report any unauthorized charges to your card issuer immediately because card network rules generally provide that cardholders are not responsible for unauthorized charges that are reported promptly. The phone number to call is usually on the back of your payment card.

Your confidence and trust are important to us, and we sincerely apologize for any inconvenience or concern this may have caused. If you have questions, please call (877) 235-0796, Monday through Friday, from 6:00 a.m. to 4:00 p.m. PST (Closed on U.S. observed holidays), and provide reference number 3644013117 when calling. Thank you for your patience and support.

Sincerely,

Percy Higashi
President

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



Return Mail Processing
P.O. Box 399
Claysburg, PA 16625-0399



123456

123456
##C5920-L01-0123456
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN US 12345-6789



February XX, 2017

Dear Sample A Sample,

Roberts Hawaii values the relationship we have with our customers and understands the importance of protecting payment card information. We are writing to inform you about an incident that may involve some of that information.

Roberts Hawaii received reports from several customers of fraudulent charges appearing on their payment cards shortly after they were used to make a purchase on our website. We immediately initiated an investigation and engaged a leading cyber security firm to examine our website network. The investigation determined that an unauthorized person gained access to the web server for robertshawaii.com and airportwaikikishuttle.com and installed code that was designed to copy information entered during the checkout process, including, name, address, email address, phone number, payment card number, expiration date and card security code. Information from purchases made between July 30, 2015 and December 14, 2016 may have been affected. You are being notified because you placed an order through one of these websites (robertshawaii.com, airportwaikikishuttle.com) using the payment card ending in XXXX during this time period.

Caring for our customers is a top priority for Roberts Hawaii, and we worked swiftly to address this situation. We have stopped the incident, removed the unauthorized code, and are taking steps to further strengthen the security of our website to help prevent this from happening in the future. We encourage you to remain vigilant for incidents of fraud and identity theft. You should review your payment card account statements closely and report any unauthorized charges to your card issuer immediately because card network rules generally provide that cardholders are not responsible for unauthorized charges that are reported promptly. The phone number to call is usually on the back of your payment card.

Your confidence and trust are important to us, and we sincerely apologize for any inconvenience or concern this may have caused. If you have questions, please call (877) 235-0796, Monday through Friday, from 6:00 a.m. to 4:00 p.m. PST (Closed on U.S. observed holidays), and provide reference number 3644013117 when calling. Thank you for your patience and support.

Sincerely,

Percy Higashi
President

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