MULLEN COUGHLIN

Ryan Loughlin, Esquire
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.legal

1275 Drummers Lane, Suite 300
Wayne, PA 19087

November 21, 2016

VIA U.S. MAIL

Attorney General Joseph Foster
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concrod, NH 03301

Re: Notice of Data Security Incident

Mr. Foster:

We represent BWTX Associates, 4408 Spricewood Springs Road, Austin, TX 78759 ("BWTX"), and are writing to notify you of a data security incident that may affect the security of payment card information of one (1) New Hampshire resident. The investigation into this incident is ongoing and will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, BWTX does not waive any rights or defenses regarding the applicability of New Hampshire law or personal jurisdiction.

Nature of the Cyber Security Incident

BWTX recently began investigating unusual activity reported by its credit card processor. Leading third party forensic experts were retained to assist BWTX with this investigation and to determine what happened and who may be impacted. On or around September 15, 2016, malicious files were identified on a BWTX device used to process payment information for guests' hotel bookings. Upon identifying these files, BWTX quickly removed and replaced the device to better prevent any further risk to payment information processed on this device. The investigation has since determined that the malicious files collected payment card information provided to BWTX between April 1, 2016 and September 15, 2016. The information collected included the cardholder's name, card number, expiration date and CVV.

Notice to New Hampshire Resident

In early October 2016, BWTX's forensic experts completed their review of the BWTX device used to process payment information and the file containing guest data generated by the malware.

BWTX then moved to identify the guests who may be impacted by this incident and to provide them with notice of this incident.

On November 21, 2016, BWTX will begin mailing notice letters to potentially affected individuals which includes one (1) New Hampshire resident. The notice will be provided in substantially the same form as the letter attached here as ***Exhibit A.***

Other Steps Taken

BWTX is providing potentially affected individuals with information on how to protect against identity theft and fraud, including a recommendation to review credit card statements for any suspicious activity, information on how to contact the Federal Trade Commission, the state attorney general, and law enforcement to report any attempted or actual identity theft and fraud. In addition to providing notice of this incident to you, BWTX is providing written notice of this incident to other state regulators where required.

Contact Information

Should you have any questions regarding this notification or other aspects of the cyber security incident, please contact me at (267) 930-4786.

Very Truly Yours,

Ryan Loughlin of
MULLEN COUGHLIN LLC

Enclosure

EXHIBIT A

<<MemberFirstName>> <<MemberLastName>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip Code>>

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

RE: Notice of Data Breach

Dear <<MemberFirstName>> <<MemberLastName>>,

BWTX Associates ("BWTX") is writing regarding a recent data security incident that may impact certain payment card information used by you. We wanted to provide you with information about this incident, our response and steps you can take to prevent fraud, should you feel it necessary to do so.

What Happened? We recently began investigating unusual activity reported by our credit card processor. Leading third party forensic experts were retained to assist us with this investigation and to determine what happened and who may be impacted. On or around September 15, 2016, malicious files were identified on a BWTX device used to process payment information for guests' hotel bookings. Upon identifying these files, BWTX quickly removed and replaced the device to help prevent further risk to payment information processed on this device. The investigation has since determined that the files collected payment card information processed on the device.

What Information Was Involved? The investigation has determined that the malicious files collected payment card information provided to BWTX between April 1, 2016 and September 15, 2016. This information collected included the cardholder's name, card number, expiration date and CVV.

What We Are Doing. BWTX takes the security of your personal information very seriously. We have removed the malicious files and replaced the impacted device so that credit or debit cards used after September 15, 2016 are not at risk from files involved in this incident. We are also taking steps to further enhance the security of our systems to better protect against future incidents. We are providing notice of this incident to those who may be impacted so that they can take steps to prevent against possible fraud, should they feel it is necessary to do so. We will also be notifying certain state regulators about this incident.

What You Can Do. You can stay vigilant by reviewing your credit card statements for any suspicious charges. You can also review the enclosed Steps You Can Take to Protect Against Identity Theft and Fraud which includes guidance on steps you can take to better protect against the possibility of fraud and identify theft.

For More Information. If you have questions or concerns that are not addressed in this notice letter, you may call the dedicated call center we've established regarding this incident. You can call the call center at 1-855-366-0141. The call center is available Monday through Friday, 9:00 a.m. to 6:00 p.m. E.S.T (excluding U.S. holidays).

We take the privacy of your personal information seriously. We sincerely regret any inconvenience or concern this incident has caused you. The security of your information is a priority to us and we have taken precautionary measures to better prevent something like this from happening again.

Sincerely,

Jeffrey Kolessar

Jeffrey Kolessar
Member

9300RY-1116

Steps You Can Take to Protect Against Identity Theft and Fraud

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

At no charge, you can also have these credit bureaus place a "fraud alert" on your file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. Note, however, that because it tells creditors to follow certain procedures to protect you, it may also delay your ability to obtain credit while the agency verifies your identity. As soon as one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file. Should you wish to place a fraud alert, or should you have any questions regarding your credit report, please contact any one of the agencies listed below.

Equifax	Experian	TransUnion
P.O. Box 105069	P.O. Box 2002	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
800-525-6285	888-397-3742	800-680-7289
www.equifax.com	www.experian.com	www.transunion.com

You may also place a security freeze on your credit reports. A security freeze prohibits a credit bureau from releasing any information from a consumer's credit report without the consumer's written authorization. However, please be advised 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. If you have been a victim of identity theft, and you provide the credit bureau with a valid police report, it cannot charge you to place, list or remove a security freeze. In all other cases, a credit bureau may charge you a fee to place, temporarily lift, or permanently remove a security freeze. You will need to place a security freeze separately with each of the three major credit bureaus listed above if you wish to place a freeze on all of your credit files. To find out more on how to place a security freeze, you can use the following contact information:

Equifax Security Freeze	Experian Security Freeze	TransUnion
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022-2000
1-800-685-1111	1-888-397-3742	1-888-909-8872
(NY residents please call 1-800-349-9960)	www.experian.com/freeze/center.html	www.transunion.com/credit-freeze
https://www.freeze.equifax.com		

You can further educate yourself regarding identity theft, fraud alerts, and the steps you can take to protect yourself, by contacting the Federal Trade Commission or your state Attorney General. **For North Carolina residents**, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-919-716-6400; www.ncdoj.gov. **For Maryland residents**, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 1-888-743-0023; www.oag.state.md.us. The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. Instances of known or suspected identity theft should also be reported to law enforcement. This notice has not been delayed by law enforcement.