Shawn E. Tuma
Direct Dial: 972.324.0317
stuma@spencerfane.com

July 28, 2020

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Re: Notification of Data Security Incident

Dear Attorney General Gordon J. MacDonald:

Be advised that the undersigned and this law firm have been retained to represent Everything Kitchens, LLC ("Everything Kitchens") in connection with the data security incident described below. Everything Kitchens is located at 6820 W. Kings Street, Springfield, MO 65802 and provides kitchenware and appliances to its customers.

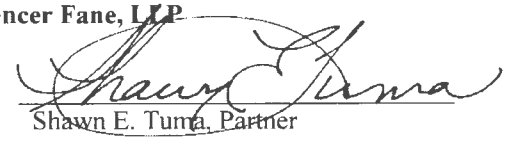
On May 28, 2020, Everything Kitchens determined that criminal hackers executed a sophisticated cyber-attack on its computer systems which resulted in the attackers gaining access to the personal information of a small number of its customers who used debit or credit cards as a form of payment on May 28, 2020, including names, addresses, email address, telephone numbers, credit card numbers, credit card expiration dates, and credit card verification numbers. No Social Security numbers were compromised as a result of this attack. Prior to this incident, Everything Kitchens had implemented a Sucuri edge-protection firewall on its public-facing site, in addition to its hosting provider, Nexcess, having its own hardware firewall. Everything Kitchens' site runs on Magento 1 and was regularly updated with the latest SUPEE security patches from the vendor. The entire public-facing codebase of the Magento 1 site was under strict source control, using monitored uncommitted files and Git repository commits. In addition, the administrative side of Everything Kitchens' site had an .htauth server level password protection, on top of the administrative panel authorization, which was whitelisted to Everything Kitchens' corporate intellectual property.

Upon learning of this incident, Everything Kitchens immediately began addressing the issue, using industry best practices and professionals who specialize in these matters. In particular, Everything Kitchens swiftly secured the server and cleaned up all malicious code, scanned the rest of the environment for malware as well as verified security patch compliance. Everything Kitchens then performed full forensics of the breach event and implemented multiple security layers to prevent further malicious activity. Since the incident, Everything Kitchens has reworked its .htauth server level password protection, removed all whitelists, installed recently released Magento 1 SUPEE, eliminated the ability for customer exports, performed a full security audit and virus scan of the server, and is in the process of setting up Iframe payments through Braintree, so credit card track data cannot be compromised in transit.

Everything Kitchens notified one (1) New Hampshire resident of this incident on July 8, 2020, via U.S. mail and has partnered with ID Experts, to make available at no cost to affected individuals its MyIDCare identity theft protection solution. The MyIDCare solution includes one year of credit monitoring and identify theft protection services.

A sample copy of the notice sent to the New Hampshire resident is enclosed.

Respectfully,
Spencer Fane, LLP

By: 
Shawn E. Tuma, Partner

Enclosures:
Notice of Data Breach

Everything Kitchens

www.everythingkitchens.com

6820 West Kings Street, Springfield MO 65802
P: 866.852.4268
F: 417.887.0779

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
https://app.myidcare.com/account-creation/protect
Enrollment Code:
<<XXXXXXXX>>

<<Date>>

Notice of Data Incident

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of an incident that affected Everything Kitchens and involved your personal information.

What Happened?
On May 28, 2020, we determined that criminal hackers executed a sophisticated cyber attack on our computer systems which resulted in the attackers gaining access to the personal information of a small number of our customers who used debit or credit cards as a form of payment on May 28, 2020. We are providing this notice because our records indicate that your payment card may have been compromised during this attack. We are working hard and increasing our efforts to better safeguard your personal data that is in our custody and protect it from future incidents.

What Information Was Involved?
The personal information compromised during this attack include names, addresses, email address, telephone numbers, credit card numbers, credit card expiration dates, and credit card verification numbers. No Social Security numbers were compromised as a result of this attack.

At this time, there is no indication that your personal information has been misused. However, our investigation is ongoing.

What We Are Doing.
Everything Kitchens values your privacy and the trust you place in us. We regularly update and strengthen our systems and processes to help prevent unauthorized access. Upon learning of this incident, we immediately began addressing the issue, using industry best practices and professionals who specialize in these matters. In particular, we swiftly secured the server and cleaned up all malicious code, scanned the rest of the environment for malware as well as verified

security patch compliance. We then performed full forensics of the breach event and implemented multiple security layers to prevent further malicious activity. We will continue to exercise vigilance and use what we have learned from this incident to help safeguard your data.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do.
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is May 26, 2021.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering and to remain vigilant in protecting your personal information. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

We are also providing you with the attached Recommended Steps document that includes additional steps you may take to help protect your personal information.

For More Information.
We value the security and privacy of your information and we apologize for any inconvenience or concern caused by this incident. Our relationship with you, your confidence in our ability to safeguard your personal information, and your peace of mind are very important to us.

If you have any questions or need additional information about this notice, please feel free to give us a call at 866-852-4268.

Sincerely,

Lucas Forrest, CTO
Everything Kitchens LLC

(Enclosure)

MyIDCare

Recommended Steps to help Protect your Information

1. Website and Enrollment. Go to https://app.myidcare.com/account-creation/protect and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.

2. Activate the credit monitoring provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.

3. Telephone. Contact MyIDCare at 1-800-939-4170 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

4. Review your credit reports. We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General in your State.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (www.oag.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, 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, 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, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

New York Residents: the Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, 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/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.