



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

RECEIVED

MAY 07 2019

CONSUMER PROTECTION

Ryan C. Loughlin
Office: 267-930-4786
Fax: 267-930-4771
Email: rloughlin@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

April 30, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Privacy Event

Dear Attorney General Gordon J. MacDonald:

We represent Tacony Corporation located at 1760 Gilsinn Lane, Fenton, MO 63026 and write to notify your office of an incident that may affect the security of certain payment card information relating to two (2) New Hampshire residents. The investigation into this matter is ongoing, and this notice will be supplemented with any new significant facts learned subsequent to its submission. By providing this notice, Tacony Corporation does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

Tacony Corporation owns and operates the website www.amazingdesigns.com. On March 12, 2019, Tacony Corporation confirmed that code inserted into its online store, www.amazingdesigns.com, was capable of capturing customer payment card information. Working with third-party forensic investigators, Tacony Corporation investigated the nature of the unknown code. The investigation revealed that the code was capable of collecting customer payment information entered between June 7, 2018 and February 4, 2019. The code has been removed and Tacony Corporation remains vigilant for any further issues with its online payment process.

The information that could have been captured by the code includes name, address, credit card number, expiration date and associated security code information.

Notice to New Hampshire Residents

Beginning on April 30, 2019, Tacony Corporation provided written notice of this incident to affected individuals, which includes two (2) New Hampshire residents. Written notice is being provided in substantially the same form as the letter attached here as *Exhibit A*.

Attorney General Gordon J. MacDonald
April 30, 2019
Page 2

Other Steps Taken and To Be Taken

Upon discovering the event, Tacony Corporation moved quickly to investigate and respond to the incident, assess the security of www.amazingdesigns.com, and notify potentially affected individuals. While Tacony Corporation has measures in place to protect information in its systems, the organization is reviewing its existing policies and working to implement additional safeguards.

Tacony Corporation is providing potentially affected individuals access to 12 months of credit monitoring and identity restoration services, through Kroll. Additionally, Tacony Corporation is providing impacted individuals with guidance on how to better protect against identity theft and fraud, including advising individuals to report any suspected incidents of identity theft or fraud to their credit card company and/or bank. Tacony Corporation is providing individuals with information on how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud.

Contact Information

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

Very truly yours,



Ryan C. Loughlin of
MULLEN COUGHLIN LLC

RCL:jgi
Enclosure

EXHIBIT A



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

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

Dear <<FirstName>> <<MiddleName>> <<LastName>> <<NameSuffix>>,

Amazing Designs writes to inform you of a recent incident that may impact some of your payment card information. We are providing you with information about the incident, our response, and steps you may take, should you feel it necessary to do so.

What Happened? On March 12, 2019 we confirmed that code inserted into our online store, www.amazingdesigns.com, was capable of capturing customer payment card information. Working with third-party forensic investigators, Amazing Designs, along with its parent company Tacony Corporation, investigated the nature of the unknown code. The investigation revealed that the code was capable of collecting customer payment information entered between June 7, 2018 and February 4, 2019. The code has been removed and we remain vigilant for any further issues with our online payment process.

What Information was Involved? Our investigation determined that the code was capable of collecting your name, address, credit card number, expiration date and associated security code information.

What We Are Doing. The confidentiality, privacy, and security information in our care is one of our highest priorities. While we have measures in place to protect information in our systems, we are reviewing our existing policies and working to implement additional safeguards. We are notifying those customers who may be affected. We are also notifying state regulators where necessary.

We are providing you with information you can use to better protect against identity theft and fraud, as well as access to 12 months of complimentary credit monitoring and identity restoration services with Kroll. Instructions for activating the credit monitoring services, as well additional information on how to better protect against identity theft or fraud, are included in the attached Privacy Safeguards.

What You Can Do. Please review the enclosed "Steps You Can Take to Protect Your Information," which contains information on what you can do to better protect against possible misuse of your information. If you see any suspicious charges on your credit card statement, we encourage you to promptly report them to the entity that issued the card. You can also enroll to receive the complimentary credit monitoring and identity restoration services described above.

For More Information. We understand you may have questions that are not answered in this letter. If you have questions, please contact our dedicated assistance line at 1-866-775-4209, Monday through Friday 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

A handwritten signature in black ink that reads "Christine Freed".

Christine Freed
Chief Technology Officer
Tacony Corporation

STEPS YOU CAN TAKE TO PROTECT YOUR INFORMATION

Activate Credit Monitoring

Visit krollbreach.idMonitoringService.com to activate and take advantage of your identity monitoring services.

You have until **July 25, 2019** to activate your identity monitoring services.

Membership Number: <<Member ID>>

To receive credit services by mail instead of online, please call 1-844-263-8605.

Monitor Your Accounts

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. If you see any suspicious charges on your credit or debit card statements, we encourage you to promptly report these charges to the entity that issued the card.

You have the right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

PO Box 9554

Allen, TX 75013

1-888-397-3742

www.experian.com/freeze/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-888-909-8872

www.transunion.com/credit-freeze

Equifax

PO Box 105788

Atlanta, GA 30348-5788

1-800-685-1111

www.equifax.com/personal/credit-report-services

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.);
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

As an alternative to a security freeze, you have the right to place an initial or extended "fraud alert" on your file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002

Allen, TX 75013

1-888-397-3742

www.experian.com/fraud/center.html

TransUnion

P.O. Box 2000

Chester, PA 19016

1-800-680-7289

www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax

P.O. Box 105069

Atlanta, GA 30348

1-888-766-0008

www.equifax.com/personal/credit-report-services

Additional Information

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

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. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 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.

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 violators. 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. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/ff/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.

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You've been provided with access to the following services¹ from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.