

SCOT GANOW
937.641.2041
sganow@taftlaw.com

September 19, 2018

RECEIVED

SEP 20 2018

CONSUMER PROTECTION

FEDERAL EXPRESS

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: *Security Incident Notification*

Dear Attorney General MacDonald:

Our client, Tech Rabbit, LLC ("Tech Rabbit") is providing this notice of a security incident as required under New Hampshire Revised Stat. Ann. §359-C:20, et. seq.

On August 8, 2018, after an external forensics investigation, Tech Rabbit confirmed an unauthorized individual gained access to the company's online product order system, and viewed or stole a subset of customer payment records for purchases made on www.TechRabbit.com. According to the investigation, the unauthorized access took place sometime between February 22, 2017, and May 22, 2018. The company has taken steps to secure the information in its systems, address the root cause of this incident and improve its information security practices to better protect against a recurrence of this type of incident in the future. Tech Rabbit has also alerted its credit card processing company and the credit card brands in accordance with Payment Card Industry Data Security Standards (PCI-DSS).

Tech Rabbit will be providing written notification to 239 New Hampshire residents in substantially the same form as the document enclosed with this letter. The enclosed letter provides a brief description of the incident, the information compromised, information about Tech Rabbit's response to the incident, and steps consumers can take to protect themselves. These written notices will be mailed to affected individuals

Attorney General Gordon MacDonald
September 19, 2018
Page 2

on September 21, 2018. In addition, Tech Rabbit has provided a toll-free number that affected individuals can call with questions regarding the incident.

Should you have any questions about this matter, please do not hesitate to contact me.

Sincerely,

A handwritten signature in black ink, appearing to read "Scot Ganow". The signature is fluid and cursive, with the first name "Scot" and last name "Ganow" clearly distinguishable.

Scot Ganow, CIPP/US
Senior Counsel

SG:lmb
Enclosure
23541536.1



[Date]
[First Name Last Name]
[Address]
[City, State Zip]

RE: Incident Notification

Dear [First Name],

This letter is in regard to an incident at Tech Rabbit involving the security of your personal data on the company's information systems. We sincerely regret to inform you that, after completing a thorough forensics investigation, we have reason to believe your personal data may have been compromised through the access or use by an unauthorized individual. The unauthorized access resulted in the potential viewing or theft of the personal data of some customers that purchased products on Tech Rabbit's web storefront, which is available online at www.TechRabbit.com. The personal data included credit card information. Tech Rabbit has taken the steps necessary to eliminate the threat to your personal data and implement improvements to prevent such unauthorized access from happening again. We are sending this letter to provide you more information about the incident and what you can do to remain vigilant and protect your information.

What Happened

On August 8, 2018, after an external forensics investigation conducted in accordance with our obligations under the Payment Card Industry Data Security Standards, and in collaboration with our credit card processor and the major credit card brands, Tech Rabbit confirmed an unauthorized individual gained access to the company's online product order system. The intruder viewed or stole a subset of customer payment records for purchases made on the Tech Rabbit website. According to the forensics investigation, the unauthorized access was made possible through the use of malicious software in a variety of attacks that took place between February 22, 2017, and May 22, 2018.

What Information Was Involved

The accessed systems contained the following personal information.

- Payment information, including credit card numbers, security code and date of card expiration;
- Customer first and last name;
- Customer mailing address;
- Customer email address; and
- Customer telephone number.

We are not able to confirm, specifically, whether your personal data was viewed or removed from our systems as a result of this incident. We only know that the viewing or removal of some customer data was possible or occurred between February 22, 2017 and May 22, 2018.

What We Did and What We Are Doing

Once aware of the threat to customer data, we promptly took steps to secure the system and identify the scope of the incident with the help of a contracted security firm and forensics investigator. We have continued to implement the recommendations from the security firm and continue to review and audit our practices to prevent this from happening again. We have also coordinated our investigation and response to the incident with the credit card brands, our credit card processor and applicable banks in accordance with Payment Card Industry Data Security

Standards (PCI-DSS). We have also provided notice of this incident to state authorities and credit reporting agencies as required under applicable state laws.

What You Can Do

We highly recommend you review all credit card statements for activity on any credit cards you may have used on the Tech Rabbit store website. Remain vigilant and report any fraudulent activity to your card-issuing bank or card issuer as soon as possible. Regardless of whether or not you note any fraudulent activity on your card statement, we still recommend that you contact your card-issuing bank and request a replacement card.

Should you have concerns about identity theft, you can contact local law enforcement and file a police report. You may also contact the Federal Trade Commission or one of the credit bureaus for more information about how to protect your identity.

For More Information:

You can place an identity theft/fraud alert, get credit freeze information for your state, or order a free credit report by calling any of the following credit reporting agencies at one of the phone numbers listed below or visiting their respective websites. Some states may charge a fee for such services.

Equifax - 1-888-766-0008
P.O. Box 740256
Atlanta, GA 30348
www.equifax.com

Experian - 1-888-397-3742
P.O. Box 4500
Allen, TX 75013
www.experian.com

Trans Union - 1-800-680-7289
P.O. Box 2000
Chester, PA 19022
www.transunion.com

Under state law, a security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware 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 reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you a fee to place, temporarily lift, or permanently remove a security freeze. To place a security, freeze on your credit report, you must send a written request to each of the three major credit reporting agencies listed above. The credit reporting agencies may also allow you to request such a security freeze online.

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;
8. If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

The Federal Trade Commission (FTC) provides more information about how to protect your identity at either <https://www.ftc.gov/> or <https://www.identitytheft.gov/>. You may also find additional information on any applicable rights under the Fair Credit Reporting Act. You can also contact the FTC by using the information below.

Federal Trade Commission
1-202-326-2222
Bureau of Consumer Protection
600 Pennsylvania Avenue, NW
Washington, DC 20580

Maryland Residents. Additional information about identity theft protection may be available from your Attorney General's office.

Maryland Attorney General's Office
Toll Free Consumer Line: 888-743-0023
Identity Theft Unit
E-mail: idtheft@oag.state.md.us
200 St. Paul Place
16th Floor
Baltimore, MD 21202
<http://www.marylandattorneygeneral.gov/Pages/IdentityTheft/default.aspx>

Massachusetts Residents. Massachusetts residents should not be charged more than \$5.00 to place, temporarily lift, or remove a security freeze. Massachusetts residents have a right to obtain a police report in regard to the incident.

North Carolina Residents. Additional information may be available from your Attorney General's office.

North Carolina Attorney General's Office
Consumer Protection Division
9001 Mail Service Center

Raleigh, NC 27699-9001
877-566-7226 (Toll-free within North Carolina)
919-716-6000
www.ncdoj.gov

Again, we sincerely regret that this incident has occurred. If you have any questions, please contact us at:

Contact: Tech Rabbit, LLC
Email: HELP@TECHRABBIT.COM
Telephone: 888-556-1230
Address: Tech Rabbit, LLC
601 Lehigh Ave
Union, NJ, 07083

Sincerely,

Tech Rabbit, LLC

23541536.1