



Hogan Lovells US LLP
Columbia Square
555 Thirteenth Street, NW
Washington, DC 20004
T +1 202 637 5600
F +1 202 637 5910
www.hoganlovells.com

RECEIVED

MAY 27 2020

CONSUMER PROTECTION

May 26, 2020

By FedEx

Consumer Protection Bureau
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Security Incident Notification

To Whom It May Concern:

I am writing on behalf of Hello Doggie, Inc. ("Company") to inform you of an incident that may have impacted personal information of 5 New Hampshire residents. On April 6, 2020, the Company learned of suspicious activity associated with a company email account and promptly reset account credentials and updated email account settings. The Company launched an investigation involving external forensic experts to determine the nature and scope of the incident and to identify the information contained in the email account. At this time, the Company has identified suspicious email account activity as early as March 23, 2020. The email account contained files or messages that included information such as name, physical address, Social Security number, financial account information, and communications regarding health-insurance reimbursement and similar matters.

Although the Company is not currently aware of any evidence indicating that unauthorized individuals were seeking to access or acquire personal information, the Company has decided out of an abundance of caution to notify individuals whose personal information covered by N.H. Rev. Stat. § 359-C:19 may have been impacted as a result of the incident. Company is also reviewing and updating its security practices to help prevent this type of incident from occurring again, including moving to a cloud-based service to enhance protections for the transmission of data related to current and former personnel and implementing additional training regarding security for email accounts.

On May 22, 2020, the Company sent notice by postal mail to the potentially impacted New Hampshire residents. A sample copy of the notice is enclosed. In addition to providing information regarding credit reporting agencies, security freezes, fraud alerts, and other identity theft prevention tools, the Company is offering credit monitoring and identity protection services for 1 year through ID Experts to affected individuals, at no cost to them.

Please feel free to contact me if you have any questions or require additional information.

Sincerely,

James Denvil

Senior Associate
w.james.denvil@hoganlovells.com
D 1 202-637-5521

Enclosure

Hello Doggie, Inc.
C/O ID Experts
P.O. Box 1907
Suwanee, GA 30024

To Enroll, Please Call:

(833) 579-1093

Or Visit:

<https://app.myidcare.com/account-creation/protect>

Enrollment Code: <<XXXXXXX>>

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

May 22, 2020

NOTICE OF DATA BREACH

Dear <<First Name>> <<Last Name>>:

Hello Doggie, Inc. is writing to provide you with information regarding some unusual activity that we detected in one of our email accounts. This incident may have affected personal information related to you. We received that personal information in association with the work that you or a family member performed with us. Below please find information about what we have discovered regarding the incident, the steps we have taken to address the situation, and additional actions you can take to protect yourself.

WHAT HAPPENED

On April 6, 2020, Hello Doggie, Inc. learned of suspicious activity indicating that an unauthorized individual may have accessed a company email account that contained communications including personal information relating to you. After learning of the incident, we contacted law enforcement and promptly reset the credentials and updated settings for the affected email account. We initiated and undertook an investigation to determine the full nature and scope of the incident with the assistance of external forensic experts. At this time, we have identified suspicious email account activity as early as March 23, 2020. Although we are not aware of any evidence indicating that the unauthorized email account activity was an attempt to access or misuse your personal information, we are providing this notice out of an abundance of caution so that you can take steps to protect yourself.

WHAT INFORMATION WAS INVOLVED

The personal information about you that may have been accessed includes your name, physical address, Social Security number, financial account information, and information related to health-insurance reimbursements or similar matters that you or others may have sent to us.

WHAT WE ARE DOING

We take the privacy and security of your personal information seriously, and we regret that this incident occurred. After learning of the incident, we took steps to eliminate the unauthorized access and we have not identified activity suggesting that such unauthorized access is ongoing. We are reviewing and updating our security practices to help prevent this type of incident from occurring again, including implementing additional phishing awareness training and password-related controls. Additionally, we have arranged for you to obtain MyIDCare™ identity protection services from ID Experts at no cost to you. The package of services for adults includes credit monitoring, monitoring for signs of potential acquisition or misuse of your personal information, access to fraud prevention and identity restoration services from ID Experts, and up to \$1,000,000 in identity theft insurance.

WHAT YOU CAN DO

We know that the security of your personal information is important to you. We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (833) 579-1093 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 9 am - 9 pm Eastern Time. Please note the deadline to enroll is August 22, 2020.

Although we are not aware of any evidence indicating that your personal information has been misused, we recommend that you remain vigilant and review your financial records and statements for signs of suspicious activity. Please find additional information in Attachment 1 to this letter.

FOR MORE INFORMATION

Again, we regret any inconvenience this incident may cause. If you have any questions or need additional information, please call (833) 579-1093 or go to <https://app.myidcare.com/account-creation/protect>.

Sincerely,



Jill Katz, President

Enclosures

Attachment 1: Additional Information

You should be cautious about using email to provide sensitive personal information, whether sending it yourself or in response to email requests. You should also be cautious when opening attachments and clicking on links in emails. Scammers sometimes use fraudulent emails or other communications to deploy malicious software on your devices or to trick you into sharing valuable personal information, such as account numbers, Social Security numbers, or usernames and passwords. The Federal Trade Commission (FTC) has provided guidance at <https://www.consumer.ftc.gov/articles/0003-phishing>.

You should review your financial statements and accounts for signs of suspicious transactions and activities. If you find any indication of unauthorized accounts or transactions, you should report the possible threat to local law enforcement, your State's Attorney General's office, or the FTC. You will find contact information for some of those entities below. If you discover unauthorized charges, promptly inform the relevant payment card companies and financial institutions.

Fraud Alert Information

Whether or not you enroll in the credit monitoring product offered, we recommend that you consider placing a free "Fraud Alert" on your credit file. Fraud Alert messages notify potential credit grantors to verify your identification before extending credit in your name in case someone is using your information without your consent. A Fraud Alert can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit. Fraud alerts last one year. Identity theft victims can get an extended fraud alert for seven years.

Call only one of the following three nationwide credit reporting companies to place your Fraud Alert: TransUnion, Equifax, or Experian. As soon as the credit reporting company confirms your Fraud Alert, they will also forward your alert request to the other two nationwide credit reporting companies so you do not need to contact each of them separately. The contact information for the three nationwide credit reporting companies is:

Equifax PO Box 740256 Atlanta, GA 30374 www.alerts.equifax.com 1-800-525-6285	TransUnion PO Box 2000 Chester, PA 19016 www.transunion.com/fraud 1-800-680-7289	Experian PO Box 9554 Allen, TX 75013 www.experian.com/fraud 1-888-397-3742
---	--	--

Free Credit Report Information

You have rights under the federal Fair Credit Reporting Act. These include, among others, the right to know what is in your credit file; the right to dispute incomplete or inaccurate information; and the right to ask for a credit score. Under federal law, you are also entitled to one free credit report once every 12 months from each of the above three major nationwide credit reporting companies. Call 1-877-322-8228 or make a request online at www.annualcreditreport.com.

Even if you do not find any suspicious activity on your initial credit reports, we recommend that you check your account statements and credit reports periodically. You should remain vigilant for incidents of fraud and identity theft. Victim information sometimes is held for use or shared among a group of thieves at different times. Checking your credit reports periodically can help you spot problems and address them quickly.

If you find suspicious activity on your credit reports or have reason to believe your information is being misused, call your local law enforcement agency or state attorney general and file a police report. Get a copy of the report; many creditors want the information it contains to alleviate you of the fraudulent debts. You also should file a complaint with the FTC using the contact information below. Your complaint will be added to the FTC's Consumer Sentinel database, where it will be accessible to law enforcers for their investigations.

You may also contact the FTC at the contact information below to learn more about identity theft and the steps you can take to protect yourself. If you are a resident of Maryland, North Carolina, or Rhode Island, you can also reach out to your respective state's Attorney General's office using the contact information below:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue NW
Washington, DC 20580
1.877.FTC.HELP (382.4357)
www.ftc.gov/idtheft

Maryland Attorney General's Office
200 St. Paul Place
Baltimore, MD 21202
1-888-743-0023 / www.marylandattorneygeneral.gov

North Carolina Attorney General's Office
90001 Mail Service Center
Raleigh, NC 27699
1-919-716-6400 / <https://ncdoj.gov/>

Rhode Island Attorney General's Office
150 South Main Street
Providence, Rhode Island 02903
1-401-274-4400 / <http://www.riag.ri.gov/>

Security Freeze Information

You can request a free Security Freeze (aka “Credit Freeze”) on your credit file by contacting each of the three nationwide credit reporting companies via the channels outlined below. When a Credit Freeze is added to your credit report, third parties, such as credit lenders or other companies, whose use is not exempt under law will not be able to access your credit report without your consent. A Credit Freeze can make it more difficult for someone to get credit in your name; however, please be aware that it also may delay your ability to obtain credit.

Equifax Security Freeze
PO Box 105788
Atlanta, GA 30348
www.freeze.equifax.com
1-800-349-9960

TransUnion Security Freeze
PO Box 2000
Chester, PA 19016
www.transunion.com/freeze
1-888-909-8872

Experian Security Freeze
PO Box 9554
Allen, TX 75013
www.experian.com/freeze
1-888-397-3742

To request a Credit Freeze, you may 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.)