



RECEIVED

JUL 01 2019

CONSUMER PROTECTION

DLA Piper LLP (US)
1201 North Market Street
Suite 2100
Wilmington, Delaware 19801-1147
www.dlapiper.com

Edward J. McAndrew
Ed.McAndrew@dlapiper.com

VIA: FIRST-CLASS MAIL

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

June 26, 2019

Re: Security Incident Notification

Dear Attorney General MacDonald:

We are providing notice on behalf of IM Shopping, Inc. ("IM Shopping", "we"), pursuant to N.H. Rev. Stat. Ann. § 359-C:20, about an incident involving 33 New Hampshire residents. IM Shopping operates in the prepaid card, gift card and payment card business and offers, among other things, software solutions to sell and redeem gift cards online. As explained below, the incident at issue involves our Gift Card Mall ("GCM") website (www.giftcardmall.com).

Our investigation is ongoing and the information provided in this letter with respect to the security incident may change should additional relevant information be discovered. On May 21, 2019, our information security team identified an unauthorized script placed in the code of the GCM website. The changes to the GCM site code appear to have occurred on April 24, 2019 and appear to have been designed to forward, to an external site, data inputted by a consumer into the order form on the GCM site. Our investigation revealed no evidence that the personal information of GCM website users was actually accessed by any unauthorized party.

We continue to diligently investigate and assess this incident and continue to monitor for suspicious activity. We are continuing to enhance our identity, authentication and remote access controls, and to educate our workforce about cybersecurity issues. Any of the New Hampshire residents affected by this breach are offered 24 months of credit monitoring and identity protection services to affected New Hampshire residents at no charge and we will ask these residents to contact our toll-free number or to visit our website for additional information or assistance. We provided written notification to the 33 affected New Hampshire residents on June 14, 2019, a sample copy of which is enclosed.



VIA FIRST-CLASS MAIL

The Honorable Gordon J. MacDonald

Page Two

If you should have any questions or if we can provide further assistance to any of the New Hampshire residents affected by this incident, please feel free to contact me at (302) 468-5685 or at ed.mcandrew@dlapiper.com.

Respectfully submitted,

DLA Piper LLP (US)

A handwritten signature in blue ink, appearing to read 'EJ McAndrew', written over the printed name below.

Edward J. McAndrew

IMshopping

C/O ID Experts

<<Address 1>>

<<City>> <<State>> <<ZIP>>

ENDORSE



ZDcode
SEQ

CARE OF

NAME

ADDRESS1

ADDRESS2

CSZ

COUNTRY

BREAK

To Enroll, Please Call:

1-800-397-9573

Or Visit:

<https://ide.myidcare.com/imshopping>

Enrollment Code: <<XXXXXXXXXX>>

June 14, 2019

Notice of Data Security Incident

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

We are writing to notify you of a data security incident related to the Gift Card Mall (“GCM”) website (www.giftcardmall.com), which may have affected your personal information if you interacted with the GCM website between April 24, 2019 and May 21, 2019.

What Happened: On May 21, 2019, we identified an unauthorized script placed in the code of the GCM website. The changes to the GCM site code appear to have occurred on April 24, 2019 and appear to have been designed to forward, to an external site, data inputted by a consumer into the order form on the GMC site. Our investigation of this incident revealed no evidence that your personal information was actually accessed by any unauthorized party.

Personal Information Involved: The following types of personal information entered into the website order page between April 24, 2019 and May 21, 2019 may have been affected: name, address, payment card number, card expiration date, and security code.

What We Are Doing: Upon becoming aware of the incident, we promptly launched an investigation with the assistance of a leading cybersecurity firm and took steps to remove the unauthorized script from the code of the GCM website. In an abundance of caution, we also logged out all users who interacted with the GCM website between April 24, 2019 and May 21, 2019. Due to these security precautions, you will not be able to access your account using your current password and will need to change your password by following the instructions contained on the GSM website login page.

As an added precaution, we are providing access to 24 months of MyIDCare™ credit monitoring and identity protection services at no cost to you, through ID Experts. MyIDCare services include: 24 months of credit 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: In order to regain access to your online account, you will need to change your password by going to www.giftcardmall.com, clicking “Sign In” in the upper right corner, and entering your email under “Forgot Your Password,” and click “SUBMIT.” A password recovery link will be sent to your email address with directions to create a new password.

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling 1-800-397-9573 or going to <https://ide.myidcare.com/imshopping> 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 September 14, 2019.



Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://ide.myidcare.com/imshopping> 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 1-800-397-9573 to gain additional information about this event and 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.

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
1-800-525-6285
P.O. Box 105069
Atlanta, GA 30348-5069
www.alerts.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
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. To find out more on how to place a security freeze, you can use the following contact information:

Equifax
P.O. Box 105788
Atlanta, GA 30348
1-800-685-1111

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013
1-888-397-3742

TransUnion
P.O. Box 2000
Chester, PA 19022-2000
1-888-909-8872

Websites:

www.freeze/equifax.com

www.experian.com/freeze/center.html

www.transunion.com/credit-freeze

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.

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.

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

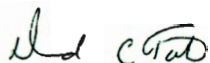
All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.

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. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

For More Information: Please call 1-800-397-9573 or go to <https://ide.myidcare.com/imshopping> for assistance or for any additional questions you may have. You also may consult the resources included on the enclosed form, which provides additional information about protecting your personal information online.

We take very seriously the security of the personal information that our customers entrust into our care and regret any inconvenience caused by this incident. Working to ensure that this does not happen again is one of our highest priorities.

Sincerely,

A handwritten signature in cursive script, appearing to read "David Tate".

David Tate
Senior Vice President, Sales & Marketing

(Enclosure)