PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

+1.206.359.8000
+1.206.359.9000
PerkinsCoie.com

February 5, 2016

Amelia M. Gerlicher
AGerlicher@perkinscoie.com
D. +1.206.359.3445
F. +1.206.359.4445

State of Hawaii Office of Consumer Protection
Executive Director Bruce B. Kim
Leiopapa A Kamehameha Building
235 South Beretania Street, Suite 801
Honolulu, HI 96813

ocp@dcca.hawaii.gov

Re: **Security Breach Notification**

Dear Mr. Kim:

I am writing on behalf of Gyft, Inc. to inform you of a recent security breach incident involving unauthorized access to Gyft user information. Gyft, a company that provides an online service and mobile application that allows users to purchase and store gift cards, has learned that two of its cloud providers were accessed without authorization between October 3 and December 18, 2015. The information potentially accessed from the cloud providers included names, addresses, dates of birth, phone numbers, email addresses, and gift card numbers.

This incident first came to Gyft's attention on December 3, 2015, when it learned that a file available on the Internet appeared to contain Gyft user records. It was not immediately apparent how the file had been created, and Gyft did not discover that its cloud providers had been accessed without authorization until approximately December 28, 2015. The unknown individual(s) that accessed the cloud providers used valid Gyft credentials. As of the date of this letter, Gyft has not determined how the credentials were obtained or who obtained them.

When Gyft became aware of this incident, it appeared that log files, including usernames and passwords, dating as far back as March 19, 2015 had been compromised. Accordingly, Gyft immediately reset user passwords for all users who had logged in during that time period. Upon identifying unauthorized logins to its cloud providers, Gyft reviewed all files stored with the cloud providers that were potentially accessed without authorization, and is notifying all Gyft users whose sensitive personal information was available in the potentially accessed files. Gyft has also forced password resets and/or logouts for additional affected users as those users were identified.

As of the date of this letter, Gyft has not discovered evidence that anyone used the information potentially compromised in this incident to access Gyft accounts or make unauthorized purchases. In particular, during the period that potentially exposed credentials were still valid, it did not see an increase in account logins that would be consistent with exploitation of those credentials.

c/o ID Experts
PO Box 6336
Portland, OR 97228-6336

<<mail id>>
<<Name1>>
<<Address1>>
<<Address2>>
<<City>><<State>><<Zip>>

<<Date>>

Notice of Data Breach

Dear Gyft User,

We are writing to let you know about an incident that potentially involves your Gyft account. As described below, an unknown party may have gained unauthorized access to certain Gyft user information. We are taking this incident very seriously. As soon as Gyft learned about the exposure, we began investigating how this user information was accessed and what risks this potentially posed to Gyft customers. Fortunately, we have not discovered evidence that anyone used the information potentially compromised in this incident to access Gyft accounts or make unauthorized purchases.

Nonetheless, please carefully read this notice.

What Happened?
Beginning on October 3 and continuing through December 18, 2015, an unknown party accessed without authorization two cloud providers used by Gyft. This unknown party was able to view or download certain Gyft user information stored with these cloud providers and make a file containing some of that user information.

What Information Was Involved?
The information potentially accessed from the cloud providers included names, addresses, dates of birth, phone numbers, email addresses, and gift card numbers. Gift card numbers could have been used to make unauthorized purchases. In addition, if you attempted to use Gyft between March 19 and December 4, 2015, your Gyft log-in credentials may have been compromised. An unauthorized party who acquired your credentials could have accessed your Gyft account and used any gift cards in your account with unused balances, or used available reward points or a Coinbase-enabled account to purchase additional gift cards. Importantly, no credit cards stored in your Gyft account were compromised because full credit card numbers are not visible in Gyft accounts and any credit card purchases require the three- or four -digit security code on the back or front of your credit card, which was not part of the information that may have been compromised.

What Are We Doing?
Shortly after discovering this issue, Gyft acted to prevent unauthorized access by forcing users whose passwords were potentially compromised to reset their passwords and logging out other affected users. Affected users who have not already done so will be forced to choose a new password the next time they log in. We also reset the Coinbase tokens for all affected customers. We are continuing to investigate the incident and will take all appropriate steps to protect Gyft customers.

For the latest information on this incident go to: **www.myidcare.com/gyft**.

What You Can Do
We recommend that you change your password for any online account where you use the same password that you used for Gyft between March 19 and December 4, 2015. As discussed above, credit cards stored through Gyft were not affected by this incident. However, if you have a Coinbase account linked to your Gyft account, we recommend

Additional Information Regarding Identity Theft and Your Credit Report

The Federal Trade Commission (FTC) provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen. You may contact the FTC at FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, www.consumer.ftc.gov, 1-877-ID-THEFT (877-438-4338). You can also contact local law enforcement or the attorney general's office in your state if you suspect that you have been the victim of identity theft.

You also may obtain a free copy of your credit report maintained by each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling toll-free 1-877-322-8228. Review the reports carefully, and if you find anything you do not understand or that is incorrect, contact the appropriate credit reporting agency.

You also may consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze or to obtain additional information regarding identity theft. An initial fraud alert is free and lasts for at least 90 days. The alert informs creditors of possible fraudulent activity within your report and requests that the credit company contact you prior to establishing any accounts in your name. In contrast, a security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without prior written permission. Placing a security freeze on your credit report may delay your ability to obtain credit.

To place a fraud alert or security freeze on your credit report, contact any the three credit reporting agencies using the contact information below:

- Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
- Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013
- TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Department, P.O. Box 2000, Chester, PA 19022-2000