PERKINSCOIE

1201 Third Avenue
Suite 4900
Seattle, WA 98101-3099

+1.206.359.8000
+1.206.359.9000
PerkinsCoie.com

February 4, 2016

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

Washington Attorney General's Office
800 5th Ave, Suite 2000
Seattle, WA 98104-3188

SecurityBreach@atg.wa.gov

Re: **Security Breach Notification**

To Whom It May Concern:

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.

Gyft is notifying 9,042 residents of your state that they may have had gift cards exposed that may be used to make unauthorized purchases up to the existing value on that card. In addition, although not required by your data breach notification statute to do so, it is notifying users whose email address and password were compromised that they should change their password on other sites where they use the same password they used for Gyft.

Gyft is providing notification to affected individuals beginning February 5, 2016. Users for whom Gyft does not have a physical address will be contacted via email, and, in compliance with your statutory substitute notice procedures, Gyft is posting a link to this notification on its homepage at Gyft.com and contacting the media in your state. These notifications are being provided without unreasonable delay after conducting the investigation described above, which was necessary to determine the relevant facts and scope of the incident, assure the reasonable integrity of Gyft's systems, and identify the individuals potentially affected.

Gyft continues to investigate this incident and it is using this event to employ additional controls to further enhance the security of the Gyft platform. If you have additional questions or concerns regarding this incident, please contact me at the above address.

Very truly yours,

Amelia M. Gerlicher

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

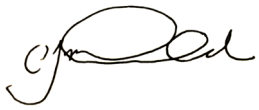
that you review any Coinbase transactions beginning in October 2015, because a linked Coinbase account could have been used to make purchases within your Gyft account. You should also monitor any gift cards that were in your Gyft account before January 8, 2016.

Although the information potentially involved in this incident does not affect your credit, we are required by law to provide you certain information about your credit report and identity theft. This information is enclosed.

You may also contact us in writing at 150 W. Evelyn Avenue, Suite 300, Mountain View, CA 94041, or you can call us at **866-287-0504**.

On behalf of Gyft, we regret any inconvenience this may cause you.

Sincerely,



CJ MacDonald
Chief Operating Officer, Gyft

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