

February 5, 2016

Iowa Attorney General Tom Miller  
Consumer Protection Division  
1305 E. Walnut Street  
Des Moines, IA 50319

[Nathan.blake@iowa.gov](mailto:Nathan.blake@iowa.gov)

Amelia M. Gerlicher  
[AGerlicher@perkinscoie.com](mailto:AGerlicher@perkinscoie.com)  
D. +1.206.359.3445  
F. +1.206.359.4445

**Re: Security Breach Notification**

Dear Mr. Miller:

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.

Security Breach Notification  
February 5, 2016

Gyft is notifying approximately 1,746 users in your state that the information compromised may have included their gift card numbers, which could be used to make unauthorized purchases up to the existing value on that card (value cannot be added by unauthorized users unless user accounts were Coinbase enabled, as described below). Gyft's system does not have the functionality to know if gift cards in user accounts were used or had balances, so it is notifying all users who owned potentially exposed cards. In most cases, the gift card numbers were only accessible if an unauthorized party used exposed Gyft credentials to access a user's account before the credentials were reset. The unauthorized party could then use any gift cards in the account with unused balances, or use available reward points or a Coinbase-enabled account to purchase additional gift cards with Bitcoin. Importantly, no credit cards saved by Gyft users 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 the card, which was not part of the information that may have been compromised.

In addition, although your state's data breach notification statute does not require it to do so, Gyft is also notifying all users whose email address and password were potentially compromised, but who had no gift cards in their account, that they should change their passwords on any other sites where they use the same password they used for Gyft.

Attached is a copy of the notification that will be sent to individuals whose gift cards were compromised beginning February 5, 2016. Users for whom Gyft does not have a physical address will be contacted via email.

Gyft is also arranging notification of certain users who were sent URLs to claim gift cards that the URLs (which allow access to the gift cards without user credentials) may have been potentially compromised. These users received cards through third party resellers and did not register as Gyft customers; Gyft is coordinating with the third party resellers to arrange notice. This pool is not included in the number above, but it is relatively small, comprising less than 10% of the overall notice pool.

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](http://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,

A handwritten signature in black ink, appearing to read 'CJ MacDonald', written in a cursive style.

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