Michael Best & Friedrich LLP
Attorneys at Law
Adrienne S. Ehrhardt, CIPP/US, CIPM
T 608.283.0131
E asehrhardt@michaelbest.com

Via Electronic Mail
securitybreach@atg.wa.gov

Attorney General Bob Ferguson
Office of the Attorney General
1125 Washington Street SE
PO Box 40100
Olympia, WA 98504-0100

Re: Notice of Security Incident

Dear Attorney General Ferguson:

We are writing you on behalf of our client Fetch Rewards, Inc. ("Fetch") to notify you of a recent security incident that affected the personal information of some Washington state residents. Fetch operates a mobile application that allows consumers to earn rewards for scanning various grocery and shopping receipts.

On or about June 6, 2020, as a result of a temporary API code misconfiguration, certain Fetch member profile information was returned to an unauthorized third party. Once Fetch recognized this issue on June 9, 2020, this code error was promptly fixed the next day, and Fetch permanently shut down the affected API. Because the code error called Fetch's profile database, it returned the profiles of 128,598 Washington state residents. The personal information involved included, name, email address, date of birth, and zip code. Fetch does not collect or store sensitive information such as social security number or financial account information. So, none of this type of information was involved.

Fetch immediately engaged an expert outside IT Forensics firm to investigate and respond to the incident. Its investigation confirmed that the incident was caused by the coding error and that it was successfully contained. The IT Forensics firm further determined the scope of the incident and concluded its investigation on or about July 7, 2020, and it was able to provide Fetch a preliminary list of affected individuals. Fetch is preparing notifications, validating email addresses, and setting up a call center in order to send notices to affected individuals via electronic mail as soon as logistically possible. A copy of the notification letter is attached. Fetch continues to monitor for suspicious activity and make enhancements to improve its security. It further engaged a separate cybersecurity company to ensure there were no other coding errors in other APIs. Fetch continues to improve its policies and practices to ensure a high standard of application security and data privacy.

If you have any questions, please do not hesitate to contact me.

Regards,
Adrienne S. Ehrhardt
Adrienne S. Ehrhardt
Partner

Notice of Security Incident

Dear Valued Fetch Member,

We are writing to inform you about a data incident that occurred that may have involved your personal data that was on the Fetch Rewards ("Fetch") system. We value our relationship with you and take the security of your data seriously. Please review the information provided in this letter for some steps you may take relating to this incident.

What Happened?

On or about June 6, 2020, as a result of a temporary API code misconfiguration, certain Fetch member profile information was returned to an unauthorized third party. Once Fetch recognized this issue on June 9, 2020, this code error was promptly fixed the next day.

What Information Was Involved?

This incident involved name, email address, date of birth, and zip code. Because Fetch does not collect or store sensitive information such as social security number or financial account information, none of this type of information was involved. Moreover, even though your personal information may have been accessed or acquired by an unauthorized third party, we do not have any evidence that your information was actually used by that third party.

Here's What We Are Doing and What You Can Do

Fetch hired an expert outside IT Forensics firm to investigate, respond to, and determine the scope of the incident. Its investigation confirmed that the incident was caused by the coding error and that it was successfully contained. In addition to fixing the coding error, Fetch shut down the API entirely. Fetch further engaged a separate cybersecurity company to ensure there were no other coding errors in other APIs. The cybersecurity company confirmed that the unauthorized access was limited in scope to that outlined above. We continue to monitor for suspicious activity and will continue to make enhancements to our systems to ensure a high standard of application security and data privacy.

In addition, we are providing you with the enclosed information about Identity Theft Protection. Although Social Security numbers and other sensitive personal information were not at risk in this incident, as a general practice, we recommend that you carefully check your credit reports for accounts you did not open or for inquiries from creditors you did not initiate. If you see anything you do not understand, call the credit agency immediately. You should also regularly review your credit or debit card account statements to determine if there are any discrepancies or unusual activity listed. If you see something you do not recognize, immediately notify your financial institution.

We sincerely apologize for any inconvenience or concern this incident may cause. If you have questions, please call us at 844-952-2218 or send us an email at concerns@fetchrewards.com.

Sincerely,

The Fetch Privacy Team

Information about Identity Theft Protection

Review Accounts and Credit Reports: It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies. To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:
Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You should remain vigilant with respect to reviewing your account statements and credit reports, and you should promptly report any suspicious activity or suspected identity theft to the proper law enforcement authorities, including local law enforcement, your state's attorney general, and/or the Federal Trade Commission ("FTC"). You may contact the FTC or your state's regulatory authority to obtain additional information about avoiding and protection against identity theft: Federal Trade Commission, Consumer Response Center 600 Pennsylvania Avenue, NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft.

Security Freezes and Fraud Alerts:

You have a right to place a security freeze on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization. The security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a security freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit.

A security freeze does not apply to a person or entity, or its affiliates, or collection agencies acting on behalf of the person or entity, with which you have an existing account that requests information in your credit report for the purposes of reviewing or collecting the account. Reviewing the account includes activities related to account maintenance, monitoring, credit line increases, and account upgrades and enhancements. Please contact the three major credit reporting companies as specified below to find out more information about placing a security freeze on your credit report.

As an alternative to a security freeze, you have the right to place an initial or extended fraud alert on your credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer's credit file. Upon seeing a fraud alert display on a consumer's credit file, a business is required to take steps to verify the consumer's identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting 7 years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies at the addresses or toll-free numbers listed at the bottom of this page.

For more information, including information about additional rights, you can visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf,https://www.consumerfinance.gov/learnmore/, or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You can obtain more information about fraud alerts and credit freezes by contacting the FTC or one of the national credit reporting agencies listed below.

Equifax (www.equifax.com) **General Contact:** P.O. Box 740241 Atlanta, GA 30374 800-685-1111 **Fraud Alerts**: P.O. Box 740256, Atlanta, GA 30374 **Credit Freezes**: P.O. Box 105788, Atlanta, GA 30348	Experian (www.experian.com) **General Contact:** P.O. Box 2002 Allen, TX 75013 888-397-3742 **Fraud Alerts and Security Freezes:** P.O. Box 9554, Allen, TX 75013	TransUnion (www.transunion.com) **General Contact, Fraud Alerts and Security Freezes:** P.O. Box 2000 Chester, PA 19022 888-909-8872