



1900 M Street, NW • Suite 250 • Washington, D.C. 20036
(202) 296-3585

July 11, 2018

Michelle Anderson
Attorney, ZwillGen PLLC
c/o WeWork One Beacon Street
Boston, MA 02108
michelle@zwillgen.com

Via FedEx

Attorney General Joseph Foster
New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

STATE OF NH
DEPT OF JUSTICE
2018 JUL 12 AM 11:00

Re: Notice of Fruitful Yield e-Commerce Security Incident

Dear Attorney General Foster:

On behalf of my client, The Fruitful Yield, Inc. (“Fruitful Yield”), I am writing to inform you of a data security incident that involved the personal information of five individuals in New Hampshire due to vendor-related security issues with select Fruitful Yield e-commerce websites.

On June 15, 2018, Fruitful Yield became aware of a security flaw affecting the abovementioned websites. After working with a third-party consultant, Fruitful Yield confirmed that from May 29, 2018 to June 13, 2018, an unauthorized user gained access to the websites through a third-party vendor’s extension and may have acquired the following information about our client’s customers: name; billing and shipping address; credit card number, expiration date, and CVV; and customer username and password for the Fruitful Yield website(s).

Within hours of discovering the issue, my client notified the vendor, who was previously unaware of the vulnerability and immediately began investigating the incident. Since that date, Fruitful Yield’s outside consultant has identified and patched the point-of-entry, conducted an in-depth review of server logs, created and deployed security patches, set up and conducted nightly in-depth security scans for malware, and removed all files and script references uploaded by the unauthorized user. In addition, Fruitful Yield has taken steps to mitigate similar incidents from occurring, including working with its security consultant and updating its prioritization of security patches to address issues relating to this vendor and its e-commerce websites.

Fruitful Yield is sending the enclosed notice to individuals today, July 11th. The notice includes information regarding how individuals can register for complimentary identity monitoring services from Kroll, which include: Credit Monitoring, Web Watcher, Public Persona, Quick Cash

Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

Please let me know if you have any questions regarding this incident using my contact information provided above.

Sincerely,

ZwillGen PLLC

A handwritten signature in blue ink that reads "Michelle Anderson". The signature is written in a cursive style with a large initial "M".

Michelle Anderson

Encl: Template individual notice



<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberMiddleName>> <<MemberLastName>> <<Suffix>>

<<Address1>>

<<Address2>>

<<City>>, <<State>> <<ZipCode>>

IMPORTANT NOTICE OF Fruitful Yield e-Commerce Incident

Dear <<MemberFirstName>> <<MemberLastName>>,

You are receiving this notice because of a data security incident that may have involved some of your personal information because of a recent purchase you made online from one of the following Fruitful Yield, Inc. ("Fruitful Yield") e-commerce websites:

FruitfulYield.com

NOW-2-U.com

VitaminExperts.com

Just because you made a purchase during this timeframe on one of these websites does not mean you are a victim of fraud. We encourage you to review the information in this letter for some steps that you can take to protect yourself against the potential misuse of your information.

What Happened?

It recently came to our attention that during the time period from May 29, 2018 to June 13, 2018, an unauthorized user gained access to the affected sites through a third party vendor's extension, and may have acquired certain information about our customers.

We value your business and respect the privacy of your information, and take this matter very seriously. We began investigating the incident as soon as we became aware of unusual activity and took immediate action, including working with our security consultant, conducting an investigation into this matter, and reporting it to the third party vendor, who was previously unaware of the vulnerability with its extension.

What Information Was Involved?

The personal information potentially exposed included:

- Customer name and address
- Credit card number, expiration date and CVV
- Customer username and password for the website

What Are We Doing?

In addition to the steps noted above, we have taken steps to remediate the incident and prevent similar incidents from occurring in the future. Specifically, we have identified and patched the point-of-entry, conducted an in-depth review of server logs, created and deployed security patches, set-up and conducted nightly in-depth security scans for malware, and removed all files and script references uploaded by the unauthorized user, and updated our prioritization of security patches to address issues relating to this vendor and our e-commerce websites.

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Web Watcher, Public Persona, Quick Cash Scan, \$1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration. For more information about the services and how to enroll, please see the attachment to this letter.

What You Can Do

While we will continue to take steps to improve our security, there are also some steps that you can take to help protect yourself, such as:

- *Regularly Review Your Financial Statements.* We recommend you remain vigilant by regularly reviewing your credit card and bank account statements. This is the most important step that you can take to detect and prevent any unauthorized use of your credit card number.
- *Contacting Your Credit Card Issuer.* We are taking steps to notify the various credit card companies about this breach. We ask that you remain vigilant by carefully reviewing your credit card account statements and immediately alerting your credit card issuing bank of any suspicious charges.
- *Changing Your Passwords.* Fruitful Yield does not store plain text passwords in its database, but it is possible that the unauthorized user had access to passwords in plain text before they got to our database. Thus, you should immediately change your password for any or all of the above-mentioned websites. Additionally, we highly recommend customers who utilize similar credentials across other platforms reset any passwords on accounts that may use the same or a similar login password.
- *Obtain a Free Credit Report.* You may request a free copy of your U.S. credit report once every 12 months by visiting www.annualcreditreport.com or by calling 1-877-322-8228 toll free. You can print a copy of the request form at <http://www.ftc.gov/bcp/menus/consumer/credit/rights.shtml>.
- *Carefully Review Your Credit Report.* Carefully review any credit reports you receive. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. Also, look for personal information, such as home address and Social Security number, that is not accurate. If you see anything you do not understand, call the credit agency at the telephone number on the report. We also suggest that you consider contacting one of the major credit bureaus listed below to place a fraud alert on your credit reports:

Equifax: 800 525-6285; www.equifax.com; P.O. Box 740231, Atlanta, GA 30374-0241

Experian: 888 397-3742; www.experian.com; P.O. Box 9532, Allen, TX 75013;

TransUnion: 800 680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

- *Place a Security Freeze on Your Account.* In addition to a fraud alert, you may also have a security freeze placed on your credit file. A security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services. The fees for placing a security freeze vary by state, and a consumer reporting agency may charge a fee of up to \$10.00 to place a freeze or lift or remove a freeze. To place a security freeze on your credit report, you may send a written request to each of the major consumer reporting agencies by regular, certified, or overnight mail. You can also place security freezes online by visiting each consumer reporting agency online.

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp; Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348;

Experian: 888 397-3742; <https://www.experian.com/freeze/center.html>; Experian Security Freeze, P.O. Box 9554, Allen, TX 75013;

TransUnion: <https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>; TransUnion LLC, P.O. Box 2000, Chester, PA 19016

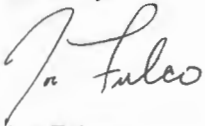
- *Contact Law Enforcement.* If you believe you are the victim of identity theft, you should immediately contact your local law enforcement agency, your state's attorney general, or the Federal Trade Commission. Please visit <http://www.ftc.gov/idtheft> or call 1-877-ID-THEFT (877-438-4338), or write to the Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580 for additional guidance. Your complaint will be added to the FTC's Identity Theft Data Clearinghouse, where it will be accessible to law enforcement for investigation.

Other Important Information

- *Federal Trade Commission.* The Federal Trade Commission also provides helpful information about fraud alerts, security freezes, and how to avoid identity theft.
- *State-Specific Information.* If you are a resident of one of the following states, the following information applies to you.
 - For residents of Maryland, North Carolina, and Rhode Island: For information on how to avoid identity theft or to contact your state's attorney general, please use the below information:
Maryland Attorney General, 1-410-576-6491, ldtheft@oag.state.md.us, Identity Theft Unit, Attorney General of Maryland, 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, <https://www.oag.state.md.us/>; **North Carolina Attorney General**, 1-877-566-7226 (within North Carolina) or 1-919-716-6000 (if outside North Carolina), consumer@ncdoj.gov, Consumer Protection Division, Attorney General's Office, Mail Service Center 9001, Raleigh, NC 27699-9001, <http://www.ncdoj.gov>; **Rhode Island Attorney General**, 1-401-274-4400, consumers@riag.ri.gov; Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov/>
 - For residents of Massachusetts: Please see the enclosed "Information for Massachusetts Residents".
 - For residents of Rhode Island: Under Rhode Island law, you have the right to obtain a police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Fruitful Yield sincerely apologizes for any inconvenience this may cause you. We appreciate that you have chosen to do business with us and we are taking the necessary steps to regain your trust. Should you have any questions or concerns, please contact: 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time.

Sincerely,



Joe Fulco
General Manager
The Fruitful Yield, Inc.

INFORMATION for Massachusetts Residents

You have a right to obtain a police report. You also have a right to be informed about how to request a security freeze, the necessary information to be provided when requesting a security freeze, and information regarding any fees required to be paid to any of the consumer reporting agencies for placing a security freeze. In addition to the security freeze information provided in the letter, please note the following:

As noted above, a security freeze will block a credit bureau from releasing information from your credit report without your prior written authorization. Please be aware that it may delay, interfere with, or prevent the timely approval of any requests you make for new loans, mortgages, employment, housing or other services.

If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze.

To place a security freeze on your credit report, you must send a written request to each of the three major consumer reporting agencies by regular, certified or overnight mail at the addresses below:

Equifax: https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp; Equifax Security Freeze, P.O. Box 105788, Atlanta, Georgia 30348;

Experian: 888 397-3742; <https://www.experian.com/freeze/center.html>; Experian Security Freeze, P.O. Box 9554, Allen, TX 75013;

TransUnion: <https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp>; TransUnion LLC, P.O. Box 2000, Chester, PA 19016

To request a security freeze, you will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
- Social Security Number;
- Date of birth;
- If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years;
- Proof of current address such as a current utility bill or telephone bill;
- A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.); and
- If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.
- If you are not a victim of identity theft, include payment by check, money order, or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number (PIN) or password, or both, that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze, as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Take Advantage of your Identity Monitoring Services:

We are offering you access to a complimentary 12-month membership of identity monitoring services through Kroll.

To enroll, visit: <<IDMonitoringURL>> and follow the online instructions to take advantage of your identity monitoring services.¹

You have until <<Date>> to activate your identity monitoring services.

Membership Number: <<Member ID>>

If you require assistance with activation or would like to enroll and receive credit services by mail instead of online, please call 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:00 p.m. Central Time.

Once you activate, your identity monitoring services include:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who can help you determine if it's an indicator of identity theft.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your Social Security number. If information is found, you'll receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You'll receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator can dig deep to uncover the scope of the identity theft, and then work to resolve it.

¹ Kroll's activation website is only compatible with the current version or one version earlier of Internet Explorer, Chrome, Firefox, and Safari. To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.