October 6, 2020

Anjali C. Das
312.821.6164 (direct)
Anjali.Das@wilsonelser.com

Via E-MAIL

Attorney General Bob Ferguson
Attorney General's Office
1123 Washington Street
P.O. Box 40100
Olympia, WA 98504
SecurityBreach@atg.wa.gov

Re: Data Security Incident

Dear Attorney General Ferguson:

Wilson Elser Moskowitz Edelman and Dicker LLP ("Wilson Elser") represents Gymshark Limited ("Gymshark") with regard to a data security incident (hereinafter, the "Incident") involving Shopify Inc. ("Shopify") described in more detail below.

Gymshark is an online fitness apparel store based in the United Kingdom, and Shopify is an e-commerce website hosting platform that is used by Gymshark and many other merchants. Gymshark operates globally and has several dedicated online stores for specific regions of the world, including the United States.

1. Nature of the security Incident.

On Friday, September 18, 2020 Shopify first informed Gymshark, as well as around two hundred (200) other Shopify merchants, about a data security incident that occurred on the Shopify platform. Specifically, Shopify informed Gymshark that personal information belonging to Gymshark's customers was accessed in an unauthorized fashion by Philippines-based Shopify contractors. The potentially-impacted Gymshark customers include resident of the State of Washington, as described below. The personal information that was affected includes Gymshark customers' names, addresses, dates of birth and partial payment card numbers. Shopify has assured Gymshark that Gymshark customer account passwords and complete credit card and debit card information was not obtained as a result of the incident.

2. Number of Washington residents affected.

According to information Gymshark received from Shopify, fifty-nine thousand, seven hundred sixty-nine (59,769) Washington residents were potentially affected by this Incident. Of this population, fourteen thousand eight hundred and twenty-two (14,822) individuals' dates of birth were exposed. Gymshark first notified affected residents of Washington State of the Incident on October 5, 2020, via email. Residents of Washington State whose dates of birth were exposed as a result of the Incident will receive an additional incident notification letter from Gymshark, mailed to their home address, on or about October 13, 2020. A sample copy of the Incident notification email that was sent to potentially affected residents of Washington on October 5, 2020 is included with this letter at **Exhibit A**.

3. Steps taken.

Gymshark takes the security of all information in its control very seriously, and is taking steps to mitigate the risks posed by this incident. Specifically, immediately after learning about this incident Gymshark communicated with Shopify, carried out exhaustive internal investigations, and engaged an external third-party forensics team to conduct an investigation and learn more about the incident. Gymshark has encouraged Washington residents to remain vigilant in response to this incident and also provided an addendum to affected residents which includes additional information and steps Washington residents can take to further safeguard their personal information.

4. Contact information.

Gymshark remains dedicated to protecting the sensitive information in its control. If you have any questions or need additional information, please do not hesitate to contact me at Anjali.Das@WilsonElser.com or (312)-821-6164.

Very truly yours,

Wilson Elser Moskowitz Edelman & Dicker LLP

Anjali C. Das

Enclosure

EXHIBIT A

Subject Heading: Important notice about your Data
Preview: A message from our CEO Steve Hewitt

Hey [Name],

We only ever want to hit your inbox with positivity and awesome new products, but we need to get a little serious for a second. Here's the lowdown:

Our website platform is hosted by our e-commerce partner, Shopify. Recently, there was an incident at Shopify involving the data it collects and holds for us, as well as around 200 other Shopify merchants. First of all, before you sweat too much…

This data does **not** include:

- Full payment card numbers
- CVV numbers
- Passwords

But it **does** include:

- Name
- Date of Birth
- Email address
- Postal address
- Telephone number
- First and last few numbers of payment card (again, **not** the full payment card number)
- Other information related to orders

In this case, we're sorry to say that your data was involved in the incident. There's nothing pressing that you need to do, as your financial information and password are safe. Just a heads up, though, that you may be more exposed to illegitimate communications (such as scam emails or messages), so please be super conscious of that, especially if you receive anything that seems strange or claims to be from Gymshark. We will be following this email up with a similar postal notification to your door though, so that's something you should expect from us in the near future.

You may have some questions, and understandably so, so we've put together a quickfire Q&A below, and we've set up a bespoke live chat service for any questions we haven't covered at http://notice.gymshark.com/.

Again, we're really sorry to have to tell you this, but please know that we, and Shopify, are taking this very seriously. The Gymshark family – and its trust in us – is our first, last and everything in between. We'll honour that here.

Steve Hewitt
CEO

Customer Q&A

So, what exactly has happened?

Shopify have told us that two rogue members of its support team were involved in a plan to obtain customer transactional records. You can read more about the details of the incident here.

What's Shopify doing about it?

As soon as Shopify discovered what happened, it launched an investigation with law enforcement and third-party experts in data and cyber forensics to understand what information was taken, how it was taken and who it was taken by.

How could this happen?

That's a good question, and it's one we've asked Shopify. We need to let their team finish the investigation and work with law enforcement before we get the answer, but we're keeping in very close contact with Shopify to protect your data going forward.

How can you be sure that my full credit card details haven't been taken?

Shopify doesn't handle payments for Gymshark purchases, meaning they don't actually have access to full payment card details. We use separate partners to handle card payments which haven't been affected by this incident at Shopify. We're confident full card numbers and CVV numbers weren't taken.

Am I safe to shop the Gymshark website now?

Absolutely! We understand that this incident wasn't the result of a technical fault in the Shopify platform – it's simply down to two rogue Shopify employees, and their access and employment has now been terminated. We're in close contact with Shopify, and we're confident this incident is being dealt with thoroughly.

What should I do?

Your financial information and password are safe. Please just be super conscious of any emails or other communications that you aren't expecting or that look different than normal.

My friend/family member bought something from Gymshark but hasn't received this email. How come?

We're actively emailing all Gymshark customers who've been affected by this incident. If your friends or family members haven't heard from us, it's because there's nothing for them to hear and their data hasn't been affected.

---ends---

Gymshark Ltd
GSHQ
Blythe Valley Park
3 Central Boulevard
Solihull
B90 8AB

[insert date] October 2020

Hey [insert name]

We're writing to inform you of a data security incident involving Shopify Inc. ("Shopify"), our e-commerce website platform provider that may have resulted in the unauthorized access to some of your personal information.

We're really sorry to have to tell you this, but please know that we, and Shopify, are taking this very seriously. Your trust in us is our priority so we wanted to tell you what has happened, the action we, and Shopify have taken, and the resources we are making available to you to protect your information going forward.

On September 18 2020, Shopify informed us about a data security incident that occurred on or around 25th August 2020 on its platform, affecting Gymshark and around 200 other Shopify merchants.

As a result of this incident, some of your personal information may have been viewed by unauthorized individuals, including your name, address, date of birth and partial credit card or debit card number. We want to reassure you that account passwords and complete credit card and debit card information was not obtained.

We take the security of all information in our control very seriously and are taking steps to minimize the risks posed by this incident. Since learning about this, we have communicated with Shopify, carried out exhaustive internal investigations and engaged an external third-party forensics team to investigate. We encourage you to stay alert and have included a resource below which covers additional information and steps you can take to further protect your personal information for the future.

You may have some additional questions, and understandably so, so we've put together an FAQ page for any questions you may have at www.notice.gymshark.com/. If you've got any questions or concerns that aren't fixed by these FAQs, remember you can always contact our support team at www.gymshark.com/contact/.

Washington law also allows consumers to place a security freeze on their credit reports, free of charge**.** A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. Just be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit mortgages, employment, housing or other services.

To place a security freeze on your credit report, you'll need to make a direct request by telephone, secure electronic means (website), or written request to each of the three major consumer reporting agencies: Equifax; Experian; and TransUnion at the addresses and/or numbers below:

Equifax Security Freeze P.O. Box 105788 Atlanta, GA 30348 my.equifax.com/consumer-registration (800) 349-9960	Experian Security Freeze P.O. Box 9554 Allen, TX 75013 experian.com/freeze (888) 397-3742	TransUnion Security Freeze Fraud Victim Assistance Dept. P.O. Box 2000 Chester, PA 19022-2000 transunion.com/credit-freeze (888) 909-8872

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

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.).
2. Social Security number.

3. Date of birth.
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five (5) years.
5. Proof of current address, such as a current utility bill or telephone bill.
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. 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.

The credit reporting agencies have one (1) business day after receiving a telephone or secure electronic request, or three (3) business days after receiving your written 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 permanently remove the security freeze, or to temporarily lift the security freeze for a specified period of time or to provide a specified entity access to your credit report, you must make a request either by phone, through secure electronic means (online), or by sending a written request to the credit reporting agencies by mail. Requests must include proper identification (name, address, and Social Security number) and the PIN or password provided to you when you placed the security freeze. To temporarily remove the security freeze, include the specific period of time you want the credit report available or the name of the entity you want to have access to your credit report.

If your request is by phone or made online, the security freeze will be lifted within one (1) hour after receiving the request for removal; or in the case of a request that is by mail, the credit reporting agencies have three (3) business days after receiving your request to permanently or temporarily remove the security freeze.

Again, we're really sorry to have to tell you this, but please know that we, and Shopify, are taking this very seriously. The Gymshark family, and its trust in us is our first, last and everything in between.

Steve Hewitt, CEO

Additional Important Information

For residents of *Hawaii, Michigan, Missouri, Virginia, Vermont,* and *North Carolina*: It is recommended by state law that you remain vigilant for incidents of fraud and identity theft by reviewing credit card account statements and monitoring your credit report for unauthorized activity.

For residents of *Illinois, Iowa, Maryland, Missouri, North Carolina, Oregon*, and *West Virginia*:
It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account. You may obtain a free copy of your credit report from each of the three nationwide credit reporting agencies. To order your 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 at https://www.consumer.ftc.gov/articles/0155-free-credit-reports) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA, 30348-5281.

For residents of *Iowa*:
State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of *Oregon*:
State laws advise you to report any suspected identity theft to law enforcement, including the Attorney General, and the Federal Trade Commission.

For residents of Arizona, Colorado, Maryland, Rhode Island, Illinois, New York, and North Carolina:
You can obtain information from the Offices of the Attorney General and the Federal Trade Commission about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Maryland Office of the Attorney General Consumer Protection Division 200, St. Paul Place Baltimore, MD 21202 1-888-743-0023 www.oag.state.md.us
Rhode Island Office of the Attorney General Consumer Protection 150 South Main Street, Providence RI 02903 1-401-274-4400 www.riag.ri.gov
North Carolina Office of the Attorney General Consumer Protection Division, 9001 Mail Service Center Raleigh, NC 27699-9001 1-877-566-7226 www.ncdoj.com
Federal Trade Commission Consumer Response Center, 600 Pennsylvania Ave, NW Washington, DC 20580 1-877-IDTHEFT (438-4338) www.ftc.gov/idtheft
New York Office of Attorney General Consumer Frauds & Protection, The Capitol Albany, NY 12224 1-800-771-7755 https://ag.ny.gov/consumer-frauds/identity-theft
Colorado Office of the Attorney General Consumer Protection 1300 Broadway, 9th Floor, Denver, CO 80203 1-720-508-6000 www.coag.gov
Arizona Office of the Attorney General Consumer Protection & Advocacy Section, 2005 North Central Avenue, Phoenix, AZ 85004 1-602-542-5025
Illinois Office of the Attorney General Consumer Protection Division 100 W Randolph St., Chicago, IL 60601 1-800-243-0618 www.illinoisattorneygeneral.gov

For residents of *Massachusetts*: It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft

For residents of all states:

Fraud Alerts: You can place fraud alerts with the three credit bureaus by phone and online with Equifax (https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf);TransUnion (https://www.transunion.com/fraud-alerts); or Experian (https://www.experian.com/fraud/center.html). A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. As of September 21, 2018, initial fraud alerts last for one year. Victims of identity theft can also get an extended fraud alert for seven years. The phone numbers for all three credit bureaus are at the bottom of this page.

Monitoring: You should always remain vigilant and monitor your accounts for suspicious or unusual activity.

Security Freeze: You also have the right to place a security freeze on your credit report. A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you need to make a request to each consumer reporting agency. You may make that request by certified mail, overnight mail, regular stamped mail, or by following the instructions found at the websites listed below. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse or a minor under the age of 16, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, display your name and current mailing address, and the date of issue. As of September 21, 2018, it is free to place, lift, or remove a security freeze. You may also place a security freeze for children under the age of 16. You may obtain a free security freeze by contacting any one or more of the following national consumer reporting agencies:

Equifax Security Freeze	**Experian Security Freeze**	**TransUnion (FVAD)**
P.O. Box 105788	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348	Allen, TX 75013	Chester, PA 19022
www.freeze.equifax.com	www.experian.com/freeze	freeze.transunion.com
800-525-6285	888-397-3742	800-680-7289

More information can also be obtained by contacting the Federal Trade Commission listed above.