Appendix

We are writing on behalf of our client, Fat Face, to provide additional information pertaining to the security incident previously reported to your office on March 25, 2021, which involves twenty Maine residents. Per our initial notification letter, on January 17, 2021, Fat Face identified some suspicious activity within its network. Upon discovering the incident, Fat Face immediately took steps to secure its network. In addition, a cybersecurity firm was engaged, and a thorough investigation was conducted. The investigation determined that an unauthorized third party gained access to certain systems operated by Fat Face between December 25, 2020 and January 18, 2021. After completing additional review of the systems involved, on April 15, 2021, Fat Face identified two additional Maine residents[1] whose names and one or more of the following were potentially involved: (1) Social Security numbers; and (2) financial account information, including account numbers and routing numbers.

Beginning today, April 27, 2021, Fat Face is providing written notice to the Maine residents by mailing a letter via United States Postal Service First-Class mail. A sample copy of the notification letter is enclosed. Fat Face is offering a complimentary, one-year membership of identity monitoring services provided by Experian to the Maine residents. Fat Face also established a dedicated phone number where all twenty Maine residents involved may obtain more information regarding the incident.

To help prevent a similar incident from occurring in the future, Fat Face is taking steps to further enhance its existing security measures.

[1] Fat Face discovered that the personal information of a total of twenty Maine residents was potentially involved.

FATFACE

<<Date>>

<<First Name>> <<Last Name>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<Zip>>

Notice of security incident – USFS042021(1)

Dear <<First Name>>:

We are contacting you as one of our valued former employees to let you know about a recent security incident which involved some of our systems, including those that potentially held some information about you.

While we are unaware of any attempted or actual misuse of any of your information, out of an abundance of caution, we wanted to give you some information about the event so that you can understand what happened, how you may be involved, the steps we have taken, and some steps you can take in response.

We would like to reassure you this incident is now resolved, that our systems are fully secure, and your information is safe.

What Happened?
On January 17, 2021, FatFace identified some suspicious activity within its IT systems. We immediately launched an investigation with the assistance of experienced security specialists who, following thorough investigation, determined that an unauthorized third party had gained access to certain systems operated by us during a limited period of time earlier the same month. FatFace quickly contained the incident and started the process of reviewing and categorizing the data potentially involved in the incident.

On April 15, 2021, we completed additional analysis and discovered that information pertaining to you may have been included in the affected systems. We are contacting you because we want to provide as much information as possible to assist you.

What We Have Done.
FatFace takes the security of your information extremely seriously. As soon as we became aware of the incident, we launched an investigation with assistance from experienced third-party security specialists. Over the past weeks, our teams have been working flat out to fully investigate the circumstances of the incident and confirm whose data may have been involved.

FatFace had various preventative security measures in place at the time of this incident to protect your data, in line with the expected security practices and related technology for the retail sector FatFace operates in. Unfortunately, like many organizations, we were subject to a sophisticated criminal attack which involved access to our systems despite these measures.

Consistent with our focus on care for our personnel and regulatory requirements, FatFace's priority has been to clearly identify who was (and was not) involved in this incident and to identify precisely what information was involved, so that we could explain to you what happened and let you know what you can do in response. This identification effort was comprehensive and coordinated by our external security experts; it therefore took time to thoroughly analyze and categorize the data to ensure we can provide the most accurate information possible.

As an organization, the security of data, including your information, is a top priority and we take the protection of personal and business data very seriously. We have been working with the relevant authorities and external security experts to ensure a comprehensive response to the incident. In addition, we have notified law enforcement authorities of this incident.

We have taken various additional steps to further strengthen the security of our systems. Please rest assured that our systems are secure, our website remains fully operational, and FatFace is a safe place to shop, both in-store (when we can reopen our shops) and online.

What Information was Involved?
Some of your personal data may have been involved in the incident. This could include some or all of the below listed categories of employment-related information relating to you.

- first name and surname;
- Social Security number; and/or
- bank details (routing number and account number).

What You Can Do.
As a general matter and for best practice, we would encourage you to remain vigilant to everyday phishing attempts including any risk of identity theft and fraud which, unfortunately, is generally prevalent during the current COVID-19 pandemic. There are various steps you can take to help protect your personal information including those set out below.

- Continue to be alert to the risk of phishing and any related fraud including any emails asking you to enter login credentials, provide financial information or give up any other personal data.
- Check your bank statement regularly for any unusual activity that you do not recognize.
- Check your Experian Credit Report regularly for newly opened accounts or credit searches that you do not recognize.
- Use strong passwords and change them regularly. Use passwords which are at least eight characters long and use numbers, upper case, lower case and symbols.
- Never give out personal details over the phone unless you are sure who you are speaking to.

Please note we would never contact you by email to ask you to provide us with any payment card information. To give you peace of mind, we are offering you one year of Experian credit and web monitoring services at no cost to you.

Your Complimentary Experian® IdentityWorks℠ Credit 3B Membership.

We are offering you a complimentary one-year membership in Experian® IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with identity protection services focused on immediate identification and resolution of identity theft. IdentityWorks is completely free to you and enrolling in this program will not hurt your credit score.

For more information on identity theft prevention, further steps you can take in response, and instructions on how to activate your complimentary one-year membership, please see the additional information provided with this letter.

For More Information:
If you have any questions about the incident, we have set up a dedicated support line on Tel. +44 (0)20 7129 7049. Alternatively, noting the above options are more likely to offer a quicker response time, if you would like to reach us by email then please contact us at: individualenquiries@fatface.com.

The security of personal data really is a priority at FatFace. We can assure you that we have been doing, and will continue to do, everything we can to ensure the ongoing resilience of our systems and to prevent this type of incident from occurring again.

Sincerely,

Liz Evans
Chief Executive Officer | FatFace Limited

ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a complimentary one-year membership of Experian's® IdentityWorks℠. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by**: **July 31, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: link
- Provide your **activation code**: **[code]**

If you have questions about the product, need assistance with identity restoration or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at **877.288.8057** by **July 31, 2021.** Be prepared to provide engagement number **xx** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR ONE-YEAR EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian, Equifax and Transunion files for indicators of fraud.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARE™**: You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to $1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at **877.288.8057**. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

* Offline members will be eligible to call for additional reports quarterly after enrolling.

** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any 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 companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

- *Federal Trade Commission*, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

Fraud Alerts and Credit or Security Freezes:

Fraud Alerts: There are two types of general fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.
After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

FatFace's mailing address is Unit 3 Ridgway, Havant, Hampshire, PO9 1QJ, England and its phone number is +44 (0)330 124 0000.

Additional information for residents of the following states:

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov.

Rhode Island: This incident involves twenty-six Rhode Island residents. Under Rhode Island law, you have the right to file and obtain a copy of a police report. You also have the right to request a security freeze, as described above. You may contact and obtain information from your state attorney general at: *Rhode Island Attorney General's Office*, 150 South Main Street, Providence, RI 02903, 1-401-274-4400, www.riag.ri.gov.