BakerHostetler

RECEIVED

MAR 26 2021

CONSUMER PROTECTION

Baker&Hostetler LLP

2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891

T 215.568.3100
F 215.568.3439
www.bakerlaw.com

David B. Sherman
direct dial: 215.564.8380
dsherman@bakerlaw.com

March 25, 2021

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

We are writing on behalf of our client, Fat Face, to notify you of a security incident potentially involving seventeen New Hampshire residents. Fat Face is a clothing and accessories retailer based in the United Kingdom.

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. Fat Face then completed a careful review of the systems involved to identify what information they contained, and on March 9, 2021, Fat Face determined that the files contained the personal information of seventeen New Hampshire residents, including the residents' name and one or more of the following data elements: (1) Social Security number; (2) driver's license number; and/or (3) financial account information including routing number and account number.

Beginning today, March 25, 2021, Fat Face is providing written notice to the New Hampshire residents by mailing a letter via United States Postal Service First-Class mail. Sample copies of the notification letters are enclosed. Fat Face is offering a complimentary, one-year membership of identity monitoring services provided by Experian to the involved individuals. Fat Face also established a dedicated phone number where the individuals 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.

Please do not hesitate to contact me if you have any questions regarding this incident.

Sincerely,

David B. Sherman
Partner

Enclosures

FATFACE

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 25, 2021

G3296-L01-0000001 T00001 P001 *****AUTO**MIXED AADC 159
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Strictly private and confidential - Notice of security incident – [redacted]

Dear Sample A. Sample,

We are contacting you as one of our valued 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 that this incident is now resolved, that our systems are fully secure, and your information is safe.

Please do keep this letter and the information included within it strictly private and confidential.

What Happened?
On January 17, 2021, Fat Face 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. Fat Face quickly contained the incident and started the process of reviewing and categorizing the data potentially involved in the incident.

On March 9, 2021, we completed our review and discovered that your information 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.
Fat Face 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.

Fat Face 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 Fat Face 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 customer care and regulatory requirements, Fat Face'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 Fat Face 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 together with any information connected to any of your online purchases via our website as a customer, where applicable.

- first name and surname;
- Social Security number;
- driver's license;
- passport 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 that 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 12 months 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 12-month 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)20-7138-9090, which will be open for a period of 3 weeks. The support line will be operating from Monday to Friday (4 am to 2 pm ET / 8am to 6pm GMT) and also open on Saturday, March 27, 2021, and Sunday, March 28, 2021 (4 am to 2 pm ET / 8am to 6pm GMT).

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: employeeenquiries@fatface.com.

The security of personal data really is a priority at Fat Face. 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.

Finally, I wanted to say that I regret that it has been necessary to contact you in such circumstances and to thank you for your ongoing support.

Sincerely,

Liz Evans.

Liz Evans
Chief Executive Officer | Fat Face Limited

0000001

G3296-L01

ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a **complimentary** 12-month membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **June 30, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: ABCDEFGHI**

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) 890-9332**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit
or call (877) 890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **(877) 890-9332**.

* 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.

Fat Face'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-four 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.

FATFACE

Return Mail Processing
PO Box 589
Claysburg, PA 16625-0589

March 25, 2021

G3296-L04-0000004 T00001 P001 *****AUTO**MIXED AADC 159
APT ABC
123 ANY ST
ANYTOWN, ST 12345-6789

Strictly private and confidential - Notice of security incident – [redacted]

Dear Sample A. Sample,

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.

Please do keep this email and the information included within it strictly private and confidential.

What Happened?
On January 17, 2021, Fat Face 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. Fat Face quickly contained the incident and started the process of reviewing and categorizing the data potentially involved in the incident.

On March 9, 2021, we completed our review and discovered that your information 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.
Fat Face 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.

Fat Face 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 Fat Face 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 customer care and regulatory requirements, Fat Face'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 Fat Face 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 together with any information connected to any of your online purchases via our website as a customer, where applicable.

- first name and surname;
- Social Security number;
- driver's license;
- passport number;
- date of birth; and
- 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 12 months 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 12-month membership, please see the additional information provided with this letter.tm

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, which will be open for a period of 3 weeks. The support line will be operating from Monday to Friday (4 am to 2 pm ET / 8am to 6pm GMT) and also open on Saturday, March 27, 2021, and Sunday, March 28, 2021 (4 am to 2 pm ET / 8am to 6pm GMT).

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 Fat Face. 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.

Liz Evans
Chief Executive Officer | Fat Face Limited

0000004

G3296-L04

ENROLLMENT INSTRUCTIONS

To help protect your identity, we are offering a **complimentary** 12-month membership of Experian IdentityWorks℠ Credit 3B. This product helps detect possible misuse of your personal information and provides you with superior identity protection support focused on immediate identification and resolution of identity theft.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

1. ENROLL by: **June 30, 2021** (Your code will not work after this date.)
2. VISIT the **Experian IdentityWorks website** to enroll: **https://www.experianidworks.com/3bcredit**
3. PROVIDE the **Activation Code: ABCDEFGHI**

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) 890-9332**. Be prepared to provide engagement number [redacted] as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 12-MONTH EXPERIAN IDENTITYWORKS CREDIT 3B MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorks Credit 3B.

You can contact Experian **immediately without needing to enroll in the product** regarding any fraud issues. Identity Restoration specialists are available to help you address credit and non-credit related fraud.

Once you enroll in Experian IdentityWorks, you will have access to the following additional features:

- **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.
- **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

Activate your membership today at https://www.experianidworks.com/3bcredit or call (877) 890-9332 to register with the activation code above.

What you can do to protect your information: There are additional actions you can consider taking to reduce the chances of identity theft or fraud on your account(s). Please refer to www.ExperianIDWorks.com/restoration for this information. If you have any questions about IdentityWorks, need help understanding something on your credit report or suspect that an item on your credit report may be fraudulent, please contact Experian's customer care team at **(877) 890-9332**.

* 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.

Fat Face'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:

Maryland: You may contact and obtain information from your state attorney general at: *Maryland Attorney General's Office*, 200 St. Paul Place, Baltimore, MD 21202, 1-888-743-0023 / 1-410-576-6300, www.oag.state.md.us

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.

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov.

Rhode Island: This incident involves twenty-four 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.