



MULLEN
COUGHLIN LLC
ATTORNEYS AT LAW

STATE OF NH
DEPT. OF JUSTICE

2019 JAN 28 P 3: 14

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 24, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General MacDonald:

Please see the enclosed Notice of Data Event which was postmarked on Friday, January 18, 2019 but returned to our office due to a postage error.

We appreciate your courtesy in this regard.

Very truly yours,

Christopher J. DiIenno of
MULLEN COUGHLIN LLC

CJD/plm
Enclosure



MULLEN
COUGHLIN_{LLC}
ATTORNEYS AT LAW

Christopher J. DiIenno
Office: 267-930-4775
Fax: 267-930-4771
Email: cdiienno@mullen.law

1275 Drummers Lane, Suite 302
Wayne, PA 19087

January 18, 2019

VIA U.S. MAIL

Attorney General Gordon J. MacDonald
Office of the New Hampshire Attorney General
Attn: Security Breach Notification
33 Capitol Street
Concord, NH 03301

Re: Notice of Data Event

Dear Attorney General Gordon J. MacDonald:

We represent Data Facts, Inc. ("Data Facts"), 8000 Centerview Parkway, Cordova, Tennessee 38018, and we write to notify your office of an incident that may affect the security of personal information relating to five (5) New Hampshire residents. Data Facts is a national and international provider of background screening solutions for clients such as, Symmetry Medical dba Tecomet. Data Facts' investigation into this event is ongoing and this notice will be supplemented with any new significant facts learned subsequent to its submission or additional requests from Data Facts clients to provide notice on their behalf. By providing this notice, Data Facts does not waive any rights or defenses regarding the applicability of New Hampshire law, the applicability of the New Hampshire data event notification statute, or personal jurisdiction.

Nature of the Data Event

On November 5, 2018, Data Facts learned that a Data Facts employee email account was accessed by an unknown party. That account contained personally identifiable information provided to Data Facts by clients for the purpose of conducting background checks. Although Data Facts has no evidence to suggest that private information was misused, the possibility that emails and/or attachments in the account were viewed by the unauthorized party could not be ruled out. On December 7, 2018, Data Facts' investigation confirmed Symmetry Medical dba Tecomet's consumers' information was present in the account.

Data Facts takes data privacy and this incident very seriously. Immediately upon becoming aware of the incident, Data Facts took steps to block access to the account by resetting passwords and hired a leading forensics firm to help investigate. Through that investigation and following an extensive programmatic and manual review of the emails and attachments, Data Facts determined that an unauthorized party had access to records which may have included consumer name, address, Social Security number and Driver's license number.

Notice to New Hampshire Residents

On or about December 20, 2018, Data Facts began notifying the affected Clients whose consumers' sensitive information was present in the account and offered to notify affected consumers and applicable regulators on their behalf.

On January 18, 2018, Data Facts mailed written notice of this incident to five (5) New Hampshire residents affected in the incident, on behalf of Symmetry Medical dba Tecomet in substantially the same form as the letter attached hereto and labeled as *Exhibit A*.

Other Steps Taken and To Be Taken

Upon discovering this incident, Data Facts immediately launched an investigation to determine the nature and scope of the event, as well as whose data may potentially be affected. At Symmetry Medical dba Tecomet's request, Data Facts is mailing written notice to affected consumers and certain regulators. This notice includes guidance on how to better protect against identity theft and fraud, how to place a fraud alert and security freeze on one's credit file, the contact details for the national consumer reporting agencies, information on how to obtain a free credit report, a reminder to remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring free credit reports, and encouragement to contact the Federal Trade Commission, their state Attorney General, and law enforcement to report attempted or actual identity theft and fraud. As an added precaution, Data Facts arranged to have AllClear ID provide the affected consumers twelve (12) months of credit monitoring and identity restoration services at no cost to the individual. Data Facts is also providing notice of this event to other state and federal regulators as requested

Data Facts has taken steps to ensure the security of the information they store. As part of its ongoing efforts to help prevent another incident from occurring in the future, it is re-educating employees on cyber best practices and enhancing existing security measures by implementing two-factor authentication for remote email access. Data Facts also implemented a 60-day forced password reset protocol across all systems and subscribed to an email security program for inbound and outbound filtering and blocking of emails potentially containing personally identifiable information.

Attorney General Gordon J. MacDonald
January 18, 2019
Page 3

Contact Information

Should you have any questions regarding this notification or other aspects of the data security event, please contact us at 267-930-4775.

Very truly yours,

A handwritten signature in black ink, appearing to read "C. DiLenno".

Christopher J. DiLenno of
MULLEN COUGHLIN LLC

CJD/NSJ
Enclosure

EXHIBIT A


00007
R90140D




January 18, 2019

Notice of Data Breach

Dear :

Data Facts is a national and international provider of background screening solutions. Recently, Data Facts processed your background check on behalf of . Regrettably, we are writing to inform you about an incident involving certain information provided to us during the background check process.

What Happened? On November 5, 2018, we confirmed that one of our employee email accounts was accessed by an unknown party. That account contained personally identifiable information provided to us by clients for the purpose of conducting a background check. Although we do not have any evidence that private information was exported or misused, we could not rule out the possibility that emails and/or attachments in the account may have been viewed by the unauthorized party.

What Information Was Involved? Immediately upon becoming aware of the incident, Data Facts took steps to block access to the account, and hired a leading forensics firm to help investigate. Through that investigation, we determined that an unauthorized party may have viewed emails in the affected account containing your personal information, which may have included some or all of the following: 

What We Are Doing. Data Facts takes this incident very seriously and, as part of our ongoing efforts to help prevent something like this from happening in the future, we are re-educating our employees on cyber best practices and enhancing existing security measures by implementing two-factor authentication for remote email access. We sincerely regret that this incident occurred and apologize for any concern this may cause you.

What You Can Do. Further, Data Facts is offering 12 months of complimentary credit monitoring and identity theft protection services through AllClear ID. Please see the attached information for instructions on how to activate the monitoring services.



For More Information. We regret any inconvenience or concern this may cause you. If you have any questions, please call 1-855-239-9532 between 8:00 am and 8:00 pm CT, Monday through Saturday, excluding major holidays.

Sincerely,

A handwritten signature in black ink, appearing to read "Daphne J. Large". The signature is fluid and cursive, with the first name being the most prominent.

Daphne Large, CEO

Credit Monitoring

As an added precaution, we have arranged to have AllClear ID protect your identity for 12 months at no cost to you. The following identity protection services start on the date of this notice and you can use them at any time during the next 12 months.

AllClear Identity Repair: This service is automatically available to you with no enrollment required. If a problem arises, simply call 1-855-239-9532 and a dedicated investigator will help recover financial losses, restore your credit and make sure your identity is returned to its proper condition.

AllClear Fraud Alerts with Credit Monitoring: This service offers the ability to set, renew, and remove 90-day fraud alerts on your credit file to help protect you from credit fraud. In addition, it provides credit monitoring services, a once annual credit score and credit report, and a \$1 million identity theft insurance policy. For a child under 18 years old, AllClear ID ChildScan identifies acts of fraud against children by searching thousands of public databases for use of your child's information. To enroll in this service, you will need to provide your personal information to AllClear ID. You may sign up online at enroll.allclearid.com or by phone by calling 1-855-239-9532 using the following redemption code: Redemption Code.

Please note: Following enrollment, additional steps are required by you in order to activate your phone alerts and fraud alerts, and to pull your credit score and credit file. Additional steps may also be required in order to activate your monitoring options.

Consumer Financial Protection Bureau

Remedying the Effects of Identity Theft *Para informacion en espanol, visite www.consumerfinance.gov/learnmore o escribe a la* Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

You are receiving this information because you have notified a consumer reporting agency that you believe that you are a victim of identity theft. Identity theft occurs when someone uses your name, Social Security number, date of birth, or other identifying information, without authority, to commit fraud. For example, someone may have committed identity theft by using your personal information to open a credit card account or get a loan in your name. For more information, visit www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

The Fair Credit Reporting Act (FCRA) gives you specific rights when you are, or believe that you are, the victim of identity theft. Here is a brief summary of the rights designed to help you recover from identity theft.

1. You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you. It also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide consumer reporting agencies. As soon as that agency processes your fraud alert, it will notify the other two, which then also must place fraud alerts in your file.

- Equifax: 1-800-685-1111; www.equifax.com
- Experian: 1-888-397-3742; www.experian.com
- TransUnion: 1-800-888-4213; www.transunion.com

An initial fraud alert stays in your file for at least 90 days. An extended alert stays in your file for seven years. To place either of these alerts, a consumer reporting agency will require you to provide appropriate proof of your identity, which may include your Social Security number. If you ask for an extended alert, you will have to provide an identity theft report. An identity theft report includes a copy of a report you have filed with a federal, state, or local law enforcement agency, and additional information a consumer reporting agency may require you to submit. For more detailed information about the identity theft report, visit www.consumerfinance.gov/learnmore.



2. You have the right to free copies of the information in your file (your "file disclosure"). An initial fraud alert entitles you to a copy of all the information in your file at each of the three nationwide agencies, and an extended alert entitles you to two free file disclosures in a 12-month period following the placing of the alert. These additional disclosures may help you detect signs of fraud, for example, whether fraudulent accounts have been opened in your name or whether someone has reported a change in your address. Once a year, you also have the right to a free copy of the information in your file at any consumer reporting agency, if you believe it has inaccurate information due to fraud, such as identity theft. You also have the ability to obtain additional free file disclosures under other provisions of the FCRA. See www.consumerfinance.gov/learnmore.

3. You have the right to obtain documents relating to fraudulent transactions made or accounts opened using your personal information. A creditor or other business must give you copies of applications and other business records relating to transactions and accounts that resulted from the theft of your identity, if you ask for them in writing. A business may ask you for proof of your identity, a police report, and an affidavit before giving you the documents. It may also specify an address for you to send your request. Under certain circumstances, a business can refuse to provide you with these documents. See www.consumerfinance.gov/learnmore.

4. You have the right to obtain information from a debt collector. If you ask, a debt collector must provide you with certain information about the debt you believe was incurred in your name by an identity thief - like the name of the creditor and the amount of the debt.

5. If you believe information in your file results from identity theft, you have the right to ask that a consumer reporting agency block that information from your file. An identity thief may run up bills in your name and not pay them. Information about the unpaid bills may appear on your consumer report. Should you decide to ask a consumer reporting agency to block the reporting of this information, you must identify the information to block, and provide the consumer reporting agency with proof of your identity and a copy of your identity theft report. The consumer reporting agency can refuse or cancel your request for a block if, for example, you don't provide the necessary documentation, or where the block results from an error or a material misrepresentation of fact made by you. If the agency declines or rescinds the block, it must notify you. Once a debt resulting from identity theft has been blocked, a person or business with notice of the block may not sell, transfer, or place the debt for collection.

6. You also may prevent businesses from reporting information about you to consumer reporting agencies if you believe the information is a result of identity theft. To do so, you must send your request to the address specified by the business that reports the information to the consumer reporting agency. The business will expect you to identify what information you do not want reported and to provide an identity theft report.

To learn more about identity theft and how to deal with its consequences, visit www.consumerfinance.gov/learnmore, or write to the Consumer Financial Protection Bureau. You may have additional rights under state law. For more information, contact your local consumer protection agency or your state Attorney General.

In addition to the new rights and procedures to help consumers deal with the effects of identity theft, the FCRA has many other important consumer protections. They are described in more detail at www.consumerfinance.gov/learnmore.

Additional Steps You Can Take to Protect Against Identity Theft

We encourage you to remain vigilant against incidents of identity theft and fraud, to review your account statements, and to monitor your credit reports for suspicious activity. Under U.S. law you are entitled to one free credit report annually from each of the three major credit reporting bureaus. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also contact the three major credit bureaus directly to request a free copy of your credit report.

You have the 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. Pursuant to federal law, you cannot be charged to place or lift a security freeze on your credit report. Should you wish to place a security freeze, please contact the major consumer reporting agencies listed below:

Experian

P.O. Box 9554
Allen, TX 75013
1-888-397-3742
[www.experian.com/freeze/
center.html](http://www.experian.com/freeze/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016
1-888-909-8872
[www.transunion.com/
credit-freeze](http://www.transunion.com/credit-freeze)

Equifax

P.O. Box 105788
Atlanta, GA 30348-5788
1-800-685-1111
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

In order to request a security freeze, you will 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 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.

As an alternative to a security freeze, you have the right to place an initial or extended “fraud alert” on your 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 seven years. Should you wish to place a fraud alert, please contact any one of the agencies listed below:

Experian

P.O. Box 2002
Allen, TX 75013
1-888-397-3742
[www.experian.com/fraud/
center.html](http://www.experian.com/fraud/center.html)

TransUnion

P.O. Box 2000
Chester, PA 19016
1-800-680-7289
[www.transunion.com/fraud-victim-
resource/place-fraud-alert](http://www.transunion.com/fraud-victim-resource/place-fraud-alert)

Equifax

P.O. Box 105069
Atlanta, GA 30348
1-888-766-0008
[www.equifax.com/personal/
credit-report-services](http://www.equifax.com/personal/credit-report-services)

You can further educate yourself regarding identity theft, fraud alerts, security freezes, and the steps you can take to protect yourself, by contacting the consumer reporting agencies, the Federal Trade Commission, or your state Attorney General.

The Federal Trade Commission can be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580, www.identitytheft.gov, 1-877-ID-THEFT (1-877-438-4338); TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.



For North Carolina residents, the Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001, 1-877-566-7226 or 1-919-716-6400, www.ncdoj.gov.

For Maryland residents, the Attorney General can be contacted at 200 St. Paul Place, 16th Floor, Baltimore, MD 21202, 1-888-743-0023, www.oag.state.md.us.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.