

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

November 20, 2018

RECEIVED
NOV 26 2018
CONSUMER PROTECTION

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing to notify your office of a recent incident at Medtronic Minimed, involving potential unauthorized access to protected health information ("PHI") and personal information of 12 New Hampshire residents.

On October 11, 2018, a document was discovered in a Medtronic facility that contained handwritten sensitive customer personal information about two customers. Upon learning of the incident, Medtronic took immediate action to identify the employee who had taken this information, ensure that access to Medtronic information was suspended, and began a thorough investigation. In the process, we determined that the employee improperly recorded sensitive customer personal information of at least two additional customers. Our investigation has revealed no evidence of broader theft of sensitive personal information and no evidence of any compromise of our systems. However, we are unable to confirm that the employee misappropriated information about only a few known customers. Out of an abundance of caution, and because of the sensitive nature of this information, we are notifying all customers whose sensitive personal or financial information might have been accessed by this employee.

The information potentially accessed and taken may have included customer name, address, phone number, email, date of birth, credit card number, CVC number, credit card expiration date, and social security number.

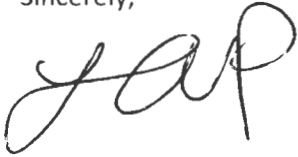
Medtronic began an investigation immediately upon learning of this incident, including a forensic investigation of the employee's workspace, physical documents, computer and our systems. The employee's system access was immediately suspended, and employment has subsequently been terminated.

In addition to the steps described above, we have also contacted the Department of Health and Human Services, and applicable state agencies regarding this incident. We are continuing our investigation, reviewing our policies and procedures, and implementing further training with our employees to avoid any future incidents. Medtronic has also notified law enforcement about the incident.

Notification will be provided to potentially impacted New Hampshire residents on November 21, 2018. A copy of the template notification letter is attached. Medtronic is offering credit monitoring services to all potentially impacted customers for a period of two years, as described in more detail in the attachment to the notification letter.

If you have any questions or require further information, please contact me at lauren.a.popp@medtronic.com or 763-505-0974.

Sincerely,

A handwritten signature in black ink, appearing to read 'L. Popp', written in a cursive style.

Lauren Popp
Data Protection and Privacy
Medtronic
18000 Devonshire St
Northridge, CA 91325

Medtronic Diabetes

C/O ID Experts
PO Box 10444
Dublin, Ohio 43017-4044

To enroll, please call:
(866) 680-8691
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment code: <<XXXXXXXXXX>>

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

November 21, 2018

Dear <<First Name>> <<Last Name>>:

We are sending this letter to you as part of our commitment to our customers' privacy. We take customer privacy very seriously, and it is important to us that you are aware of an incident we learned of on October 11, 2018, which may have compromised your sensitive personal information.

What happened?

On October 11, 2018, a document was discovered in a Medtronic facility that contained handwritten sensitive customer personal information about two customers. Upon learning of the incident, Medtronic took immediate action to identify the employee who had taken this information, ensure that access to Medtronic information was suspended, and began a thorough investigation. In the process, we determined that the employee improperly recorded sensitive customer personal information of at least two additional customers and as a result was terminated. Our investigation has revealed no evidence of broader theft of sensitive personal information and no evidence of any compromise of our systems. However, we are unable to confirm that the employee misappropriated information about only a few known customers. Out of an abundance of caution, and because of the sensitive nature of this information, we are notifying all customers whose sensitive personal or financial information might have been accessed by this employee.

What information was impacted?

The information accessed and taken may have included your name, address, phone number, email, date of birth, credit card number, CVC number, credit card expiration date, and social security number.

What are we doing to help?

We are alerting you and others who may have been impacted so that you can take steps to protect yourself. As a precaution, we are offering identity theft protection services through ID Experts® to provide you with MyIDCare™. MyIDCare services include: 24 months of triple bureau credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

Medtronic is not affiliated in any way with ID Experts; however, their services have come highly recommended. With this protection, ID Experts will help you resolve issues if your identity is compromised.

Instructions for enrolling in credit monitoring:

We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling (866) 680-8691 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 5 am - 5 pm Pacific Time. Please note the deadline to enroll is February 22, 2019.

Enclosed is an information sheet for you called "**Recommended Steps to Complete Enrollment with ID Experts**," which outlines additional steps you may wish to take in addition to enrolling with ID Experts. As mentioned in the information sheet, we recommend you regularly review your account statements, monitor your credit reports, and take other appropriate actions to protect against potential fraud or identity theft.

What are we doing?

Medtronic began an investigation immediately upon learning of this incident, including a forensic investigation of the employee's workspace, physical documents, computer and our systems. The employee's system access was immediately suspended when Medtronic learned of the incident on October 11, 2018, and employment has been terminated.

In addition to the steps described above, we have also contacted the Department of Health and Human Services, and the applicable state agencies regarding this incident. In addition, we are continuing our investigation, reviewing our policies and procedures, and implementing further training with our employees to avoid any future incidents. We have also contacted law enforcement and are cooperating with their investigation.

What can you do?

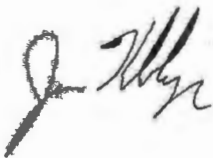
Monitor your accounts for any unusual activity. You may also wish to consider contacting the three credit reporting bureaus and requesting a fraud alert or a credit freeze be placed on your account. Contact information and a guide for how to make these requests appears on the following pages.

You are also entitled to a free credit report every year from each of these agencies. You can request the report at www.annualcreditreport.com.

We understand that this may cause concern and inconvenience you. We sincerely apologize and regret that this situation has occurred. Medtronic is committed to protecting your personal health information and we want to assure you that we are dedicated to ensuring that this does not happen again in the future.

Please do not hesitate to contact ID Experts with any questions about this incident, or for additional information on steps to take as a result of this incident, at (866) 680-8691.

Sincerely,



Jim Keblinger

VP Installed Base, Americas

Medtronic

Recommended Steps to help Protect your Information

- 1. Website and Enrollment.** Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at (866) 680-8691 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000

www.alerts.equifax.com

www.experian.com

www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

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 a 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. You can 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.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.