

March 28, 2018

RECEIVED

MAR 29 2018

BY OVERNIGHT MAIL

CONSUMER PROTECTION

NH Department of Justice
Gordon J. MacDonald, Attorney General
33 Capitol Street
Concord, NH 03301

Notice of Data Security Incident

Dear Attorney General MacDonald:

I am writing to notify you of a data security incident at Thermo Fisher Scientific involving the personal information of New Hampshire residents.

Thermo Fisher learned from federal law enforcement authorities that unauthorized third parties compromised a small percentage of the company's email accounts. They advised us that we were one of a large number of corporations that this group has targeted and that federal law enforcement authorities were actively investigating the group.

Upon learning of the incident, the company immediately began its own investigation with the assistance of outside experts and has been working closely with federal law enforcement authorities in connection with their ongoing criminal investigation.

Based on our investigation to date, we believe that unauthorized third parties obtained usernames and passwords for some of our company email accounts and then used those credentials to access the accounts and acquire emails sent to those accounts. Although the date when the compromise began has not been conclusively determined, our investigation confirms that emails received from on or about July 6, 2017 through October 13, 2017 were impacted. While other emails in the affected accounts also potentially were at risk, our investigation to date has not determined that any other emails actually were affected.

The company is notifying 34 New Hampshire residents of this incident. The residents include current employees who were the users of the compromised company email accounts and individuals whose name and social security number were determined to have been among the information contained in affected emails. Attached for your reference are representative samples of the notification letters we are sending to these individuals, which will be sent as expeditiously as possible via first-class mail beginning on March 30, 2018.

Thermo Fisher is offering all of these residents identity-protection services through Kroll at no charge to them for a period of one year.


Upon learning of the incident, Thermo Fisher promptly took steps to secure the affected accounts, including requiring the users of the affected email accounts to change their passwords. In addition, the company has enhanced its email security and expects to continue to make security enhancements to help prevent similar incidents from occurring in the future. We also worked closely with federal law enforcement authorities, who requested that we not make any notification of this incident until March 30, 2018 to avoid interference with

ThermoFisher
SCIENTIFIC

their criminal investigation. The company is now making this notification, pursuant to N.H. Rev. Stat. Ann. § 359-C:20.

If you have any questions, please contact me at 781-622-1053.

Sincerely,



Kathi L. Hartman
Vice President, Chief Counsel, Litigation

Encl.

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>:

I am writing to make you aware of a data security incident involving your Thermo Fisher Scientific email account. The company takes information security very seriously and, upon learning of this incident, took prompt steps to secure your account. Although the incident involved your company email account, I am notifying you in case you chose to use this account for communications that contained your sensitive personal information. This letter explains the incident, measures the company has taken, and some actions you can take in response.

What Happened

Thermo Fisher learned from federal law enforcement authorities that unauthorized third parties compromised a small percentage of the company's email accounts. They advised us that we were one of a large number of corporations that this group has targeted and that federal law enforcement authorities were actively investigating the group.

We believe that your account was among those compromised. Specifically, we believe that unauthorized third parties obtained your company email account username and password and then used those credentials to access your account and acquire certain emails.

What Information Was Involved

Based on our investigation to date, we believe that emails sent to your account during some portion of 2017 were obtained without authorization. Although the date when the compromise began has not been conclusively determined, our investigation confirms that emails received from on or about July 6, 2017 through October 13, 2017 were affected. While other emails in your account also potentially were at risk, our investigation to date has not determined that any other emails actually were affected.

In an abundance of caution, we are notifying you of this incident because, if you chose to use your company email account for personal communications that contained sensitive personal information, such as your social security, driver's license or passport numbers, that information may have been affected.

We have no indication that any emails obtained in this incident were actually viewed by any unauthorized third party or that any information from those emails has been misused.

What We Are Doing

Upon learning of the incident, Thermo Fisher immediately began its own investigation with the assistance of outside experts and has been working closely with federal law enforcement authorities in connection with their investigation. The company also promptly took steps to secure your account, including requiring you to change your password. In addition, the company has enhanced email security and expects to continue to make security enhancements to help prevent similar incidents from occurring in the future. Law enforcement authorities requested that we delay making any notification of this incident to avoid interference with their investigation. We are notifying you now, after coordinating with law enforcement, so that you can take the steps recommended below.

What You Can Do

The company encourages you to remain vigilant and take steps to protect against identity theft or fraud. While we already have required you to change your password for your Thermo Fisher Scientific email account, you also should change your passwords for any accounts for which you use or used the same or similar passwords as those that you have used for your Thermo Fisher Scientific account. When changing passwords, we recommend that you choose strong passwords that are complex and hard to guess, and that include both upper and lower case letters, numbers and symbols.

As an added precaution, we are offering you 12 months of identity monitoring services at no charge to you. The company has made arrangements with a third-party service provider, Kroll, to provide these services, which include triple bureau credit monitoring, access to a free current credit report, internet-based identity monitoring, \$1 million identity fraud loss reimbursement, fraud consultation, and identity theft restoration services.

To take advantage of these services, you will need to activate them online at my.idmonitoringservice.com.

Your Membership Number is <<Member ID>> and you must enroll by July 28, 2018 to activate these services. If you have any questions about the services or would like to receive your credit monitoring and credit report through the mail, please call Kroll at 1-833-219-9084 Monday–Friday from 9:00 a.m. to 6:00 p.m. ET. Please note that to activate these services, you will need to provide your personal information to Kroll. Additional information about the services available from Kroll is enclosed.

We recommend that you monitor your accounts and free credit reports for any signs of suspicious activity. Information about how to obtain a free credit report, security freezes, and other guidance is provided under “Additional Resources” in the enclosed document, which we encourage you to review.

As always, please be cautious of any unsolicited communications that ask you to provide your personal information electronically or over the telephone and avoid clicking on links or downloading attachments from suspicious emails.

If you have any questions or concerns and would like to speak with a company representative, please call 1-800-831-8099 Monday–Friday from 8:00 a.m. to 8:00 p.m. ET.

Sincerely,



Erik Winebrenner
Chief Information Security Officer

ADDITIONAL RESOURCES

Credit Reports, Fraud Alerts, and Security Freezes

You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You can request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies:

- **Experian**, www.experian.com, 1-888-397-3742, P.O. Box 9554, Allen, TX 75013
- **TransUnion**, www.transunion.com, 1-888-909-8872, P.O. Box 2000, Chester, PA 19016-2000
- **Equifax**, www.equifax.com, 1-800-685-1111, P.O. Box 105788, Atlanta, GA 30348

You can contact these credit bureaus to place a “fraud alert” on your credit file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. When one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please 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 must send a written request to each of the three major consumer reporting agencies listed above. You may need to pay a fee and will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five years, provide the addresses where you have lived over the prior five years
- Proof of current address such as a current utility bill or telephone bill
- A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.)
- 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.
- If you are not a victim of identity theft, include payment by check, money order or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

You can also receive information from the Federal Trade Commission (“FTC”) regarding fraud alerts, security freezes, your rights under the Fair Credit Reporting Act, and how to avoid and report identity theft: FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, consumer.ftc.gov, 1-877-438-4338.

Additional Information for Residents of Massachusetts

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. The credit reporting agencies have three (3) business days after receiving your 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 lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information for Residents of Iowa, Maryland, North Carolina, Oregon, and Rhode Island

You can contact the FTC, local law enforcement, or your state attorney general to report suspected identity theft or request information on how to prevent it.

- **Iowa:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, www.iowaattorneygeneral.gov, 1-888-777-4590
- **Maryland:** Office of the Attorney General of Maryland, 200 St. Paul Place Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023
- **North Carolina:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226
- **Oregon:** Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392
- **Rhode Island:** Office of the Attorney General of Rhode Island, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400. In Rhode Island, you may file or obtain a police report.
- Contact information for the other Attorneys General is available at www.naag.org/current-attorneys-general.php.

INFORMATION ABOUT KROLL SERVICES

The company is offering you the following services from Kroll at no charge to you. Please see the attached letter for directions on how to sign up for these services.

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you can call a Kroll fraud specialist.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your social security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

This feature reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You will have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues.

<<Date>> (Format: Month Day, Year)

<<MemberFirstName>> <<MemberLastName>> <<NameSuffix>>
<<Address1>>
<<Address2>>
<<City>>, <<State>> <<ZipCode>>

Notice of Data Security Incident

Dear <<MemberFirstName>> <<MemberLastName>>:

I am writing to make you aware of a data security incident at Thermo Fisher Scientific involving your personal information, as described below. This letter explains the incident, measures the company has taken and some actions you can take in response. Thermo Fisher takes information security very seriously and sincerely regrets that this incident occurred and any concern or inconvenience it may cause you.

What Happened

Thermo Fisher learned from federal law enforcement authorities that unauthorized third parties compromised a small percentage of the company's email accounts during some portion of 2017. They advised us that our company was one of a large number of corporations that this group has targeted and that federal law enforcement authorities were actively investigating the group. Although the date when the compromise began has not been conclusively determined, our investigation to date confirms that certain emails from on or about July 6, 2017 through October 13, 2017 were acquired by unauthorized third parties.

What Information Was Involved

Based on our investigation to date, we believe that your name and social security number were among the information contained in the affected emails.

We have no indication that any information obtained in this incident was actually viewed by any unauthorized third party or has been misused.

What We Are Doing

Upon learning of the incident, Thermo Fisher immediately began its own investigation with the assistance of outside experts and has been working closely with federal law enforcement authorities in connection with their investigation of this incident. The company also promptly took steps to secure the affected accounts, including requiring employees to change their passwords. In addition, Thermo Fisher has enhanced its email security and expects to continue to make security enhancements to help prevent similar incidents from occurring in the future. Law enforcement authorities requested that the company delay making any notification of this incident to avoid interference with their investigation. We are notifying you now, after coordinating with law enforcement, so that you can take the steps recommended below.

What You Can Do

The company encourages you to remain vigilant and take steps to protect against identity theft or fraud. We recommend that you monitor your accounts and free credit reports for any signs of suspicious activity. Information about how to obtain a free credit report, security freezes, and other guidance is provided under "Additional Resources" in the enclosed document, which we encourage you to review.

As an added precaution, we are offering you 12 months of identity monitoring services at no charge to you. The company has made arrangements with a third-party service provider, Kroll, to provide these services, which include triple bureau credit monitoring, access to a free current credit report, internet-based identity monitoring, \$1 million identity fraud loss reimbursement, fraud consultation, and identity theft restoration services.

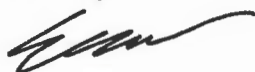
To take advantage of these services, you will need to activate them online at my.idmonitoringservice.com.

Your Membership Number is <<Member ID>> and you must enroll by July 28, 2018 to activate these services. If you have any questions about the services or would like to receive your credit monitoring and credit report through the mail, please call Kroll at 1-833-219-9084 Monday–Friday from 9:00 a.m. to 6:00 p.m. ET. Please note that to activate these services, you will need to provide your personal information to Kroll. Additional information about the services available from Kroll is enclosed.

As always, please be cautious of any unsolicited communications that ask you to provide your personal information electronically or over the telephone and avoid clicking on links or downloading attachments from suspicious emails.

If you have any questions or concerns, please call 1-833-219-9084 Monday–Friday from 9:00 a.m. to 6:00 p.m. ET.

Sincerely,



Erik Winebrenner
Chief Information Security Officer

ADDITIONAL RESOURCES

Credit Reports, Fraud Alerts, and Security Freezes

You may obtain a free copy of your credit report from each of the three credit reporting agencies by visiting www.annualcreditreport.com or by calling 1-877-322-8228. You can request information regarding fraud alerts, security freezes, and identity theft from the following credit reporting agencies:

- **Experian**, www.experian.com, 1-888-397-3742, P.O. Box 9554, Allen, TX 75013
- **TransUnion**, www.transunion.com, 1-888-909-8872, P.O. Box 2000, Chester, PA 19016-2000
- **Equifax**, www.equifax.com, 1-800-685-1111, P.O. Box 105788, Atlanta, GA 30348

You can contact these credit bureaus to place a “fraud alert” on your credit file that alerts creditors to take additional steps to verify your identity prior to granting credit in your name. When one credit bureau confirms your fraud alert, the others are notified to place fraud alerts on your file.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer’s credit report without written authorization. However, please 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 must send a written request to each of the three major consumer reporting agencies listed above. You may need to pay a fee and will need to provide the following information:

- Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
- Social Security number
- Date of birth
- If you have moved in the past five years, provide the addresses where you have lived over the prior five years
- Proof of current address such as a current utility bill or telephone bill
- A legible photocopy of a government-issued identification card (state driver’s license or ID card, military identification, etc.)
- 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.
- If you are not a victim of identity theft, include payment by check, money order or credit card (Visa, MasterCard, American Express or Discover only). Do not send cash through the mail.

You can also receive information from the Federal Trade Commission (“FTC”) regarding fraud alerts, security freezes, your rights under the Fair Credit Reporting Act, and how to avoid and report identity theft: FTC Identity Theft Clearinghouse, 600 Pennsylvania Avenue, NW, Washington, D.C. 20580, consumer.ftc.gov, 1-877-438-4338.

Additional Information for Residents of Massachusetts

Under Massachusetts law, you have the right to obtain any police report filed in regard to this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

Massachusetts law also allows consumers to place a security freeze on their credit reports. If you have been a victim of identity theft, and you provide the credit reporting agency with a valid police report, it cannot charge you to place, lift, or remove a security freeze. In all other cases, a credit reporting agency may charge you up to \$5.00 each to place, temporarily lift, or permanently remove a security freeze. The credit reporting agencies have three (3) business days after receiving your 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 lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze as well as the identities of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time. To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and social security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.

Additional Information for Residents of Iowa, Maryland, North Carolina, Oregon, and Rhode Island

You can contact the FTC, local law enforcement, or your state attorney general to report suspected identity theft or request information on how to prevent it.

- **Iowa:** Office of the Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319-0106, www.iowaattorneygeneral.gov, 1-888-777-4590
- **Maryland:** Office of the Attorney General of Maryland, 200 St. Paul Place Baltimore, MD 21202, www.marylandattorneygeneral.gov, 1-888-743-0023
- **North Carolina:** Office of the Attorney General of North Carolina, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.com, 1-877-566-7226
- **Oregon:** Oregon Department of Justice, 1162 Court St. NE, Salem, OR 97301-4096, www.doj.state.or.us, 1-877-877-9392
- **Rhode Island:** Office of the Attorney General of Rhode Island, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, (401) 274-4400. In Rhode Island, you may file or obtain a police report.
- Contact information for the other Attorneys General is available at www.naag.org/current-attorneys-general.php.

INFORMATION ABOUT KROLL SERVICES

The company is offering you the following services from Kroll at no charge to you. Please see the attached letter for directions on how to sign up for these services.

Triple Bureau Credit Monitoring and Single Bureau Credit Report

Your current credit report is available for you to review. You will also receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you can call a Kroll fraud specialist.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Public Persona

Public Persona monitors and notifies when names, aliases, and addresses become associated with your social security number. If information is found, you will receive an alert.

Quick Cash Scan

Quick Cash Scan monitors short-term and cash-advance loan sources. You will receive an alert when a loan is reported, and you can call a Kroll fraud specialist for more information.

\$1 Million Identity Fraud Loss Reimbursement

This feature reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You will have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues.