

2020 NOV 30 AM 10:20

BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Craig A. Hoffman
direct dial: 513.929.3491
cahoffman@bakerlaw.com

November 25, 2020

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, Canon U.S.A., Inc. and certain subsidiaries, predecessors, and affiliates (“Canon”), to notify your office of a security incident.¹ Canon’s headquarters are located at One Canon Park, Melville, New York 11747.

Canon identified a security incident involving ransomware on August 4, 2020. Canon immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. Canon also notified law enforcement and worked to support the investigation.

Canon determined that there was unauthorized activity on its network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on Canon’s file servers. Canon completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees from 2005 to 2020 and their beneficiaries and dependents. The information in the files included the individuals’ names and one or more of the following data elements: Social Security number, driver’s license

¹ This notice is being provided by or on behalf of Canon U.S.A., Inc. and the following subsidiaries, predecessors, and affiliates: Canon BioMedical, Inc., Canon Business Solutions-Central, Inc., Canon Business Solutions-Mountain West, Inc., Canon Business Solutions-NewCal, Inc., Canon Business Solutions-Tereck, Inc., Canon Business Solutions-West, Inc., Canon Development Americas, Inc., Canon Financial Services, Inc., Canon Information and Imaging Solutions, Inc., Canon Information Technology Systems, Inc., Canon Latin America, Inc., Canon Medical Components U.S.A., Inc., Canon Software America, Inc., Canon Solutions America, Inc., Canon Technology Solutions, Inc., Canon U.S. Life Sciences, Inc., NT-ware USA, Inc., Océ Imaging Supplies, Inc., Océ Imagistics Inc., Océ North America, Inc., Océ Reprographic Technologies Corporation, and Virtual Imaging, Inc.

Attorney General Gordon MacDonald
Office of the Attorney General
November 25, 2020
Page 2

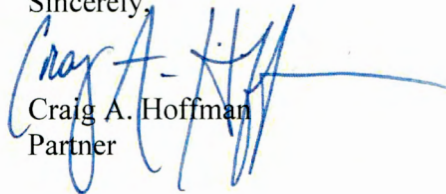
number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.

Beginning today, Canon is mailing notification letters via U.S. mail to 157 New Hampshire residents whose personal information may have been involved in the incident.² It is also issuing a press release and posting a statement on its website to provide notice of the incident. Copies of the notification letter, press release, and website statement are attached. Canon is offering a one-year membership in complimentary credit monitoring and identity protection services through Experian. Canon also has established a dedicated call center that individuals can call with questions about the incident or enrolling in credit monitoring.

To reduce the risk of a similar incident occurring in the future, Canon has already implemented additional security measures to further enhance the security of its network, including endpoint detection and response tools, 24/7/365 monitoring by a third-party security operations center, and additional hardening measures.

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

Sincerely,



Craig A. Hoffman
Partner

Enclosures

² This report does not waive Canon's objection that New Hampshire lacks personal jurisdiction over Canon regarding any claims related to this incident.



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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Canon understands the importance of protecting information.¹ We are writing to inform you of an incident that may have involved some of your information. This notice explains the incident, measures we have taken, and steps you can take in response.

We identified a security incident involving ransomware on August 4, 2020. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We notified law enforcement and worked to support the investigation. We also implemented additional security measures to further enhance the security of our network.

We determined that there was unauthorized activity on our network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on our file servers. We completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees and their beneficiaries and dependents. The information in the files may have included your name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.

We wanted to notify you of this incident and to assure you that we take it seriously. As a precaution, we have arranged for you to receive a complimentary one-year membership to Experian's® IdentityWorksSM credit monitoring service. This product helps detect possible misuse of your information and provides you with identity protection services. IdentityWorksSM is completely free to you, and enrolling in this program will not hurt your credit score. For more information on IdentityWorksSM, including instructions on how to activate your complimentary one-year membership, as well as some additional steps you can take in response, please see the additional information provided in this letter.

We regret that this occurred and apologize for any inconvenience. If you have additional questions, please call 1-833-960-3574, Monday through Friday, between 9:00 am and 6:30 pm, Eastern Time.

Sincerely,

N. Scott Millar
Senior Vice President & General Manager
Corporate Human Resources / Audit, Ethics & Business Consultation

¹ This notice is being provided by or on behalf of Canon U.S.A., Inc. and the following subsidiaries, predecessors, and affiliates: Canon BioMedical, Inc., Canon Business Solutions-Central, Inc., Canon Business Solutions-Mountain West, Inc., Canon Business Solutions-NewCal, Inc., Canon Business Solutions-Tereck, Inc., Canon Business Solutions-West, Inc., Canon Development Americas, Inc., Canon Financial Services, Inc., Canon Information and Imaging Solutions, Inc., Canon Information Technology Systems, Inc., Canon Latin America, Inc., Canon Medical Components U.S.A., Inc., Canon Software America, Inc., Canon Solutions America, Inc., Canon Technology Solutions, Inc., Canon U.S. Life Sciences, Inc., NT-ware USA, Inc., Océ Imaging Supplies, Inc., Océ Imagicistics Inc., Océ North America, Inc., Océ Reprographic Technologies Corporation, and Virtual Imaging, Inc.

Activate IdentityWorks Credit 3B Now in Three Easy Steps

To help protect your identity, we are offering a **complimentary** one-year membership of Experian IdentityWorksSM 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.

1. ENROLL by: <<b2b_text_1 (Date)>> (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: <<Member ID>>**

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 1-877-288-8057. Be prepared to provide engagement number <<b2b_text_2 (Engagement #)>> 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 1-877-288-8057 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 1-877-288-8057.

* 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.

Additional Information for Residents of the Following States:

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

West Virginia: 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, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.



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

To the Estate of

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country >

Dear Estate of <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Canon understands the importance of protecting information.¹ We are writing to inform you of an incident that may have involved some of your loved one's information. This notice explains the incident, measures we have taken, and steps you can take in response.

We identified a security incident involving ransomware on August 4, 2020. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We notified law enforcement and worked to support the investigation. We also implemented additional security measures to further enhance the security of our network.

We determined that there was unauthorized activity on our network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on our file servers. We completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees and their beneficiaries and dependents. The information in the files may have included your loved one's name and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.

We wanted to notify you of this incident and to assure you that we take it seriously. We encourage you to remain vigilant by reviewing your loved one's account statements for any unauthorized activity. Please also review the additional information on the following pages on ways to protect deceased individuals' personal information and credit records.

We regret that this occurred and apologize for any inconvenience. If you have additional questions, please call 1-833-960-3574, Monday through Friday, between 9:00 am and 6:30 pm, Eastern Time.

Sincerely,

N. Scott Millar
Senior Vice President & General Manager
Corporate Human Resources / Audit, Ethics & Business Consultation

¹ This notice is being provided by or on behalf of Canon U.S.A., Inc. and the following subsidiaries, predecessors, and affiliates: Canon BioMedical, Inc., Canon Business Solutions-Central, Inc., Canon Business Solutions-Mountain West, Inc., Canon Business Solutions-NewCal, Inc., Canon Business Solutions-Tereck, Inc., Canon Business Solutions-West, Inc., Canon Development Americas, Inc., Canon Financial Services, Inc., Canon Information and Imaging Solutions, Inc., Canon Information Technology Systems, Inc., Canon Latin America, Inc., Canon Medical Components U.S.A., Inc., Canon Software America, Inc., Canon Solutions America, Inc., Canon Technology Solutions, Inc., Canon U.S. Life Sciences, Inc., NT-ware USA, Inc., Océ Imaging Supplies, Inc., Océ Imagicistics Inc., Océ North America, Inc., Océ Reprographic Technologies Corporation, and Virtual Imaging, Inc.

Protecting Deceased Individuals

The following steps are recommended to help protect the personal information of deceased individuals. Typically, the Social Security Administration will notify the credit reporting agencies (CRAs) of a death when they update their files. It is advisable to contact the CRAs in writing to notify them of the death, request that a “deceased” alert be placed on the individual’s credit report, and obtain a copy of the credit report for your records. A review of each report will provide information regarding active credit accounts that need to be closed, or any pending collection notices. The addresses for reporting this information to the three major CRAs are:

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

Contact all credit issuers, collection agencies, and other financial institutions where the deceased individual had accounts to inform them of the death. Each entity may have its own required notification procedures, but the following general information can serve as a guide:

- Obtain at least 12 copies of the official death certificate when it becomes available. In some cases, you may be able to use a photocopy, but certain entities will request an original. In some cases, a business may require additional information as proof of death.
- Include the following information in your correspondence:
 - Name and SSN of deceased
 - Last known address of the deceased, and previous addresses for the past 5 years
 - Date of birth and date of death
- To speed up processing, include all of the documentation required by that specific agency or organization in your first letter.
- Send important correspondence by certified mail with return receipt requested.
- Keep copies of all correspondence, noting date sent and any response(s) you receive.

Please note that the CRAs may require a court order or other paperwork to prove that you are the executor of an estate. Friends, neighbors, relatives and others do not have the same rights as the executor or a deceased individual’s spouse. In most cases these other individuals are considered third parties, and a CRA may not disclose credit reports or update a consumer file without authorization from the spouse or executor. CRAs may make exceptions for unique situations, which they handle on a case-by-case basis. You may write to the CRA to explain your situation and request assistance.

If you have reason to believe your family member’s personal information has been misused, you should contact the Federal Trade Commission. 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

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.

Additional Information for Residents of the Following States:

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

West Virginia: 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, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit “prescreened” offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.

FOR IMMEDIATE RELEASE

Canon Identifies and Addresses Data Security Incident

MELVILLE, NEW YORK, November 25, 2020 – Today, Canon, a leading provider of consumer, business-to-business, and industrial digital imaging solutions, announced that it identified and addressed a data security incident.¹

Canon identified a security incident involving ransomware on August 4, 2020. Canon immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. Canon notified law enforcement and worked to support the investigation. Canon also implemented additional security measures to further enhance the security of its network.

Canon determined that there was unauthorized activity on its network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on Canon's file servers. Canon completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees from 2005 to 2020 and their beneficiaries and dependents. The information in the files included the individuals' names and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.

Canon advises its current and former employees from 2005 to 2020 and their beneficiaries and dependents to remain vigilant for signs of unauthorized activity by reviewing their financial account statements. If they see charges or activity they did not authorize, Canon suggests they contact their financial institution immediately. Canon is in the process of providing notice of this incident to current and former employees from 2005 to 2020 and their beneficiaries and dependents and is offering them a complimentary membership to Experian's® IdentityWorksSM credit monitoring service. Unfortunately, Canon does not have current addresses for all such individuals. Canon encourages its current and former employees from 2005 to 2020 and their beneficiaries and dependents to visit the website or call the telephone number below for additional information.

Canon regrets that this occurred and apologizes for any inconvenience. Additional information is available at the following websites:

- <https://usa.canon.com/internet/portal/us/home/explore/securityincident>,
- <https://csa.canon.com/internet/portal/us/csa/securityincident>,
- <https://cits.canon.com/securityincident>,
- <https://ciis.canon.com/internet/portal/ciis/home/securityincident>, and
- <https://cfs.canon.com/securityincident.html>

or by calling 1-833-960-3574, Monday through Friday, between 9:00 a.m. and 6:30 p.m., Eastern Time.

¹ This press release is being provided by or on behalf of Canon U.S.A., Inc. and the following subsidiaries, predecessors, and affiliates: Canon BioMedical, Inc., Canon Business Solutions-Central, Inc., Canon Business Solutions-Mountain West, Inc., Canon Business Solutions-NewCal, Inc., Canon Business Solutions-Tereck, Inc., Canon Business Solutions-West, Inc., Canon Development Americas, Inc., Canon Financial Services, Inc., Canon Information and Imaging Solutions, Inc., Canon Information Technology Systems, Inc., Canon Latin America, Inc., Canon Medical Components U.S.A., Inc., Canon Software America, Inc., Canon Solutions America, Inc., Canon Technology Solutions, Inc., Canon U.S. Life Sciences, Inc., NT-ware USA, Inc., Océ Imaging Supplies, Inc., Océ Imagistics Inc., Océ North America, Inc., Océ Reprographic Technologies Corporation, and Virtual Imaging, Inc.

About Canon U.S.A., Inc.

Canon U.S.A., Inc., is a leading provider of consumer, business-to-business, and industrial digital imaging solutions to the United States and to Latin America and the Caribbean markets. With approximately \$33 billion in global revenue, its parent company, Canon Inc. (NYSE:CAJ), ranks third overall in U.S. patents granted in 2019[†] and was named one of Fortune Magazine's World's Most Admired Companies in 2020. Canon U.S.A. is dedicated to its Kyosei philosophy of social and environmental responsibility. To keep apprised of the latest news from Canon U.S.A., sign up for the Company's RSS news feed by visiting www.usa.canon.com/rss and follow us on Twitter @CanonUSA.

[†] Based on weekly patent counts issued by United States Patent and Trademark Office.

#

Editorial Contact:

Chris Sedlacek

Canon U.S.A., Inc.

631.330.5642

csedlacek@cusa.canon.com

November 25, 2020

Notice of Data Security Incident

California Residents Please Click Here

Canon understands the importance of protecting information. We are informing current and former employees who were employed by Canon U.S.A., Inc. and certain subsidiaries, predecessors, and affiliates¹ from 2005 to 2020 and those employees' beneficiaries and dependents of an incident that involved some of their information. This notice explains the incident, measures we have taken, and steps you can take in response.

We identified a security incident involving ransomware on August 4, 2020. We immediately began to investigate, a cybersecurity firm was engaged, and measures were taken to address the incident and restore operations. We notified law enforcement and worked to support the investigation. We also implemented additional security measures to further enhance the security of our network.

We determined that there was unauthorized activity on our network between July 20, 2020 and August 6, 2020. During that time, there was unauthorized access to files on our file servers. We completed a careful review of the file servers on November 2, 2020 and determined that there were files that contained information about current and former employees from 2005 to 2020 and their beneficiaries and dependents. The information in the files included the individuals' names and one or more of the following data elements: Social Security number, driver's license number or government-issued identification number, financial account number provided to Canon for direct deposit, electronic signature, and date of birth.

We wanted to notify our current and former employees and their beneficiaries and dependents of this incident and to assure them that we take it seriously. As a precaution, we have arranged for them to receive a complimentary membership to Experian's® IdentityWorksSM credit monitoring service. This product helps detect possible misuse of an individual's information and provides the individual with identity protection services. IdentityWorksSM is completely free to the individual, and enrolling in this program will not hurt the individual's credit score. If you are a current or former employee, or the beneficiary or dependent of a current or former employee, and would like more information on IdentityWorksSM, including instructions on how to activate your complimentary membership, please call our dedicated call center for this incident at 1-833-960-3574. For information on additional steps you can take in response, please see the additional information provided below.

We regret that this occurred and apologize for any inconvenience. If you have additional questions, please call 1-833-960-3574, Monday through Friday, between 9:00 a.m. and 6:30 p.m., Eastern Time.

¹ This notice is being provided by or on behalf of Canon U.S.A., Inc. and the following subsidiaries, predecessors, and affiliates: Canon BioMedical, Inc., Canon Business Solutions-Central, Inc., Canon Business Solutions-Mountain West, Inc., Canon Business Solutions-NewCal, Inc., Canon Business Solutions-Tereck, Inc., Canon Business Solutions-West, Inc., Canon Development Americas, Inc., Canon Financial Services, Inc., Canon Information and Imaging Solutions, Inc., Canon Information Technology Systems, Inc., Canon Latin America, Inc., Canon Medical Components U.S.A., Inc., Canon Software America, Inc., Canon Solutions America, Inc., Canon Technology Solutions, Inc., Canon U.S. Life Sciences, Inc., NT-ware USA, Inc., Océ Imaging Supplies, Inc., Océ Imagistics Inc., Océ North America, Inc., Océ Reprographic Technologies Corporation, and Virtual Imaging, Inc.

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.

Additional Information for Residents of the Following States:

Connecticut: You may contact and obtain information from your state attorney general at: *Connecticut Attorney General's Office*, 165 Capitol Ave, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

District of Columbia: You may contact and obtain information from your attorney general at: Office of the Attorney General for the District of Columbia, 441 4th Street NW, Washington, DC 20001, 1-202-727-3400, www.oag.dc.gov

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

Massachusetts: Under Massachusetts 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: *Office of the Massachusetts Attorney General*, One Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

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 309 individuals in Rhode Island. 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

West Virginia: 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, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street NW, Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- 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 reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a 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.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.