



Todd Rowe, Partner
20 North Wacker
Suite 4120
Chicago, IL 60606
Tel.: 773.558.2363
trowe@constangy.com

August 7, 2024

VIA EMAIL

Attorney General Anthony G. Brown
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith and Prophete LLP (“Constangy”) represents Noritsu America Corporation (“Noritsu”) in connection with an incident described in greater detail below. The purpose of this letter is to notify you, in accordance with Maryland data breach notification statute, that this incident may have affected the personal information of 7 Maryland residents. Noritsu hereby reserves all rights and defenses in connection herewith.

1. Nature of Incident

On April 29, 2024, Noritsu identified unusual activity in its network environment. As soon as Noritsu discovered this, it immediately took steps to contain the activity and engaged a cybersecurity firm to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. Noritsu’s investigation revealed that certain Noritsu data may have been accessed or acquired without authorization in connection with the incident on or about April 29, 2024. Noritsu thereafter undertook a review of the potentially affected data, which revealed that certain information for Noritsu employees may have been involved in this incident. Noritsu then worked to verify the affected information and mailing addresses for impacted individuals to ensure Noritsu had the most up to date contact information. This process was completed on July 31, 2024.

The potentially impacted information included individuals’ names and Social Security numbers.

2. Number of Maryland residents affected

Noritsu notified 7 Maryland residents of the incident via first class U.S. mail on August 7, 2024. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the incident

In response to the incident, Noritsu retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. Noritsu implemented additional security measures to further harden its environment in an effort to prevent a similar event from occurring in the future. Noritsu also reported this incident to federal law enforcement and is cooperating with the investigation.

Noritsu is notifying the affected individuals and providing resources and steps individuals can take to help protect their information. In addition, Noritsu is offering affected individuals complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: 12 months of credit monitoring, CyberScan dark web monitoring, fully managed identity recovery services, and \$1 million in identity theft insurance coverage. IDX will also support a call center for at least 90 days to answer incident related questions.

4. Contact information

If you have any questions or need additional information, please do not hesitate to contact me at 773.558.2363 or trowe@constangy.com.

Very truly yours,

A handwritten signature in black ink that reads "Todd N. Rowe". The signature is written in a cursive, slightly slanted style.

Todd Rowe of
Constangy, Brooks, Smith & Prophete, LLP

Encl.: Sample Consumer Notification Letter

Noritsu America Corporation
P.O. Box 989728
West Sacramento, CA 95798-9728

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

Enrollment Code: <<XXXXXXXX>>

To Enroll, Scan the QR Code Below:



Or Visit:

<https://app.idx.us/account-creation/protect>

August 7, 2024

Subject: Notice of Data <<Variable Data 1: Security Incident / Breach>>

Dear <<First Name>> <<Last Name>>,

Noritsu America Corporation (“Noritsu”) is writing to inform you of a data security incident that may have involved your personal information. Noritsu is committed to maintaining the trust of our employees, and the privacy and security of all information in our possession is a top priority. That is why we are notifying you of the event and providing you with resources to help protect your information. Please read this letter carefully as it contains important details about the incident and resources you may utilize to help protect your information.

What Happened? On April 29, 2024, we identified unusual activity in our network environment. As soon as we discovered this, we immediately took steps to contain the activity and engaged a cybersecurity firm to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. Our investigation revealed that certain Noritsu data may have been accessed or acquired without authorization in connection with the incident on or about April 29, 2024. Noritsu thereafter undertook a review of the potentially affected data, which revealed that certain information for Noritsu employees may have been involved in this incident. On July 31, 2024, Noritsu learned that your personal information may have been impacted in connection with the incident which is the reason for this notification.

What Information Was Involved? The potentially affected information may have included your name along with your social security number.

What We Are Doing? As soon as we discovered this incident, we took the steps referenced above. We also implemented additional security features to reduce the risk of a similar incident occurring in the future. We notified the Federal Bureau of Investigation and will cooperate with any resulting investigation.

Additionally, although we have no evidence that your information has or will be misused as a result of this incident, Noritsu is also offering you the opportunity to enroll in complimentary credit monitoring and identity theft protection services through IDX, A Zero Fox Company. IDX identity protection services include: <<Membership Offering Length 12/24>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. To enroll scan the QR image, go to <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter or call 1-800-939-4170. The deadline to enroll in these services is November 7, 2024.

Noritsu America Corporation
6900 Noritsu Ave.
Buena Park, CA 90620-1372

What You Can Do. We encourage you to enroll in the complimentary identity protection services we are offering. With this protection, IDX can help you resolve issues if your identity is compromised. Please also review the guidance at the end of this letter which includes additional resources you may utilize to help protect your information.

For More Information. IDX Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 6:00 a.m. to 6:00 p.m. Pacific Time, Monday through Friday, excluding holidays. Please call the help line at 1-800-939-4170 and supply the specialist with your unique code listed above.

Protecting your information is important to us. Please know that we take this incident very seriously, and we deeply regret any worry or inconvenience this may cause you.

Sincerely,

Noritsu America Corporation
6900 Noritsu Ave.
Buena Park, CA 90620-1372

STEPS YOU CAN TAKE TO PROTECT YOUR PERSONAL INFORMATION

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Copy of Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <http://www.annualcreditreport.com/>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <http://www.annualcreditreport.com>.

Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you including your full name, Social Security number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Internal Revenue Service Identity Protection PIN (IP PIN): You may also obtain an Identity Protection PIN (IP PIN) from the Internal Revenue Service, a six-digit number that prevents someone else from filing a tax return using your Social Security number or Individual Taxpayer Identification Number. The IP PIN is known only to you and the IRS, and helps the IRS verify your identity when you file your electronic or paper tax return. Even though you may not have a filing requirement, an IP PIN still protects your account. If you do not already have an IP PIN, you may get an IP PIN as a proactive step to protect yourself from tax-related identity theft either online, by paper application or in-person. Information about the IP PIN program can be found here: <https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin>.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
<https://www.marylandattorneygeneral.gov/>
1-888-743-0023

New York Attorney General

Bureau of Internet and Technology
Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA, and your rights pursuant to the FCRA, please visit https://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.