

420 Main St Suite 1100, Buffalo, New York 14202
75 S. Clinton Ave., 510 Clinton Square, Suite 555, Rochester, New York 14604
3 Columbus Circle, #1500, New York, New York 10019
600 Broadway, Suite 700, San Diego, California 92101
2 Bala Plaza, Suite 300, #704, Bala Cynwyd, Pennsylvania 19004



716.898.2102
octillolaw.com
info@octillolaw.com

March 24, 2023

VIA Email

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

Attorney General Brown:

On behalf of Rohde & Schwarz USA, Inc. ("RSA") and pursuant to the Personal Information Protection Act ("PIPA"), Md. Code Ann. Comm. Law 14-3504, this letter provides notice of a recent data security incident.

Description of the Incident

On March 8, 2023, three (3) anonymous emails were sent from the email account RSASalaries@proton.me which is an account with the company Proton Mail. Proton Mail is an encrypted email platform that has features that can be used to conceal the identity of the account holder.

The following provides a summary of the emails:

1. One (1) anonymous email was sent to one (1) former RSA employee at that former employee's personal email address and contained the personal information of sixty-one (61) RSA employees, specifically:
 - a. first and last names,
 - b. dates of birth,
 - c. RSA email addresses, and
 - d. self-reported Covid-19 vaccination status from a September 2021 RSA employee inquiry.

The former employee that received the anonymous email immediately and voluntarily told RSA that they received the anonymous email.

2. Two (2) identical anonymous emails were sent to one (1) current RSA employee at a personal email address and one (1) attorney for RSA at their firm's email address. These emails contained an excel spreadsheet attachment with the names and compensation information for 629 RSA employees for fiscal year 2021-2022, including base salary and any commissions earned. The individuals that received these emails immediately and voluntarily told RSA that they received the anonymous emails.
3. One (1) anonymous email was sent to a group of thirty-two (32) current and former RSA employees at their RSA email addresses and contained the information of those same thirty-two (32) employees, including their names, dates of birth, and nationality.

Of the three (3) anonymous emails, only the first anonymous email contained any "Personal Information" as that term is defined by PIPA (specifically, "Health Information").

Number of Individuals Residing in Maryland

Again, only the first anonymous email included the Personal Information of any Maryland residents as that term is defined by PIPA. That email included the information of fourteen (14) individuals who are or are believed to be Maryland residents.

Steps RSA has Taken

RSA is committed to protecting the security of its employees' information. RSA continues to investigate and implement appropriate measures to further improve the security of its systems and information.

RSA has engaged data security professionals to aid in its investigation and response and is working closely with law enforcement to identify the individual behind the anonymous emails and prevent any further incidents.

Based on the information that is currently available, RSA believes that a former RSA employee sent these anonymous emails. That employee's employment with RSA was terminated in September 2022. RSA believes that this former employee unlawfully obtained the information in the anonymous emails while still employed with RSA (i.e., prior to September 2022). RSA currently does not believe, nor does RSA have any evidence to suggest that the March 8, 2023 emails result from any new unauthorized access to RSA information, whether by this former employee or any other person.

Individual Notice

Out of an abundance of caution, RSA is notifying the individuals identified in the first and third anonymous emails via letters sent by mail and email. Attached for your convenience are copies of the template notification letters that RSA will send to the affected Maryland residents.



Office of the Attorney General

March 24, 2022

Page 3

Please feel free to contact me with any questions at (716) 898-2102 or bmyers@octillolaw.com.

OCTILLO

A handwritten signature in blue ink, appearing to read "B. H. Myers", with a long horizontal flourish extending to the right.

Brian H. Myers, Esq.

Encl.





March 24, 2023

Via U.S. Mail and email

[NAME]

[ADDRESS]

Dear [First Name] [Last Name],

Rohde & Schwarz USA, Inc. ("RSA") is writing to advise you that RSA recently became aware of anonymous emails that involved your personal information ("Personal Information"). This letter provides you with information about these anonymous emails, our investigation, and although we are not aware of any misuse of your Personal Information, steps you can take to protect your Personal Information.

What Happened?

On March 8, 2023, three (3) anonymous emails were sent from the email account RSASalaries@proton.me which is an account with the company Proton Mail. Proton Mail is an encrypted email platform that has features that can be used to conceal the identity of the account holder.

The following provides a summary of the three (3) March 8, 2023 emails. However, only the first two (2) emails included your Personal Information. We are providing a summary of all three (3) just to provide you with additional context:

1. One (1) anonymous email was sent to one (1) former RSA employee at that former employee's personal email address and contained the personal information of sixty-one (61) RSA employees, including your own Personal Information. Specifically, this email included: your first and last name, your date of birth, your RSA email address, and your self-reported Covid-19 vaccination status from a September 2021 RSA employee inquiry. That former employee immediately and voluntarily told RSA that they received the anonymous email.
2. Two (2) identical anonymous emails were sent to one (1) current RSA employee at a personal email address and one (1) attorney for RSA at their firm's email address. These emails contained an excel spreadsheet attachment with the names and compensation information for 629 RSA employees for fiscal year 2021-2022, including your own Personal Information. Specifically, this email included: your name and compensation information. The individuals that received these emails immediately and voluntarily told RSA that they received the anonymous emails.
3. Finally, an anonymous email was sent to a group of thirty-two (32) current and former RSA employees at their RSA email addresses and contained the personal information of those same thirty-two (32) employees, including their names, dates of birth, and nationality. Again, this email did **not** include your Personal Information in any way, and we are describing it just to provide you with additional context.

RSA did not authorize anyone to send these anonymous emails.

Other than the emails themselves, we do not have any evidence at this time that your Personal Information has been misused in any fashion; nevertheless, we are providing this notice.

What Information Was Involved?

As noted above, only the first two (2) anonymous emails included any of your Personal Information. The first anonymous email included the following Personal Information: your first and last name, your date of birth, your RSA email address, and your Covid-19 vaccination status that you self-reported to RSA in or around September 2021 in connection with an employee inquiry.

The second anonymous email included your first and last name and compensation information for fiscal year 2021-2022, including your base salary and any commissions earned that year.

Again, the third anonymous email did not include your Personal Information in any way.

Notably, the anonymous emails involved here did not include any government-issued identification numbers such as your social security number or a driver's license number, and the anonymous emails did not include any bank account information or debit or credit card information.

What We Are Doing.

RSA is committed to protecting your information. We continue to investigate and implement appropriate measures to further improve the security of our systems and information. We have engaged leading data security professionals to aid in our investigation and response and we are working closely with law enforcement to identify the individual behind the anonymous emails and prevent any further incidents.

Based on the information that is currently available, we believe that a former RSA employee sent these anonymous emails. That employee's employment with RSA was terminated in September 2022. We believe that this former employee unlawfully obtained the information in the anonymous emails while still employed with RSA (i.e., prior to September 2022). We currently do not believe, nor do we have any evidence to suggest that the March 8, 2023 emails result from any new unauthorized access to RSA information, whether by this former employee or any other person.

What You Can Do.

It is always recommended that you regularly monitor free credit reports and review account statements, and that you report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Personal Information.

For More Information.

If you have any questions, or if you have any information that could support our investigation, please contact [REDACTED].

Sincerely,

A handwritten signature in blue ink that reads "Frank Dunn". The signature is fluid and cursive, with a long horizontal stroke at the end.

President and CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, <https://www.alabamaag.gov/generalcontact>, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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

For Minnesota Residents: You may contact the Office of the Minnesota Attorney General, 445 Minnesota St Ste 1400, Saint Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.



March 24, 2023

Via US Mail and email

[Name]

[Address]

Dear [First Name] [Last Name],

Rohde & Schwarz USA, Inc. ("RSA") is writing to advise you that RSA recently became aware of anonymous emails that involved your personal information ("Personal Information"). This letter provides you with information about these anonymous emails, our investigation, and although we are not aware of any misuse of your Personal Information, steps you can take to protect your Personal Information.

What Happened?

On March 8, 2023, three (3) anonymous emails were sent from the email account RSASalaries@proton.me which is an account with the company Proton Mail. Proton Mail is an encrypted email platform that has features that can be used to conceal the identity of the account holder.

The following provides a summary of the three (3) March 8, 2023 emails. However, only the first two (2) emails included your Personal Information. We are providing a summary of all three (3) just to provide you with additional context:

1. An anonymous email was sent to a group of thirty-two (32) current and former RSA employees at their RSA email addresses – including yourself – and contained the personal information of those same thirty-two (32) employees, including your own Personal Information. Specifically, the email included: your name, date of birth, nationality, RSA email address, RSA unique ID number, RSA personnel number, and years of service with RSA.
2. Two (2) identical anonymous emails were sent to one (1) current RSA employee at a personal email address and one (1) attorney for RSA at their firm's email address. These emails contained an excel spreadsheet attachment with the names and compensation information for 629 RSA employees for fiscal year 2021-2022, including your own Personal Information. Specifically, this email included: your name and compensation information. The individuals that received these emails immediately and voluntarily told RSA that they received the anonymous emails.
3. Finally, an anonymous email was sent to one (1) former RSA employee at that former employee's personal email address and contained the personal information of sixty-one (61) RSA employees, including their first and last names, dates of birth, RSA email addresses and self-reported Covid-19 vaccination status from a September 2021 RSA employee inquiry. That former employee immediately and voluntarily told RSA that they received the anonymous email. Again, this email did **not** include your Personal Information in any way, and we are describing it just to provide you with additional context.

RSA did not authorize anyone to send these anonymous emails.

Other than the March 8, 2023 emails themselves, we do not have any evidence at this time that your Personal Information has been misused in any fashion; nevertheless, we are providing this notice.

What Information Was Involved?

As noted above, only the first two (2) anonymous emails included any of your Personal Information. The first anonymous email included the following Personal Information: your first and last name, your date of birth, your nationality, your RSA email address, your RSA unique ID number, your RSA personnel number, and your years of service with RSA.

The second anonymous email included your first and last name and compensation information for fiscal year 2021-2022, including your base salary and any commissions earned that year.

Again, the third anonymous email did not include your Personal Information in any way.

Notably, the anonymous emails involved here did not include any government-issued identification numbers such as your social security number or a driver's license number, and the anonymous emails did not include any bank account information or debit or credit card information.

What We Are Doing.

RSA is committed to protecting your information. We continue to investigate and implement appropriate measures to further improve the security of our systems and information. We have engaged leading data security professionals to aid in our investigation and response and we are working closely with law enforcement to identify the individual behind the anonymous emails and prevent any further incidents.

Based on the information that is currently available, we believe that a former RSA employee most likely sent these anonymous emails. That employee's employment with RSA was terminated in September 2022. We believe that this former employee unlawfully obtained the information in the anonymous emails while still employed with RSA (i.e., prior to September 2022). We currently do not believe, nor do we have any evidence to suggest that the March 8, 2023 emails result from any new unauthorized access to RSA information, whether by this former employee or any other person.

What You Can Do.

It is always recommended that you regularly monitor free credit reports and review account statements, and that you report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Personal Information.

For More Information.

If you have any questions, or if you have any information that could support our investigation, please contact [REDACTED]

Sincerely,

A handwritten signature in blue ink that reads "Frank Dunn". The signature is written in a cursive style with a long horizontal flourish at the end.

President and CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, <https://www.alabamaag.gov/generalcontact>, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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

For Minnesota Residents: You may contact the Office of the Minnesota Attorney General, 445 Minnesota St Ste 1400, Saint Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.



March 24, 2023

Via US Mail and email

[Name]

[Address Line 1]

[Address Line 2]

[City], [State] [Zip]

[email]

Dear [First Name] [Last Name],

Rohde & Schwarz USA, Inc. ("RSA") is writing to advise you that RSA recently became aware of anonymous emails that involved your personal information ("Personal Information"). This letter provides you with information about these anonymous emails, our investigation, and although we are not aware of any misuse of your Personal Information, steps you can take to protect your Personal Information.

What Happened?

On March 8, 2023, three (3) anonymous emails were sent from the email account RSASalaries@proton.me which is an account with the company Proton Mail. Proton Mail is an encrypted email platform that has features that can be used to conceal the identity of the account holder.

The following provides a summary of the three (3) March 8, 2023 emails. However, only the first email included your Personal Information. We are providing a summary of all three (3) just to provide you with additional context:

1. An anonymous email was sent to a group of thirty-two (32) current and former RSA employees at their RSA email addresses – including yourself – and contained the personal information of those same thirty-two (32) employees, including your own Personal Information. Specifically, the email included: your name, date of birth, nationality, RSA email address, RSA unique ID number, RSA personnel number, and years of service with RSA.
2. Two (2) identical anonymous emails were sent to one (1) current RSA employee at a personal email address and one (1) attorney for RSA at their firm's email address. These emails contained an excel spreadsheet attachment with the names and compensation information for 629 RSA employees for fiscal year 2021-2022, including their base salary and any commissions earned. The individuals that received these emails immediately and voluntarily told RSA that they received the anonymous emails. Again, this email did **not** include your Personal Information in any way, and we are describing it just to provide you with additional context.
3. Finally, an anonymous email was sent to one (1) former RSA employee at that former employee's personal email address and contained the personal information of sixty-one (61) RSA employees, including their first and last names, dates of birth, RSA email addresses and self-reported Covid-19 vaccination status from a September 2021 RSA employee inquiry. That

former employee immediately and voluntarily told RSA that they received the anonymous email. Again, this email did **not** include your Personal Information in any way, and we are describing it just to provide you with additional context.

RSA did not authorize anyone to send these anonymous emails.

Other than the March 8, 2023 emails themselves, we do not have any evidence at this time that your Personal Information has been misused in any fashion; nevertheless, we are providing this notice.

What Information Was Involved?

As noted above, only the first anonymous email included any of your Personal Information. The first anonymous email included the following Personal Information: your first and last name, your date of birth, your nationality, your RSA email address, your RSA unique ID number, your RSA personnel number, and your years of service with RSA.

Again, the second and third anonymous emails did not include your Personal Information in any way.

Notably, the anonymous emails involved here did not include any government-issued identification numbers such as your social security number or a driver's license number, and the anonymous emails did not include any bank account information or debit or credit card information.

What We Are Doing.

RSA is committed to protecting your information. We continue to investigate and implement appropriate measures to further improve the security of our systems and information. We have engaged leading data security professionals to aid in our investigation and response and we are working closely with law enforcement to identify the individual behind the anonymous emails and prevent any further incidents.

Based on the information that is currently available, we believe that a former RSA employee most likely sent these anonymous emails. That employee's employment with RSA was terminated in September 2022. We believe that this former employee unlawfully obtained the information in the anonymous emails while still employed with RSA (i.e., prior to September 2022). We currently do not believe, nor do we have any evidence to suggest that the March 8, 2023 emails result from any new unauthorized access to RSA information, whether by this former employee or any other person.

What You Can Do.

It is always recommended that you regularly monitor free credit reports and review account statements, and that you report any suspicious activity to financial institutions. Please also review the "Additional Resources" section included with this letter, which outlines other resources you can utilize to protect your Personal Information.

For More Information.

If you have any questions, or if you have any information that could support our investigation, please contact [REDACTED]

Sincerely,

A handwritten signature in blue ink that reads "Frank Dunn". The signature is written in a cursive style with a long horizontal flourish at the end.

President and CEO

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19022, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant for incidents of fraud and identity theft by reviewing account statements and monitoring your credit report for 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 agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Fraud Alert. You may place a fraud alert in your file by calling one of the three nationwide credit reporting agencies above. 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.

Security Freeze. You have the ability to place a security freeze on your credit report.

A security freeze is intended to prevent credit, loans, and services from being approved in your name without your consent. To place a security freeze on your credit report, you may be able to use an online process, an automated telephone line, or a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past five years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. 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 home state. You may also contact these agencies for information on how to prevent or avoid identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Alabama Residents: You may contact the Attorney General's Office for the State of Alabama, Consumer Protection Division, 501 Washington Avenue, Montgomery, AL 36104, <https://www.alabamaag.gov/generalcontact>, 1-800-392-5658.

For District of Columbia Residents: You may contact the District of Columbia Office of the Attorney General, 400 6th Street NW, Washington, D.C. 20001, consumer.protection@dc.gov, (202) 442-9828.

For Illinois Residents: You may contact the Illinois Office of the Attorney General, 100 West Randolph Street, Chicago, IL 60601, https://illinoisattorneygeneral.gov/about/email_ag.jsp, 1-800-964-3013.

For Iowa Residents: You may contact the Iowa Office of the Attorney General, 1305 E. Walnut Street, Des Moines IA 50319, consumer@ag.iowa.gov, 1-888-777-4590.

For Kansas Residents: You may contact the Kansas Office of the Attorney General, Consumer Protection Division, 120 SW 10th Ave, 2nd Floor, Topeka, KS 66612-1597, <https://ag.ks.gov/>, 1-800-432-2310.

For Kentucky residents: You may contact the Kentucky Office of the Attorney General, Consumer Protection Division, 1024 Capital Center Drive, Suite 200, Frankfort, Kentucky 40601, www.ag.ky.gov, 1-800-804-7556.

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

For Minnesota Residents: You may contact the Office of the Minnesota Attorney General, 445 Minnesota St Ste 1400, Saint Paul, MN 55101, www.ag.state.mn.us, 1-800-657-3787.

For Missouri Residents: You may contact the Missouri Office of the Attorney General, Consumer Protection, 207 W. High St., P.O. Box 899, Jefferson City, MO 65102, www.ago.mo.gov, 1-800-392-8222.

For New Mexico Residents: You may contact the New Mexico Office of the Attorney General, Consumer Protection Division, 408 Galisteo Street, Villagra Building, Santa Fe, NM 87501, www.nmag.gov, 1-844-255-9210.

For New York Residents: You may contact the New York Office of the Attorney General, Office of the Attorney General, The Capitol, Albany, NY 12224-0341, <https://ag.ny.gov>, 1-800-771-7755.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Main Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7266.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, Consumer Protection Division, 150 South Main Street, Providence, RI 02903, www.riag.ri.gov, 1-401-274-4400.

For Texas Residents: You may contact the Texas Office of the Attorney General, Office of the Attorney General, PO Box 12548, Austin, TX 78711-2548, www.texasattorneygeneral.gov, 1-800-621-0508.

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For North Carolina Residents: You are advised to report any suspected identity theft to law enforcement or to the North Carolina Attorney General.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident.