

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

November 17, 2022

VIA EMAIL

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

Dear Sir or Madam:

On behalf of our client Radio Free Asia ("RFA"), and pursuant to the Personal Information Protection Act ("PIPA"), this letter provides notice of a recent data security incident. By providing this notice, RFA does not waive any rights or defenses regarding the applicability of Maryland law or personal jurisdiction.

On June 28, 2022, RFA became aware of unknown activity within their email system which indicated unauthorized access to a limited number of servers (the "Incident"). Out of an abundance of caution and immediately following detection, RFA took systems offline and took measures to address and contain the Incident including launching an investigation, engaging data privacy and security professionals, working with law enforcement, changing passwords, and migrating to a new cloud-based email environment. The investigation determined that unauthorized access resulted from an exploit of a service provider's vulnerability, unknown by RFA at the time of the compromise. At this time, there is no evidence information has been misused; nevertheless, we are providing this notice.

We determined that the following types of information may have been impacted: name, address, social security number, driver's license number, passport number or other state identification number, health insurance information, medical information, and limited financial account information. Note that this describes all categories of information involved in this Incident, and it likely includes categories that are not relevant to each individual.

Since the Incident, RFA has implemented measures to further improve the security of its systems and practices including implementing stricter authentication keys and password reset policies and working with data privacy and security professionals to build a scalable and structured information security and privacy program.

A total of 3,779 individuals, including 693 Maryland residents, may have been affected by this Incident. Individual notice to these 693 Maryland residents was provided today, November 17, 2022. A copy of the mailed letter provided to potentially affected Maryland residents is attached hereto.

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

Sincerely,

A handwritten signature in black ink, appearing to read 'D. Greene', with a stylized flourish extending to the right.

Daniel P. Greene Esq.
Certified Information Privacy Professional, United States (CIPP/US)
Certified Information Privacy Professional, Europe (CIPP/E)

Encl.



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<Date>>

I am writing to inform you that we, Radio Free Asia (“RFA” or “we”) recently experienced a data security incident (“Incident”) which potentially involved your personal information (“Information”). This letter provides you with information about this Incident, the investigation, and although we are unaware of any misuse of your Information, steps you can take to protect your Information.

What Happened?

On June 28, 2022, we became aware of the Incident within our email system which indicated unauthorized access to a limited number of servers. Out of an abundance of caution and immediately following detection, RFA took systems offline and took measures to address and contain the Incident including launching an investigation, engaging data privacy and security professionals, working with law enforcement, changing passwords, and migrating to a new cloud-based email environment. The investigation determined that unauthorized access resulted from an exploit of a service provider’s vulnerability, unknown by RFA at the time of the compromise. At this time, there is no evidence Information has been misused; nevertheless, we are providing this notice.

What Information Was Involved?

We determined that the following types of Information may have been potentially impacted: name, address, social security number, driver’s license number, passport number or other state identification number, health insurance information, medical information, and limited financial information. Note that this list describes all categories of Information involved in this Incident, and it likely includes categories that are not relevant to you.

What We Are Doing.

Upon becoming aware of the Incident, we immediately implemented measures to further improve the security of our systems and practices. We worked with a leading privacy and security firm to aid in our investigation and response, and we are reporting this Incident to relevant government agencies.

As an added precaution to help protect your identity, we are offering a complimentary twenty-four (24) month credit monitoring through EQUIFAX. To activate your membership and start monitoring your personal Information please follow the steps below:

- You must **enroll by:** <<Enrollment Deadline>> (Your code will not work after this date.)
- Visit the EQUIFAX website to enroll: www.equifax.com/activate
- Provide your activation code: <<Activation Code>>

If you have questions or need assistance enrolling in EQUIFAX online, please contact [REDACTED] by <<Enrollment Deadline>>.

What Can You Do?

Through EQUIFAX, credit monitoring services are available to you at no cost for twenty-four (24) months. However, 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 Information.

For More Information.

If you have any questions about the Incident, please call [REDACTED], Monday through Friday, from 9:00 a.m. to 9:00 p.m. Eastern (excluding some U.S. national holidays).

Sincerely,

A handwritten signature in black ink, appearing to read "Bay Fang", written in a cursive style.

Bay Fang

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.



Enter your Activation Code: <<Activation Code>>

Enrollment Deadline: <<Enrollment Deadline>>

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product.

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications¹ when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts², which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock³
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to \$1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft⁴

Enrollment Instructions

Go to www.equifax.com/activate.

Enter your unique Activation Code of <<Activation Code>> then click “Submit” and follow these 4 steps:

1. **Register:**
Complete the form with your contact information and click “Continue”.
If you already have a myEquifax account, click the ‘Sign in here’ link under the “Let’s get started” header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4.
2. **Create Account:**
Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
Upon successful verification of your identity, you will see the Checkout Page.
Click ‘Sign Me Up’ to finish enrolling.
You’re done!
The confirmation page shows your completed enrollment.
Click “View My Product” to access the product features.

¹WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers’ personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers’ personal information is at risk of being traded.

²The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

³Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer’s identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com.

⁴The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.