



December 21, 2023

BY EMAIL

Orrick, Herrington & Sutcliffe LLP

401 Union Street
Suite 3300
Seattle, WA 98101-2668

+1 206 839 4300

orrick.com

Joseph C. Santiesteban

E jsantiesteban@orrick.com

D +1 206 839 4352

F +1 206 839 4301

To Whom It May Concern:

I am writing on behalf of our client, Qorvo, Inc. ("Qorvo"), to notify you of a cybersecurity event.

On August 7, 2023, Qorvo identified that an unauthorized actor had accessed some of its IT systems. After becoming aware of the access, Qorvo immediately began taking steps to stop and remediate the access, including taking certain systems offline. An investigation was then launched with assistance from external cybersecurity experts, and Qorvo promptly notified law enforcement. Qorvo subsequently discovered the unauthorized actor had accessed and may have acquired files containing personal information. Qorvo is unable to determine whether the files with your resident's personal information that were accessed were also exfiltrated.

Once Qorvo was able to identify the affected files, Qorvo began a process to determine what types of personal information were affected and to whom it relates. Qorvo determined that the personal information associated with 1 Maryland resident was in the files. The types of personal information that were in the affected files for the Maryland resident include their driver's license number and passport number.

Qorvo began notifying individuals on December 21, 2023, via U.S. First Class Mail. While Qorvo is not aware of any evidence that personal information has been misused as a result of this incident, Qorvo is offering individuals two years of free credit monitoring and identity protection services from TransUnion.

Prior to the incident, Qorvo had a number of cybersecurity measures in place, including endpoint detection and response tools across the environment. After becoming aware of this incident, Qorvo took steps to prevent further access to the impacted systems, including taking certain systems offline. As Qorvo brought systems back online, they took a series of steps to further strengthen their security controls.

A sample notice is attached as Attachment A to this letter. If you have any questions, please do not hesitate to contact me at +1 (408) 772-0709 or at jsantiesteban@orrick.com.

Respectfully yours,

/s/ Joseph C. Santiesteban

Partner, Orrick Herrington & Sutcliffe LLP

Qorvo Inc.
c/o Cyberscout
1 Keystone Ave., Unit 700
Cherry Hill, NJ 08003
DB-08273 1-1



Sample A. Sample
123 Main Street

December 21, 2023

Notice of Security Event

Dear _____,

We are writing to inform you of a recent cybersecurity incident that affected some of our internal IT systems. Please read this notice carefully, as it provides up-to-date information on what happened and what we are doing, as well as information on how you can obtain complimentary credit monitoring.

What happened?

Qorvo, Inc. ("Qorvo") experienced an unauthorized actor infiltrating some of our IT systems in August 2023 (the "Cybersecurity Incident"). After becoming aware of the access, we immediately began taking steps to stop and remediate the access, including taking certain systems entirely offline. An investigation was then launched with assistance from external cybersecurity experts, and we promptly notified law enforcement. Recently, we determined that the unauthorized actor had accessed and may have acquired files containing your personal information. We are unable to determine whether the files that were accessed were also exfiltrated.

What personal information was involved?

Once Qorvo identified the accessed files, we began a process to determine what types of personal information were affected and to whom it relates. While we worked quickly, this was a time-consuming process, and we wanted to provide you with accurate information.

Your personal information that was accessed during the Cybersecurity Incident included: [data elements].

What we are doing:

Prior to the incident, Qorvo had a number of cybersecurity measures in place, including endpoint detection and response tools across the environment. After becoming aware of this incident, we took steps to prevent further access to the impacted systems, including taking certain systems offline. As we brought systems back online, we took a series of steps to further strengthen our security controls.

At this time, we are not aware of any evidence that personal information has been misused as a result of this incident. However, Qorvo is offering you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score/Cyber Monitoring** services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Cyber monitoring will look out for your personal information on the dark web and alert you if your personally identifiable information is found online. Finally, we are providing you with proactive fraud assistance to help with any questions that you might have or in event that you become a victim of fraud.

These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

To activate your membership and start monitoring your personal information please log on to <https://secure.identityforce.com/benefit/qorvous> and follow the instructions provided. When prompted please provide the following unique code to receive services: [CODE]

In order for you to receive the monitoring services described above, you must enroll by March 20, 2024. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What you can do:

It is always a good idea to remain vigilant against threats of identity theft or fraud and to regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity. If you ever suspect that you are the victim of identity theft or fraud, you can contact your local police. You can also enroll in the credit monitoring being offered to you. Additional information about how to protect your identity is contained in this mailing.

For more information:

Qorvo has set up a dedicated call center to answer questions about the incident as well as the services that we are offering to you. Representatives are available for 90 days from the date of this letter. If you have questions, please call 1-800-405-6108 Monday through Friday from 8:00 a.m. to 8:00 p.m. Eastern time, and provide your unique code listed above.

We take the security of our data very seriously and we regret any inconvenience this incident may have caused you.

Sincerely,

The Qorvo Security Team

MORE INFORMATION ABOUT IDENTITY PROTECTION

INFORMATION ON OBTAINING A FREE CREDIT REPORT

U.S. residents are entitled under U.S. law to one free credit report annually from each of the three major credit bureaus. To order your free credit reports, visit www.annualcreditreport.com or call toll-free (877) 322-8228.

INFORMATION ON IMPLEMENTING A FRAUD ALERT OR SECURITY FREEZE

You can contact the three major credit bureaus at the addresses below to place a fraud alert on your credit report. A fraud alert indicates to anyone requesting your credit file that you suspect you are a possible victim of fraud. A fraud alert does not affect your ability to get a loan or credit. Instead, it alerts a business that your personal information might have been compromised and requires that business to verify your identity before issuing you credit. Although this may cause some short delay if you are the one applying for the credit, it might protect against someone else obtaining credit in your name.

A security freeze prohibits a credit reporting agency from releasing any information from a consumer's credit report without written authorization. However, please be aware that placing a security freeze on your credit report may delay, interfere with, or prevent the timely approval of any requests you make for new loans, credit, mortgages, employment, housing, or other services. A credit reporting agency may not charge you to place, temporarily lift, or permanently remove a security freeze.

To place a fraud alert or security freeze on your credit report, you must contact the three credit bureaus below:

Equifax	Experian	TransUnion
Consumer Fraud Division	Credit Fraud Center	TransUnion LLC
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19022-2000
(888) 766-0008	(888) 397-3742	(800) 680-7289
www.equifax.com	www.experian.com	www.transunion.com

To request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security Number;
3. Date of birth;
4. If you have moved in the past five (5) years, the addresses where you have lived over those prior five years;
5. Proof of current address such as a current utility bill or telephone bill; and
6. A legible photocopy of a government-issued identification card (state driver's license or ID card, military identification, etc.).

You may also contact the U.S. Federal Trade Commission ("FTC") for further information on fraud alerts, security freezes, and how to protect yourself from identity theft. The FTC can be contacted at 400 7th St. SW, Washington, DC 20024; telephone +1 (877) 382-4357; or www.consumer.gov/idtheft.

ADDITIONAL RESOURCES

Your state attorney general may also have advice on preventing identity theft, and you should report instances of known or suspected identity theft to law enforcement, your state attorney general, or the FTC.

District of Columbia Residents: The District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; oag@dc.gov, and www.oag.dc.gov.

California residents: Visit the California Office of Privacy Protection (<https://oag.ca.gov/privacy>) for additional information on protection against identity theft.

Iowa Residents: The Attorney General can be contacted at Office of Attorney General of Iowa, Hoover State Office Building, 1305 E. Walnut Street, Des Moines, Iowa 50319, +1 (515) 281-5164, www.iowaattorneygeneral.gov.

Maryland Residents: The Attorney General can be contacted at Office of Attorney General, 200 St. Paul Place, Baltimore, Maryland 21202; +1 (888) 743-0023; or www.marylandattorneygeneral.gov.

Massachusetts Residents: Under Massachusetts law, you have the right to obtain any police report filed in connection to the cybersecurity event. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it.

North Carolina Residents: The Attorney General can be contacted at 9001 Mail Service Center, Raleigh, NC 27699-9001; 877-566-7226 (Toll-free within North Carolina); +1 (919) 716-6400; or www.ncdoj.gov.

New Mexico Residents: You have rights under the federal Fair Credit Reporting Act (FCRA), which governs the collection and use of information pertaining to you by consumer reporting agencies. For more information about your rights under the FCRA, please visit <https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0096-fair-credit-reporting-act.pdf> or www.ftc.gov.

New York Residents: The Attorney General can be contacted at the Office of the Attorney General, The Capitol, Albany, NY 12224-0341, +1 (800)-771-7755; or www.ag.ny.gov.

Oregon Residents: The Attorney General can be contacted at Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, +1 (877) 877-9392 (toll-free in Oregon), +1 (503) 378-4400, or www.doj.state.or.us.

Rhode Island Residents: The Attorney General can be contacted at 150 South Main Street, Providence, Rhode Island 02903; +1 (401) 274-4400; or www.riag.ri.gov. You may also file a police report by contacting local or state law enforcement agencies.

For Arizona, California, Iowa, Montana, New York, North Carolina, Oregon, Washington, Washington, D.C., and West Virginia 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 bureaus directly to obtain such additional report(s).