



14611

MSC Software Corporation
4675 MacArthur Court
Suite 900
Newport Beach, CA 92660

February 26, 2019



##E4586-L01-0123456 *****SNGLP
SAMPLE A SAMPLE
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789

Activation code: ABCDEFGHI
Enrollment end date: 5/31/2019

Dear Sample A Sample:

We are writing to let you know about a data security incident. MSC Software Corporation takes the protection and proper use of your information very seriously. We are therefore contacting you to explain the incident and provide you with steps you can take to protect yourself.

What Happened

In January 2019 we discovered a potential security incident. We promptly began an investigation and engaged a cybersecurity and forensic firm to determine the nature and scope of the event, as well as whether any sensitive data was at risk. The forensic investigation confirmed that an employee's inbox had been accessed by an unauthorized actor and certain emails had been accessed and or acquired by the unauthorized actor. The forensic evidence also suggested that the goal of the unauthorized actor was to obtain fraudulent funds via wire transfer from the company. On February 7, 2019 we learned that certain personal information was contained in the affected emails.

While we have no evidence that your personal information was targeted or misused, we wanted to alert you and provide you with protective measures you can take. We encourage you to take the preventative measures outlined in this letter to help protect your information.

What Information Was Involved

While each individual case is different, the affected emails included data attributes such as: name, address, email address, phone number, social security number, date of birth, employer tax identification number, and/ or financial account number.

What are We Doing

We are notifying you so that you can take immediate action to protect yourself. We are conducting a thorough review of the potentially affected records and continue to implement additional security measures, internal controls, and safeguards, as well as continue to make changes to existing policies and procedures designed to prevent a similar occurrence from happening again.

In addition, to help protect your identity, we are offering a complimentary two-year membership of Experian's® IdentityWorksSM. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by:** Refer date on the top right hand corner above (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: www.experianidworks.com/3bcredit
- Provide your **activation code:** Refer to code on the top right hand corner above

0123456



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 877.890.9332 by May 31, 2019. Be prepared to provide engagement number **DB11008** as proof of eligibility for the identity restoration services by Experian.

Additional details regarding your 24-MONTH EXPERIAN IDENTITYWORKS Membership:

A credit card is **not** required for enrollment in Experian IdentityWorks.

You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorks:

- ◆ **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.
- ◆ **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- ◆ **Experian IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- ◆ **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 877.890.9332. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for one year from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.

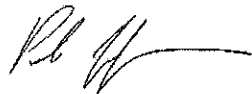
What You Can Do

We also recommend you remain vigilant with respect to reviewing your account statements and credit reports, and promptly report any suspicious activity or suspected identity theft to us and to the proper law enforcement authorities, including local law enforcement, your state's attorney general and/or the Federal Trade Commission ("FTC"). We have attached information regarding additional actions you may consider as well as resources to obtain additional information about identity theft and ways to protect yourself.

For More Information

We regret any inconvenience this incident may cause you and encourage you to take advantage of the product outlined herein. Should you have any further questions or concerns regarding this matter and/or the protections available to you, please do not hesitate to contact Olga Leanos, Human Resources, at olga.leanos@mscsoftware.com or 714-540-8900 (ext 4366).

Sincerely,



Paolo Guglielmini
CEO
MSC Software Corporation

* Offline members will be eligible to call for additional reports quarterly after enrolling

** Identity theft insurance is underwritten by insurance company subsidiaries or affiliates of American International Group, Inc. (AIG). The description herein is a summary and intended for informational purposes only and does not include all terms, conditions and exclusions of the policies described. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions

Additional Information

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 888-909-8872 P.O. Box 105281 Atlanta, GA 30348-5281 www.transunion.com

Free Credit Report. We remind you 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. 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, Maryland, Massachusetts, and New Jersey 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).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. Starting September 21, 2018, you can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

Don't confuse freezes with locks. They work in a similar way, but locks may have monthly fees. If you want a free freeze guaranteed by federal law, then opt for a freeze, not a lock.

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, display your name and current mailing address, and the date of issue.

For Colorado and Illinois residents: You may obtain information from the credit reporting agencies and the FTC about security freezes.

0123456



Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. Starting September 21, 2018, when you place a fraud alert, it will last one year, instead of 90 days. Fraud alerts will still be free and identity theft victims can still get an extended fraud alert for seven years.

For Colorado and Illinois residents: You may obtain additional information from the credit reporting agencies and the FTC about fraud alerts.

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 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 North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

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

Description of the Incident

In January 2019, MSC Software Corporation ("MSC Software") discovered a potential business email compromise after an employee found emails in their outbox that the employee had not sent. MSC Software promptly launched an investigation, contained and remediated the incident, and engaged a cybersecurity and forensic firm in order to understand the nature and scope of the event, as well as whether any sensitive data was at risk. The forensic investigation confirmed that the employee's inbox had been subject to unauthorized access and that certain emails had been accessed and or acquired by the unauthorized actor. The forensic evidence also suggested that the goal of the actor was to obtain fraudulent funds via wire transfer from the company.

Out of an abundance of caution, MSC Software undertook an extensive review of the affected emails to determine whether the emails contained any personal information. On February 7, 2019, MSC Software determined the affected emails contained Massachusetts residents' personal information. Although MSC Software understands the actor was financially motivated and is unaware of any actual or attempted misuse of the personal information, MSC Software is notifying affected individuals because their information was present in the impacted emails.