



Dear valued member of our team,

As you may know, Imaflex recently experienced a cyber security incident. We are writing to inform you that this incident may have affected your personal information.

Imaflex takes the confidentiality and security of your personal information very seriously. That's why we are informing you of this incident, advising you of the steps you can take to protect your personal information, and offering you free credit monitoring and identity protection services.

What happened?

On February 17, we detected unusual activity affecting certain systems on its network. We took immediate steps to secure the environment and hired cybersecurity experts to help us investigate.

Further to our investigation, we have reasons to believe that a third party has compromised some of our data. Unfortunately, it is possible that some of your personal information, including your contact information (phone number, address, e-mail), your social security number, your date of birth, your professional information (title, position, salary, employment history, performance appraisal, etc.) and other information contained in your human resources file, may have been affected by this compromise.

What we are doing

While we have no reason to believe that this information has been or will be misused, to protect you, we are offering you credit monitoring services for a period of 2 year(s) with Equifax. Details of these services are provided in the appendix attached to this letter.

We sincerely regret any concern this incident may cause. Protecting information is one of our highest priorities. We are already in the process of implementing additional security measures that will help us prevent similar incidents.

What you can do

In addition to signing up for the free credit monitoring services we offer, we recommend that you be vigilant about emails, text messages or phone calls asking you to provide sensitive information or to click on links or attachments, even if they appear to come from Imaflex or someone you know or trust. This will help protect you against targeted phishing campaigns.

We also recommend that you take the following additional steps to protect yourself:

- Carefully monitor all your accounts for any suspicious transactions or changes and inform the financial institutions where you hold accounts of this matter. This will help protect you against any attempt to use your information to access your bank accounts.
- Also monitor your credit reports for suspicious activity. 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 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 can print this form at <https://www.annualcreditreport.com/cra/requestformfinal.pdf>.

You can also contact the three national credit reporting agencies with the following contact details, to obtain more information about credit alerts:

Equifax

P.O. Box 740241
Atlanta, GA 30374
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

- You may also contact the three national credit reporting agencies with the above contact details to request a credit (security) freeze. Doing so can limit access to your credit reports, which may help protect you from some types of credit fraud. You may request a credit freeze online, over the phone or by mail.

Online. To freeze your credit reports online, please log in to your account with the credit reporting agency and go to the credit freeze management center.

Over the phone. To freeze your report over the phone, please contact the credit reporting agencies at the contact information provided above. You may need to verify your identity by entering your information or answering questions.

By mail. To freeze your report by mail, please follow each bureau's instructions. You may need to download and fill out a form and include copies (don't send originals) of documents to verify your identity and address.

These might include your:

- Social Security card
- Government-issued IDs
- Pay stubs or tax forms
- Utility bills or a lease agreement

There shall be no charge for a security freeze. For more information, please visit:
<https://www.usa.gov/credit-freeze>

The U.S. Government does not recommend creating a new social security number when affected by a data breach, since it does not protect you from fraud or identity theft as your old social security number remains active. For more information, please visit: <https://www.ssa.gov/>.

If you suspect your identity has been compromised, please reach out to the police to make a complaint. You can also contact the Federal Trade Commission for additional information and resources:

Federal Trade Commission

600 Pennsylvania Avenue
Washington, DC 20589
1-877-FTC-HELP (382-4357)
www.ftc.gov/bcp/edu/microsites/idtheft/

We understand that you may have questions that have not been addressed at this time. If you require additional information, please reach out to ■.

Yours sincerely,