

NOTICE OF DATA BREACH

March 18, 2016

Employees,

I regret to inform you of an incident that has occurred which involved exposure of your personal information.

WHAT HAPPENED

On March 11, 2016 an unidentified third party obtained access to W-2 information of all Dynamic Aviation employees for the year 2015 via an email “phishing” attack. On March 17, 2016 the fraudulent action was identified and it was determined that the information had been exposed to an unauthorized third party whose identity is presently unknown.

WHAT INFORMATION WAS DISCLOSED

The personal information disclosed was personal W-2 tax information for calendar year 2015. The following identifying information was exposed: employee name, address, city, state, zip, social security number, and 2015 wages earned. The unauthorized third party also obtained other information: costs of company-paid benefits for life and health insurance, employee contributions to retirement, dependent and health insurance, and taxes withheld from your earnings.

WHAT WE ARE DOING

Immediately after discovering the exposure we began working with internal and external technology and security resources to determine whether any other data was exposed and to secure our system from additional attacks. At present, we do not believe any other data was exposed.

We have reported the matter to law enforcement and we are taking steps to ensure that no unauthorized exposures will occur in the future.

We have also contacted companies that provide fraud assistance, identity theft prevention and mitigation services, and credit monitoring services to engage them to provide those services to Dynamic Aviation employees at no cost. We will provide enrollment and other information as soon as possible, but wanted to notify all employees promptly, so you can take steps to protect your personal information from being used for fraudulent purposes.

WHAT CAN YOU DO

This scam is a common means for tax refund fraud. If you have not already filed your 2015 tax returns, it is possible that a fraudulent tax return could have been or could be filed. You should call the IRS at 1-800-908-

4490 to report the phishing scam and ask for assistance with any fraudulent tax activity. The IRS has a lot of information and guidance on Identity protection on their website at <https://www.irs.gov/Individuals/Identity-Protection>.

Because your social security number was involved, we recommend that you place a fraud alert on your credit files. A fraud alert requires potential creditors to use what the law refers to as 'reasonable policies and procedures' to verify your identity before issuing credit in your name. A fraud alert lasts for 90 days. Just call one of the three credit reporting agencies at one of the numbers listed below. This will let you automatically place an alert with all three agencies. You will receive letters from all three, confirming the fraud alert and letting you know how to get a free copy of your credit report from each.

Experian:

Call Toll Free: 1-888-397-3742

P.O. Box 9554

Allen, TX 75013

www.experian.com

Equifax:

Call Toll Free: 1-888-766-0008

P.O. Box 105069

Atlanta, GA 30348-5069

www.equifax.com

TransUnion:

Call Toll Free: 1-800-680-7289

Fraud Victim Assistance Department

P.O. Box 2000

Chester, PA 19022-2000

www.transunion.com

When you receive your credit reports, look them over carefully. Look for accounts you did not open. Look for inquiries from creditors that you did not initiate. And look for personal information that is not accurate, such as your home address and social security number. If you notice anything you do not understand, immediately call the credit reporting agency at the telephone number on the report.

You have the right to obtain a police report, and you should remain vigilant for incidents of fraud and identity theft. If you do find suspicious activity on your credit reports or otherwise suspect that identity theft has occurred, you should report the incidents to your local police or sheriff's office, to the Federal Trade Commission, and/or to your state's attorney general's office. If you file a police report, you should request a copy of the police report, because you may need to give copies of the police report to creditors to clear up your records.

Even if you do not find any signs of fraud on your reports, we recommend that you check your credit reports periodically. You can keep the fraud alert in place by calling again after 90 days. In addition, you can place an extended fraud alert that will remain in place for seven years. Before placing an extended fraud alert, you will first need to create a free Identity Theft Report with the Federal Trade Commission, which you can do by visiting: www.identitytheft.gov.

You should remain vigilant by reviewing financial account statements and monitoring free credit reports. Federal law grants you the right to obtain a free copy of your credit report every year from each credit

reporting company (Experian, TransUnion, and Equifax). To obtain a free credit report, go to: annualcreditreport.com or call [1-877-322-8228](tel:1-877-322-8228).

We encourage all employees to review all of their financial accounts for any unusual or unauthorized activity and review the information in the links and attachments to this notice which provide details on other steps you can take including applying extended fraud alerts or credit freezes to your accounts. Please let us know immediately if you discover or experience any fraudulent activity.

FOR MORE INFORMATION

The Federal Trade Commission also provides information about how to avoid identity theft and what to do if you suspect your identity has been stolen.

The Federal Trade Commission
600 Pennsylvania Avenue NW
Washington, D.C. 20580
www.identitytheft.gov
1-877-ID-THEFT (877-438-4338)

You can obtain additional information about fraud alerts, credit freezes, and protecting yourself from identity theft from the credit reporting agencies and the Federal Trade Commission.

You may also contact me with any questions, jshank@dynamicaviation.com, or by office phone at (540)515-3514.

We sincerely apologize for this incident and regret any inconvenience this may cause you. We will be communicating additional information as soon as it is available.

Sincerely,

Joel Shank
HR, Director