



EVAN D. WOLFF
(202) 624-2615
EWolff@crowell.com

November 20, 2019

VIA FIRST CLASS MAIL

Consumer Protection Division
Security Breach Notifications
Office of the Attorney General of Iowa
1305 E. Walnut Street
Des Moines, IA 50319-0106

To Whom It May Concern:

We represent ARINC Incorporated, part of Collins Aerospace (“Collins”) with respect to an incident involving the potential exposure of certain personal information as described below. Collins has hired IDEXperts, a leading identity theft protection provider, to offer impacted individuals one year of complimentary MyIDCare services.

1. Nature of the event

On October 17, 2019, Collins was alerted that, due to a processing error, a former employee was accidentally sent the 2018 Form W-2 Wage and Tax Statements for approximately 1500 current and former Collins employees instead of only the former employee’s own documents.

2. Number of Iowa residents affected

Based on the investigation, four (4) Iowa residents were potentially affected. A formal notification letter will be sent to the individuals on November 22, 2019 via regular mail. A copy of the notification letter is included with this letter.

3. Information compromised

The information involved was W-2-related data including employees’ names, home addresses, compensation, tax withholdings and social security numbers.

4. Steps taken and plans relating to the event

Upon discovery of the accidental transmission, Collins immediately contacted the recipient of the data and requested that the information be deleted. The individual signed a written statement confirming that: 1) the email and W-2 attachment were deleted; 2) the individual did not retain a copy of the data; and 3) did not forward the information to anyone else.

Consumer Protection Division

November 20, 2019

Page 2

Because we were able to secure the recipient's immediate cooperation, we believe this event to be isolated and highly unlikely to result in a compromise additional data. Nevertheless, we are in the process of re-examining our processing procedures to prevent a reoccurrence of this type and to put forth other safeguards that will better serve data protection.

5. Contact information

If you have any additional questions, please contact Evan Wolff at EWolff@crowell.com or (202) 624-2615 during business hours.

Sincerely,



Evan D. Wolff

Enclosure



Collins Aerospace

A United Technologies Company

C/O ID Experts
10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.myidcare.com/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

November 22, 2019

Notice of Data Breach

Dear <<First Name>> <<Last Name>>,

We are writing to inform you of an incident involving your personal information. The intent of this letter is to share what we know, what we are doing to address it, and to provide some information and resources for steps you can take to protect your personal information.

What Happened

Collins Aerospace recently discovered that, due to a processing error, a copy of your 2018 Wage and Tax Statement, Form W-2, was accidentally sent via email to another individual. This incident occurred on October 7, 2019.

What Information Was Involved

The information involved was W-2-related data including your name, home address, compensation, tax withholdings and social security number.

What We Are Doing

Upon discovery of the accidental transmission, we immediately contacted the recipient of the data and requested that the information be deleted. The individual signed a written statement confirming that: 1) the email and W-2 attachment were deleted; 2) the individual did not retain a copy of the data; and 3) did not forward the information to anyone else.

Because we were able to secure the recipient's immediate cooperation, we believe this event to be isolated and highly unlikely to result in a compromise to your data. Nevertheless, we are in the process of re-examining our processing procedures to prevent a reoccurrence of this type and to put forth other safeguards that will better serve data protection.

We thus wanted to make you aware of these events and provide you with information about how to protect yourself.

What You Can Do

Although we believe that it is highly unlikely this incident will result in a compromise to your data, Collins is making available to you credit monitoring services. We encourage you to contact ID Experts, a data breach and recovery services expert, to enroll in free MyIDCare services by calling 1-800-939-4170 or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare services include 12 months of triple bureau credit monitoring, CyberScan dark web monitoring, a \$1,000,000 insurance reimbursement policy and fully managed identity theft recovery services. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll in these services is February 22, 2020.

We also encourage you to periodically check your credit reports to ensure that no fraudulent activity has occurred. Even if there are no signs of fraud on these reports, we recommend that you remain vigilant, continue to check these credit reports and your account statements periodically, and report anything suspicious to law enforcement.

We have also included a Reference Guide that suggests other steps you may take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

Again, at this time, there is no evidence that your information has been misused. However, we encourage you to take full advantage of this service offering.

For More Information

Keeping your personal information secure is of the utmost importance to us. We sincerely regret any concern or inconvenience this event may cause you and are taking steps to help prevent this type of incident from happening in the future.

If you have questions regarding this letter, please contact Global People Services at (866) 295-4747 or PeopleServices.Collins.US@utc.com.

Sincerely,

Collins Aerospace People Services

Enclosures

Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go to <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at 1-800-939-4170 to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. 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. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

For residents of Iowa, Maryland, Michigan, Missouri, North Carolina, Oregon, and West Virginia.

It is required by state laws to inform you that you may obtain a copy of your credit report, free of charge, whether or not you suspect any unauthorized activity on your account.

For residents of Iowa.

State law advises you to report any suspected identity theft to law enforcement or to the Attorney General.

For residents of Oregon.

State laws advise you to report any suspected identity theft to law enforcement, as well as the Attorney General and Federal Trade Commission.

For residents of Massachusetts and Rhode Island.

It is required by state law that you are informed of your right to obtain a police report if you are a victim of identity theft.

For residents of Massachusetts, Rhode Island, and West Virginia.

You also have the right to place a security freeze on your credit report by contacting any of the credit bureaus listed at above. 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. The following information must be included when requesting a security freeze (note that if you 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. The consumer reporting agency may charge a fee of up to \$5.00 to place a freeze or lift or remove a freeze and free if you are a victim of identity theft or the spouse of a victim of identity theft, and you have submitted a valid police report relating to the identity theft incident to the consumer reporting agency.

For residents of Illinois, Maryland, Rhode Island and North Carolina.

You can obtain information from the Federal Trade Commission, and for residents of Maryland, Rhode Island and North Carolina, from your respective state Office of the Attorney General, about fraud alerts, security freezes, and steps you can take toward preventing identity theft.

Federal Trade Commission Consumer Response Center
600 Pennsylvania Avenue, NW Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov

Maryland Office of the Attorney General Consumer Protection Division
200 St. Paul Place Baltimore, MD 21202
1-888-743-0023
www.oag.state.md.us

Rhode Island Office of the Attorney General Consumer Protection Unit
(401) 274-4400
<http://www.riag.ri.gov>

North Carolina Office of the Attorney General Consumer Protection Division
9001 Mail Service Center Raleigh, NC 27699-9001
1-877-566-7226
www.ncdoj.com