

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K STREET, NW
TELEPHONE (202) 223-7300
WASHINGTON, DC 20006-1047

1285 AVENUE OF THE AMERICAS
NEW YORK, NY 10019-6064
TELEPHONE (212) 373-3000

UNIT 5201, FORTUNE FINANCIAL CENTER
5 DONGSANHUA ZHONGLU
CHAORYANG DISTRICT, BEIJING 100020, CHINA
TELEPHONE (86-10) 5628-6300

SUITES 3601 - 3606 & 3610
36/F, GLOUCESTER TOWER
THE LANDMARK
15 QUEEN'S ROAD, CENTRAL
HONG KONG
TELEPHONE (852) 2846-0300

ALDER CASTLE
10 NOBLE STREET
LONDON EC2V 7JU, UNITED KINGDOM
TELEPHONE (44 20) 7367 1600

535 MISSION STREET, 24TH FLOOR
SAN FRANCISCO, CA 94105
TELEPHONE (415) 432-5100

FUKOKU SEIMEI BUILDING
2-2 UCHISAIWAICHO 2-CHOME
CHIYODA-KU, TOKYO 100-0011, JAPAN
TELEPHONE (81-3) 3597-8101

TORONTO-DOMINION CENTRE
77 KING STREET WEST, SUITE 3100
P.O. BOX 226
TORONTO, ONTARIO M5K 1J3
TELEPHONE (416) 504-0520

500 DELAWARE AVENUE, SUITE 200
POST OFFICE BOX 32
WILMINGTON, DE 19899-0032
TELEPHONE (302) 655-4410

WRITER'S DIRECT DIAL NUMBER

(202) 223-7485

WRITER'S DIRECT FACSIMILE

(202) 204-7395

WRITER'S DIRECT E-MAIL ADDRESS

pcarey@paulweiss.com



July 26, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

On behalf of our client HEICO Corporation ("HEICO"), an aerospace and electronics manufacturing company, I am writing to inform you about a recent incident in which personal information relating to a Maryland resident was accessed by an unauthorized third party. HEICO's headquarters is located at 3000 Taft Street Hollywood, Florida 33021.

Specifically, HEICO was the victim of a cybersecurity incident in which a criminal gained access to certain corporate systems and data between March 2-3, 2023. After discovering the incident on March 2, 2023, HEICO worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. HEICO concluded that the criminal stole and posted on the dark web certain internal business documents related to HEICO.

Through HEICO's investigation, the company determined that the third party accessed the name and Social Security number relating to one (1) Maryland resident.

HEICO maintains a written information security program. With professional support from third-party cybersecurity experts, HEICO promptly responded to contain and investigate the incident. HEICO also alerted and cooperated with law enforcement. HEICO's containment and remediation actions included restricting network access, blocking known indicators of compromise, completing a global password reset, rebuilding affected servers and endpoints, and deploying additional security tools to provide enhanced monitoring capabilities and endpoint protection.

Office of the Attorney General
Attn: Security Breach Notification

2

HEICO will notify one (1) Maryland resident of this incident on or about January 27, 2023. HEICO will provide this individual with an offer for 24 months of complementary credit monitoring. The individual can enroll in the Equifax Credit Watch Gold service by going to www.equifax.com/activate or calling (888) EQUIFAX (378-4329) and using the unique activation code provided in the individual notice.

Attached is a copy of the letter that HEICO is providing to the Maryland resident.

Please do not hesitate to contact me at (202) 223-7485 if you have any questions. I also can be reached at pcarey@paulweiss.com and at the below address:

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, DC 20006-1047

Sincerely,

/s/ Peter Carey

Peter Carey
Counsel

Attachment



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>

July 27, 2023

Notice of Data Breach

Dear <<Name 1>>:

On behalf of HEICO Corporation ("HEICO"), I am writing to inform you about an incident that involved certain personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. HEICO was the victim of a cybersecurity incident in which a criminal gained access to certain corporate systems and data between March 2-3, 2023. After discovering the incident on March 2, 2023, HEICO worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. We concluded that the criminal stole and posted on the dark web certain internal business documents related to HEICO.

WHAT INFORMATION WAS INVOLVED. We determined that your personal information was present in the data that was stolen and posted on the dark web, including your name and <<Breached Elements>>.

WHAT WE ARE DOING. Information security is a priority for HEICO. We took immediate steps in response to the incident to stop the unauthorized access and secure our systems. We also conducted a thorough investigation, which included our full cooperation with law enforcement.

WHAT YOU CAN DO. Consistent with certain laws, we are providing you with the following information about general steps that a consumer can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary 24-month credit monitoring service. During this period, HEICO will pay for Equifax to provide you with its Credit Watch Gold service, which includes, among other things, single bureau credit monitoring, dark web monitoring, and identity theft protection and restoration services, including up to \$1,000,000 of identity theft insurance coverage. You have until <<Enrollment Deadline>> to activate the free credit monitoring service by using the following activation code: <<Activation Code>>. This code is unique for your use and should not be shared. To enroll, go to www.equifax.com/activate or call (888) EQUIFAX (378-4329).

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institution.

In addition, you may contact the Federal Trade Commission ("FTC") or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC's web site, www.ftc.gov/idtheft/, call the FTC at (877) IDTHEFT (438-4338), or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit-reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit-reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax
(800) 685-1111
P.O. Box 740241
Atlanta, GA 30374-0241
www.equifax.com/personal/credit-report-services

Experian
(888) 397-3742
P.O. Box 9701
Allen, TX 75013
www.experian.com/help

TransUnion
(888) 909-8872
Fraud Victim Assistance Division
P.O. Box 2000
Chester, PA 19022
www.transunion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and credit freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze or restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us directly at 954-744-7677 if you have any questions or concerns.

Sincerely,

Julie Dobulis
Corporate Director, Human Resources & Payroll
HEICO Corporation

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office.

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

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General	New York Department of State
Consumer Frauds & Protection Bureau	Division of Consumer Protection
120 Broadway, 3 rd Floor	99 Washington Avenue, Suite 650
New York, NY 10271	Albany, New York 12231
(800) 771-7755	(800) 697-1220
www.ag.ny.gov	www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office.

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7726
<http://www.ncdoj.com>

PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K STREET, NW
TELEPHONE (202) 223-7300

WASHINGTON, DC 20006-1047

1285 AVENUE OF THE AMERICAS
NEW YORK, NY 10019-6064
TELEPHONE (212) 373-3000

UNIT 5201, FORTUNE FINANCIAL CENTER
5 DONGSANHUAN ZHONGLU
CHAoyANG DISTRICT, BEIJING 100020, CHINA
TELEPHONE (86-10) 5828-6300

SUITES 3601 – 3606 & 3610
36/F, GLOUCESTER TOWER
THE LANDMARK
15 QUEEN'S ROAD, CENTRAL
HONG KONG
TELEPHONE (852) 2846-0300

ALDER CASTLE
10 NOBLE STREET
LONDON EC2V 7JU, UNITED KINGDOM
TELEPHONE (44 20) 7367 1600

535 MISSION STREET, 24TH FLOOR
SAN FRANCISCO, CA 94105
TELEPHONE (628) 432-5100

FUKOKU SEIMEI BUILDING
2-2 UCHISAIWAICHO 2-CHOME
CHIYODA-KU, TOKYO 100-0011, JAPAN
TELEPHONE (81-3) 3597-8101

TORONTO-DOMINION CENTRE
77 KING STREET WEST, SUITE 3100
P.O. BOX 226
TORONTO, ONTARIO M5K 1J3
TELEPHONE (416) 504-0520

500 DELAWARE AVENUE, SUITE 200
POST OFFICE BOX 32
WILMINGTON, DE 19899-0032
TELEPHONE (302) 655-4410

WRITER'S DIRECT DIAL NUMBER

(202) 223-7485

WRITER'S DIRECT FACSIMILE

(202) 204-7395

WRITER'S DIRECT E-MAIL ADDRESS

pcarey@paulweiss.com

July 26, 2023

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202

To Whom It May Concern:

On behalf of our client HEICO Corporation ("HEICO"), an aerospace and electronics manufacturing company, I am writing to inform you about a recent incident in which personal information relating to a Maryland resident was accessed by an unauthorized third party. HEICO's headquarters is located at 3000 Taft Street Hollywood, Florida 33021.

Specifically, HEICO was the victim of a cybersecurity incident in which a criminal gained access to certain corporate systems and data between March 2-3, 2023. After discovering the incident on March 2, 2023, HEICO worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. HEICO concluded that the criminal stole and posted on the dark web certain internal business documents related to HEICO.

Through HEICO's investigation, the company determined that the third party accessed the name and Social Security number relating to one (1) Maryland resident.

HEICO maintains a written information security program. With professional support from third-party cybersecurity experts, HEICO promptly responded to contain and investigate the incident. HEICO also alerted and cooperated with law enforcement. HEICO's containment and remediation actions included restricting network access, blocking known indicators of compromise, completing a global password reset, rebuilding affected servers and endpoints, and deploying additional security tools to provide enhanced monitoring capabilities and endpoint protection.

Office of the Attorney General
Attn: Security Breach Notification

2

HEICO will notify one (1) Maryland resident of this incident on or about January 27, 2023. HEICO will provide this individual with an offer for 24 months of complementary credit monitoring. The individual can enroll in the Equifax Credit Watch Gold service by going to www.equifax.com/activate or calling (888) EQUIFAX (378-4329) and using the unique activation code provided in the individual notice.

Attached is a copy of the letter that HEICO is providing to the Maryland resident.

Please do not hesitate to contact me at (202) 223-7485 if you have any questions. I also can be reached at pcarey@paulweiss.com and at the below address:

Paul, Weiss, Rifkind, Wharton & Garrison LLP
2001 K Street, NW
Washington, DC 20006-1047

Sincerely,

/s/ Peter Carey

Peter Carey
Counsel

Attachment



Secure Processing Center
P.O. Box 3826
Suwanee, GA 30024

<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<City>><<State>><<Zip>>

July 27, 2023

Notice of Data Breach

Dear <<Name 1>>:

On behalf of HEICO Corporation (“HEICO”), I am writing to inform you about an incident that involved certain personal information about you. We regret that this incident occurred and take the security of personal information seriously.

WHAT HAPPENED. HEICO was the victim of a cybersecurity incident in which a criminal gained access to certain corporate systems and data between March 2-3, 2023. After discovering the incident on March 2, 2023, HEICO worked diligently with an external forensic investigation firm to determine the source and scope of this unauthorized access. We concluded that the criminal stole and posted on the dark web certain internal business documents related to HEICO.

WHAT INFORMATION WAS INVOLVED. We determined that your personal information was present in the data that was stolen and posted on the dark web, including your name and <<Breached Elements>>.

WHAT WE ARE DOING. Information security is a priority for HEICO. We took immediate steps in response to the incident to stop the unauthorized access and secure our systems. We also conducted a thorough investigation, which included our full cooperation with law enforcement.

WHAT YOU CAN DO. Consistent with certain laws, we are providing you with the following information about general steps that a consumer can take to protect against potential misuse of personal information.

As a precaution, we have arranged for you, at your option, to enroll in a complimentary 24-month credit monitoring service. During this period, HEICO will pay for Equifax to provide you with its Credit Watch Gold service, which includes, among other things, single bureau credit monitoring, dark web monitoring, and identity theft protection and restoration services, including up to \$1,000,000 of identity theft insurance coverage. You have until <<Enrollment Deadline>> to activate the free credit monitoring service by using the following activation code: <<Activation Code>>. This code is unique for your use and should not be shared. To enroll, go to www.equifax.com/activate or call (888) EQUIFAX (378-4329).

You should always remain vigilant for incidents of fraud and identity theft, including by regularly reviewing your account statements and monitoring free credit reports. If you discover any suspicious or unusual activity on your accounts or suspect identity theft or fraud, be sure to report it immediately to your financial institution.

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement, including your Attorney General, to report incidents of identity theft or to learn about steps you can take to protect yourself from identity theft. To learn more, you can go to the FTC’s web site, www.ftc.gov/idtheft/, call the FTC at (877) IDTHEFT (438-4338), or write to the FTC at Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580.

You may also periodically obtain credit reports from each nationwide credit-reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you should request that the credit-reporting agency delete that information from your credit report file. In addition, under the federal Fair Credit Reporting Act ("FCRA"), you are entitled to one free copy of your credit report every 12 months from each of the three nationwide credit reporting agencies. You may obtain a free copy of your credit report by going to www.AnnualCreditReport.com or by calling (877) 322-8228. You may contact the nationwide credit reporting agencies at:

Equifax	Experian	TransUnion
(800) 685-1111	(888) 397-3742	(888) 909-8872
P.O. Box 740241	P.O. Box 9701	Fraud Victim Assistance Division
Atlanta, GA 30374-0241	Allen, TX 75013	P.O. Box 2000
www.equifax.com/personal/credit-report-services	www.experian.com/help	www.transunion.com/credit-help

You also have other rights under the FCRA. For further information about your rights under the FCRA, please visit: http://files.consumerfinance.gov/f/201410_cfpb_summary_your-rights-under-fcra.pdf.

In addition, you may obtain additional information from the FTC and the credit reporting agencies about fraud alerts and credit freezes. You can add a fraud alert to your credit report file to help protect your credit information. A fraud alert can make it more difficult for someone to get credit in your name because it tells creditors to follow certain procedures to protect you, but it also may delay your ability to obtain credit. You may place a fraud alert in your file by calling just one of the three nationwide credit reporting agencies listed above. As soon as that agency processes your fraud alert, it will notify the other two agencies, which then must also place fraud alerts in your file.

In addition, you can contact the nationwide credit reporting agencies at the numbers listed above to place a security freeze or restrict access to your credit report. You will need to supply your name, address, date of birth, Social Security number, and other personal information. After receiving your request, each credit reporting agency will send you a confirmation letter containing a unique PIN or password that you will need to lift or remove the freeze. You should keep the PIN or password in a safe place.

FOR MORE INFORMATION. Please know that we regret any inconvenience or concern this incident may cause you. Please do not hesitate to contact us directly at 954-744-7677 if you have any questions or concerns.

Sincerely,

Julie Dobulis
Corporate Director, Human Resources & Payroll
HEICO Corporation

IF YOU ARE A MARYLAND RESIDENT: You may obtain information about avoiding identity theft from the Maryland Attorney General's Office.

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

IF YOU ARE A NEW YORK RESIDENT: You may obtain information about security breach response and identity theft prevention and protection from the following New York state agencies:

New York Attorney General	New York Department of State
Consumer Frauds & Protection Bureau	Division of Consumer Protection
120 Broadway, 3 rd Floor	99 Washington Avenue, Suite 650
New York, NY 10271	Albany, New York 12231
(800) 771-7755	(800) 697-1220
www.ag.ny.gov	www.dos.ny.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may obtain information about preventing identity theft from the North Carolina Attorney General's Office.

North Carolina Department of Justice
Attorney General Josh Stein
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7726
<http://www.ncdoj.com>