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

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

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

December 6, 2019

Re: Notice of Data Breach

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

We are writing to let you know about a security incident that we experienced that may have involved certain personal information about you.

What Happened
On October 25, 2019, Cargolux identified that the credentials for the mailboxes of two U.S.-based Cargolux employees had been compromised. As a result of a phishing attack, an unauthorized party was able to access the mailboxes. The impacted mailboxes may have contained information collected by the Cargolux human resources department.

Cargolux has retained an independent, third-party consultant to investigate this matter. At this stage in the investigation, there is evidence that the mailboxes may have been compromised between October 17 and October 19, 2019. Because Cargolux cannot conclusively rule out the possibility that your information was accessed or acquired, we are writing to notify you of this incident.

What Information Was Involved
The compromised mailboxes contained information typically collected by the Cargolux human resources department in connection with the performance of their tasks. The unauthorized party may have accessed or acquired your name, along with one or more of the following types of personal information:

- Social Security number
- Government-issued ID number
- Financial account information
- Medical information
- Health insurance information, such as plan identification numbers

What We Are Doing
In addition to conducting an investigation, Cargolux reset the passwords for the mailboxes affected by the incident. Cargolux has also engaged a third-party consultant to analyze the security of its IT systems and has delivered updated trainings related to the identification and treatment of suspicious emails.

In addition, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 12 months of credit and CyberScan monitoring, a $1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity is compromised.

What You Can Do
As a precaution to protect against potential misuse of your personal information, we recommend that you regularly monitor your health records, explanations of benefits, account statements, and free credit reports. You are entitled to obtain a free annual credit report from each of the nationwide credit reporting companies—Equifax, Experian, and TransUnion. To do so, please go to www.annualcreditreport.com or call 1-877-322-8228. If you notice any suspicious activity, you should promptly report such activity to your service provider, the proper law enforcement agencies, the Federal Trade Commission, and your state's attorney general.

As a precaution to protect against potential misuse of your health information, we recommend that you regularly monitor any explanation of benefits statements that you receive from your health plan, to check for any unfamiliar health care services. If you notice any health care services that you did not receive listed on one of these statements, please contact your health plan.

You may also place a fraud alert on your credit file. Adding a fraud alert to your credit report file makes it more difficult for someone to get credit in your name by requiring creditors to follow certain procedures. However, this may also delay your ability to obtain credit. No one is allowed to place a fraud alert on your credit report except you, so if you elect to do so, please follow the instructions below to place the alert. To place a fraud alert on your file, contact one of the three nationwide credit reporting agencies; the first agency that processes your fraud alert will notify the others to do so as well. You may also add a security freeze to your credit report file to prohibit a credit reporting agency from releasing information from your credit report without your prior written authorization. In some cases, agencies may charge a fee to place or remove such a freeze.

Equifax	**Experian**	**TransUnion**
Consumer Fraud Division	Fraud Division	Fraud Victim Assistance Department
P.O. Box 740256	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30374	Allen, TX 75013	Chester, PA 19016
www.equifax.com	www.experian.com	www.transunion.com
1-800-525-6285	1-888-397-3742	1-800-680-7289

You may contact the FTC or your state's consumer protection authority to obtain additional information about avoiding identity theft.

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-FTC-HELP (1-877-382-4357) / www.ftc.gov/idtheft

A list of state attorneys general with contact information is available here: https://www.naag.org/naag/attorneys-general/whos-my-ag.php

For More Information
We take our responsibility to safeguard your personal information seriously and remain committed to protecting your privacy and the security of your personal information. If you have any questions about this incident, we encourage you to contact ID Experts with those questions and to enroll in free MyIDCare services by calling (800) 939-4170 or going to https://app.myidcare.com/account-creation/protect and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 6 am - 5 pm Pacific Time. Please note the deadline to enroll is March 6, 2020.

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. MyIDCare representatives have been fully versed on the incident and can answer questions or concerns you may have regarding protection of your personal information.

You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter.

Please call (800) 939-4170 or go to https://app.myidcare.com/account-creation/protect for assistance or for any additional questions you may have.

Sincerely,

Emese Bekessy

Emese Bekessy
Executive Vice President HR, Legal Affairs and Compliance

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 (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	Experian Fraud Reporting	TransUnion Fraud Reporting
1-866-349-5191	1-888-397-3742	1-800-680-7289
P.O. Box 105069	P.O. Box 9554	P.O. Box 2000
Atlanta, GA 30348-5069	Allen, TX 75013	Chester, PA 19022-2000
www.equifax.com	www.experian.com	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.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (http://www.ca.gov/Privacy) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601**,** www.ag.ky.gov, Telephone: 1-502-696-5300.

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

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit "prescreened" offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina**,** 9001 Mail Service Center
Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.