Continental Automotive Systems, Inc.
c/o Cyberscout
PO Box 1286
Dearborn, MI 48120-9998

P
[redacted]

August 15, 2023

Notice of Cyberattack and Data Breach at Continental: Your personal data is affected

Dear [redacted],

We are writing to you today to inform you about the cyberattack at Continental which, to our regret, may affect you personally. Continental is working to understand the scope of this incident - it is important to us to inform you accordingly and comprehensively. Therefore, we would like to explain to you in this letter:

- What happened during the cyberattack,
- What information was involved,
- What we have been doing and are currently doing in response to the cyberattack,
- What you can do, and
- Whom you can contact for more information related to the incident.

Please take the time to read the information carefully.

What Happened
At the beginning of August 2022, IT experts from Continental discovered that a hacker group had gained access to our IT systems from approximately July 4, 2022, to approximately August 5, 2022. We reacted immediately and removed the attackers from our systems. We were thus able to avert an encryption of our systems. However, the criminals copied and stole data during the time they had access to parts of our IT systems. The hackers have been offering data stolen from Continental on the so-called "darknet" on the Internet since November 2022. As of the date of this letter, the data has not yet been published, but the attackers have published a list with the file names of the stolen data.

What We Are Doing
From the very beginning, we have been in close contact with the relevant authorities, including the FBI, and are coordinating with them regarding how to proceed. Our efforts include compliance with all data protection and data privacy obligations. Since we became aware of the theft of the affected data, we have been conducting a comprehensive analysis of the stolen data. Within this process, we have also checked whether information about employees is contained in the data records that ended up in the hands of the criminals.

What Information Was Involved

To our great regret, the review of the stolen data has shown that your personal data may have been affected. Please be aware that our response remains active, and not everything in this letter may apply to your situation.

Specialists are working diligently to investigate the incident and its consequences.

For Current Continental Employees Only: We will keep you continually informed about the current status of the incident via our internal communication channels on the intranet.

0000101104G0500
P

In general, the affected employee data is data that we use and retain in the ordinary course of the commencement of an employment relationship, during the employment relationship, and/or upon the termination of an employment relationship. In addition, the affected data includes employee data that we use and store for purposes of occupational health and safety, to assert or defend against legal claims, or to fulfill legal obligations. Beyond this, commercial, tax, and other applicable laws require us to retain employee data for long periods after an employee leaves the company. This also includes data belonging to persons who have applied for employment with Continental in the past.

The following categories of information considered personal data under U.S. laws may be affected by the incident:

- Identity data, for example birth certificates, proof of identity (such as ID cards, passports, driver's licenses, residence permits) or individual details taken from these in internal personnel documents.
- Account and bank data as well as tax information, for example as part of pay slips or an official tax document (such as account details, IBAN, debit or credit card numbers or tax classifications).
- Health data or information on physical/mental attributes, for example in the context of previous sickness notifications or documents from occupational safety and occupational health, for example in the form of submitted sickness notifications, accident reports, documents providing information on an existing/previous severe disability or pregnancy.
- Insurance data as well as information on membership of a statutory or private health insurance fund, for example your health insurance number or information on certificates of incapacity for work.

What You Can Do

As a precautionary measure, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service for 24 months. This service is provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services. You can find information about the service and how to enroll in Appendix A to this letter. In addition, you can find more information about steps that you can take in Appendix B to this letter.

In addition to enrolling in complimentary credit monitoring service, you can protect yourself by monitoring your financial accounts and your account statements for unusual or unauthorized activity over the next 12 to 24 months and promptly reporting any suspected identity theft to the police.

You should be vigilant against possible "phishing" and other fraudulent communications and emails that appear to be (but are not) sent from Continental brand email addresses. We recommend that you pay close attention to suspicious emails in your online accounts, change your private passwords as a precaution, and do not disclose any confidential information to unknown persons. Fundamentally, you should use different passwords of appropriate length and complexity for every system. Please also do not open any attachments in suspicious emails or follow any links that may be included in a suspicious email.

BE AWARE: No reputable provider would ask you to disclose confidential login data by email or telephone.

What Measures We Have Taken

In connection with the cyberattack and its aftermath we have already taken the following measures:

- Immediately after the incident became known, technical security measures were taken designed to prevent further access to or encryption of our systems.
- The dark web is being actively monitored regarding potential publication of the affected data.
- Leading experts, particularly in the fields of cybersecurity and forensics, have been engaged to fully investigate this incident.
- There is ongoing coordination and close cooperation with domestic and foreign law enforcement authorities.
- Affected employee data has been thoroughly reviewed with regard to its criticality in order to be able to inform you as quickly as possible.
- Processes for changing bank and account data have been adapted.

For More Information

Continental has analyzed your personal data in order to investigate the incident and be able to provide you with the information contained in this letter. To the extent required by law, we will also share your data with government agencies and authorities.

If you have any questions, please contact Continental at any time:

Continental Automotive Systems, Inc.
Attn: HR – Cyber-Attack
1 Continental Drive
Auburn Hills, Michigan 48326
Phone: (248) 391-5609
Email: cyberattack_US@continental.com

0000102048000 0 P

Appendix A

In response to the incident, we are providing you with access to **Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score** services at no charge. These services provide you with alerts for 24 months from the date of enrollment when changes occur to your credit file.

How do I enroll for the free services?

To enroll in Credit Monitoring services at no charge, please log on to **https://secure.identityforce.com/benefit/continental** and follow the instructions provided. When prompted please provide the following unique code to receive services: **RYJ5N6NZ7T**

In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

What can I do on my own to address this situation?
If you choose not to use these services, we strongly urge you to do the following:

If you choose to place a fraud alert on your own, you will need to contact one of the three major credit agencies directly at:

Experian (1-888-397-3742)	**Equifax (1-800-525-6285)**	**TransUnion (1-800-680-7289)**
P.O. Box 4500	**P.O. Box 740241**	**P.O. Box 2000**
Allen, TX 75013	**Atlanta, GA 30374**	**Chester, PA 19016**
www.experian.com	www.equifax.com	www.transunion.com

Also, should you wish to obtain a credit report and monitor it on your own:

- **IMMEDIATELY obtain free copies of your credit report and monitor them upon receipt for any suspicious activity. You can obtain your free copies by going to the following website: www.annualcreditreport.com or by calling them toll-free at 1-877-322-8228. (Hearing impaired consumers can access their TDD service at 1-877-730-4204.**
- **Upon receipt of your credit report, we recommend that you review it carefully for any suspicious activity.**
- **Be sure to promptly report any suspicious activity to Continental**

You can also obtain more information from the Federal Trade Commission (FTC) about identity theft and ways to protect yourself. The FTC has an identity theft hotline: 877-438-4338; TTY: 1-866-653-4261. They also provide information on-line at www.ftc.gov/idtheft.

Appendix B

MEASURES THAT YOU CAN TAKE TO PROTECT YOURSELF WITH REGARD TO CONSUMER CREDIT REPORTING BUREAUS:

To help protect yourself against identity theft, you may consider placing a fraud alert or security freeze on your credit report.

Fraud Alert. When you place a "fraud alert" on your credit report, businesses who pull your credit report will see that you may be a victim of identity theft. The company may then choose to verify your identity before they extend credit to anyone who purports to be you. This may make it harder for an identity thief to open more accounts in your name.

To place an alert, contact any one of the three main credit reporting bureaus. That company is required to tell the other two bureaus about the alert. When you first place a fraud alert on your account, it will remain for at least 90 days, after which you can renew it. When you do place an alert on your report, be sure that all three major credit reporting companies have your current contact information so they can get in touch with you.

Security Freeze. A "security freeze" or "credit freeze" goes further than an alert and lets you restrict access to your credit report entirely, which in turn makes it more difficult for identity thieves to open new accounts in your name. This is because most creditors need to see your credit report before they approve a new account. If creditors cannot see your file, they may not extend the credit.

A credit freeze does not affect your credit score. A credit freeze also does not:

1. prevent you from getting your free annual credit report;
2. keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you are doing any of these, you will need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it is best to check with the credit reporting company in advance;
3. prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

To place a freeze on your credit reports, you need to contact each of the major credit reporting bureaus. You will need to supply your name, address, date of birth, Social Security number and other personal information. Credit reporting agencies are required to place or remove a freeze on your credit report without charge.

Below, we provide contact information for the major credit reporting agencies. You may obtain additional information from these resources about preventing or remedying identity theft, including by setting up fraud alerts or security freezes and by reviewing your credit report. The contact information of those agencies is provided below:

EQUIFAX

Fraud Alerts

Equifax Information Services LLC
P.O. Box 105069
Atlanta, GA 30348-5069
888-836-6351 (automated service line)
800-525-6285 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Security Freezes

Equifax Information Services LLC
P.O. Box 105788
Atlanta, GA 30348-5788
888-298-0045 (customer care agents)
https://my.equifax.com/consumer-registration/UCSC/#/personal-info

Credit Reports

Central Source LLC
P.O. Box 105283
Atlanta, GA 30348-5283
https://www.annualcreditreport.com/index.action

EXPERIAN

Fraud Alerts

1-888-397-3742
https://www.experian.com/fraud/center.html

Security Freezes

1-888-397-3742
https://www.experian.com/freeze/center.html

Credit Reports

1-888-397-3742
https://www.annualcreditreport.com/index.action

TRANSUNION

Fraud Alerts

TransUnion Fraud Victim Assistance
P.O. Box 2000
Chester, PA 19016
800-680-7289
https://fraud.transunion.com

Security Freezes

TransUnion
P.O. Box 160
Woodlyn, PA 19094
888-909-8872
https://freeze.transunion.com/

Credit Reports

Central Source LLC
P.O. Box 105283
Atlanta, GA 30348-5283
https://www.annualcreditreport.com/index.action

INFORMATION AND ASSISTANCE THAT YOU CAN OBTAIN FROM FEDERAL AND STATE LAW ENFORCEMENT AND CONSUMER PROTECTION AGENCIES:

If you believe that you may be the victim of identity theft, you should report that immediately to law enforcement, your state Attorney General, or the Federal Trade Commission.

You also may wish to review the resources provided by the Federal Trade Commission on how to avoid identity theft. You can reach the FTC at:

Bureau of Consumer Protection
Federal Trade Commission
600 Pennsylvania Ave., NW
Washington, DC 20580
1-877-ID-THEFT (877-438-4338)
https://www.identitytheft.gov/

PROTECTIONS OF THE FEDERAL FAIR CREDIT REPORTING ACT

The Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary or your major rights under the FCRA. In particular, the FCRA enables identity-theft victims to demand the removal of false entries on their credit reports that result from the theft. *For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.*

You must be told if information in your file has been used against you. Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment or to take another adverse action against you must tell you, and must give you the name, address, and phone number of the agency that provided the information.

You have the right to know what is in your file. You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free disclosure if:

- a person has taken adverse action against you because of information in your credit report;
- you are the victim of identity theft and place a fraud alert in your file;
- your file contains inaccurate information as a result of fraud;
- you are on public assistance;
- you are unemployed but expect to apply for employment within 60 days.

You have the right to ask for a credit score. Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

You have the right to dispute incomplete or inaccurate information. If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must

investigate unless your dispute is frivolous. *See www.ftc.gov/credit for an explanation of dispute procedures*.

Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information. Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

Consumer reporting agencies may not report outdated negative information. In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

Access to your file is limited. A consumer reporting agency may provide information about you only to people with a valid need—usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

You must give your consent for reports to be provided to employers. A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. *For more information, go to www.ftc.gov/credit*.

You may limit "prescreened" offers of credit and insurance you get based on information in your credit report. Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the lists these offers are based on. *You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688)*.

You may seek damages from violators. If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

Identity theft victims and active-duty military personnel have additional rights. *For more information, visit www.ftc.gov/credit*.