

January 16, 2025

Via Email

Idtheft@oag.state.md.us

Re: Supplement to Legal Notice of Information Security Incident

To Whom it May Concern:

I am writing on behalf of my client Craft Beer Company GP (including its subsidiaries Duvel Moortgat USA, Ltd., Boulevard Brewing Company, and Brewery Ommegang, Ltd.) ("CBC") to supplement the notice letter that was provided to your department May 8, 2024.

As explained in the previous notice, considering the sensitivity of the data involved, and in light of how long it would have taken to fully review the impacted data, CBC provided notice of the compromise prior to the investigation being finalized. This was to allow the impacted individuals notice to be able to take action as soon as possible to mitigate any potential negative impacts if their data was compromised.

We are writing to inform you that CBC has finalized their E-Discovery analysis on the data that had been exfiltrated and needs to update the original submission stating 9 Maryland residents to 14 Maryland residents. Please note that nothing has changed regarding what happened or the content of the notice letter originally provided to the impacted individuals.

Please let us know if you have any additional questions regarding this incident.

Sincerely,



Todd C. Kinney

May 8, 2024



Norton Rose Fulbright US LLP
1301 Avenue of the Americas
New York, New York 10019-6022
United States of America

Direct line +1 212 318 3080

Via Email

ldtheft@oag.state.md.us

Tel +1 212 318 3000

Fax +1 212 318 3400

Re: Legal Notice of Information Security Incident

Dear Sir or Madam:

I am writing on behalf of my client Craft Beer Company GP (including its subsidiaries Duvel Moortgat USA, Ltd., Boulevard Brewing Company, and Brewery Ommegang, Ltd.) ("CBC") to inform you of a cybersecurity incident that it was the victim of.

On March 5, 2024, CBC discovered that an unauthorized third party gained access to their network. Upon becoming aware of the incident, CBC took immediate action to contain and respond to it, including but not limited to: taking its network offline; retaining outside forensic firms to respond, investigate, and remediate the incident; and notifying law enforcement. The incident has been contained, but the investigation into its effects is still ongoing.

Although the investigation is not yet complete, it has been determined that some of CBC's data was compromised as a result of this incident, and that portions of the compromised data likely included the personal information of current and former employees, and their spouses and dependents. Considering the sensitivity of this data, and in light of how long it will take to fully review the impacted data, CBC is notifying all current and former employees, and if relevant their spouses and dependents, of the compromise so that action can be taken as soon as possible to mitigate any potential negative impacts if their data was compromised.

Because CBC is proactively notifying these individuals and cannot be sure what information was compromised at this time, the notifications will generally describe the type of information contained in the current or former employees file with CBC applicable to each individual. CBC is also offering 24-months of complimentary credit monitoring and fraud protection services to all individuals notified. There are 9 Maryland residents included within the list of current and former employees.

Thus, today May 8, 2024, CBC will begin mailing the notifications to the 9 Maryland residents. A copy of the notice letter is attached. CBC is also providing a telephone number for individuals to call with any questions regarding the incident.

As the investigation work continues, it is possible that there will be a need to notify additional individuals beyond current and former employees, and thus, if necessary we will update you further should the investigation reveal that any additional Maryland residents need to be notified.

If you have any questions or need further information regarding this incident, please do not hesitate to contact me.

Norton Rose Fulbright US LLP is a limited liability partnership registered under the laws of Texas.

Norton Rose Fulbright US LLP, Norton Rose Fulbright LLP, Norton Rose Fulbright Australia, Norton Rose Fulbright Canada LLP and Norton Rose Fulbright South Africa Inc are separate legal entities and all of them are members of Norton Rose Fulbright Verein, a Swiss verein. Norton Rose Fulbright Verein helps coordinate the activities of the members but does not itself provide legal services to clients. Details of each entity, with certain regulatory information, are available at nortonrosefulbright.com.

May 8, 2024
Page 2

 NORTON ROSE FULBRIGHT

Sincerely,

Annmarie Giblin

CRAFT BEER COMPANY GP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

7 1 1584 *****SNGLP

SAMPLE A. SAMPLE - L01

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



May 8, 2024

Dear Sample A. Sample:

Re: NOTICE OF DATA BREACH – PLEASE READ CAREFULLY

Craft Beer Company GP (including its subsidiaries Duvel Moortgat USA, Ltd., Boulevard Brewing Company, and Brewery Ommegang, Ltd.) (“CBC” or “we”) is writing to inform you of a cybersecurity incident in which your personal information may have been impacted by an unauthorized third party. This notice provides information concerning the incident, steps we have taken in response, and the services we are offering to help you protect your personal information. Additionally, at the end of this notice, we have included information on additional steps beyond the services we are providing that you may take to help protect your personal information.

What Happened?

On March 5, 2024, we discovered that an unauthorized third party gained access to our network. Upon becoming aware of the incident, we took immediate action to contain the incident and respond to it. Specifically, we promptly isolated all sites, shut down servers, and disconnected our system from the internet. We also launched an internal investigation, contacted law enforcement, and engaged external cybersecurity forensic experts to conduct an external investigation into this intrusion and help to further secure our systems against any additional potential vulnerabilities. Additionally, we promptly implemented the experts’ recommended actions to prevent the disclosure of data as we continued to investigate the situation and while we continue our work on remediating the incident. This work is continuing and while our network has been secured, we are still investigating and remediating the effects of the incident.

As our work continues, we have determined that unfortunately certain personal information of our current and former employees, and their dependents, was impacted during this incident, and thus we are commencing the reporting process for those individuals now.

What Information Was Involved?

Although we are still responding to and investigating the extent of this incident, we have already been able to determine that this incident may have impacted the personal information of CBC’s current and former employees, and potentially that of their spouses and dependents. Thus, we have commenced the reporting process for those individuals.

While we cannot be sure at this time what personal information of yours was compromised, such information could have included your name, home address, social security number, passport or other government identification such as your driver’s license, your bank account number, and other information such as regarding your health insurance and related life events, like medical leave.

What Are We Doing?

In addition to the immediate actions taken to contain the incident and respond to it as noted above, we are also taking additional appropriate steps in response to it, including re-training our staff to address how the incident occurred and working with them to understand how to avoid similar incidents in the future. We are also reviewing and updating our policies and procedures to further harden our cybersecurity program to hopefully prevent incidents of this nature from occurring again in the future.

Please note that we are still investigating this incident and took steps to notify our affected current and former employees as soon as we learned of the potential impact to their data. We will keep you updated as needed if any relevant information related to your information is learned.

Additionally, while we have no evidence at this time that your information has been misused for purposes of fraud or identity theft, we want to help prevent any such misuse, and thus we are offering you twenty-four (24) months of identity protection services and credit monitoring through Experian IdentityWorksSM. This product provides you with identity protection support focused on detection and resolution of identity theft. You can enroll in these services by following the instructions below. Please note that we strongly recommend that you enroll in Experian IdentityWorksSM, which is free of charge to you and will not hurt your credit score.

What You Can Do

In addition to enrolling in the identity protection services and credit monitoring through Experian IdentityWorksSM as detailed below, we also recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your financial account statements and free credit reports for any unauthorized activity. We also recommend that you remain alert for unsolicited communications involving your personal information.

Please review the “Additional Steps You Can Take” section at the end of this letter, which describes additional precautionary steps you can take to protect your personal information, including contacting the Federal Trade Commission and/or placing a fraud alert or security freeze on your credit file.

More Information

If you have any further questions regarding this incident, please call our dedicated and toll-free response line at 833-931-8840 between the hours of 8am to 8pm Central Time, Monday-Friday. Please reference the engagement number B120427 when calling.

Sincerely,

A handwritten signature in black ink, appearing to read 'Nick Hale', with a stylized, flowing script.

Nick Hale
General Counsel

INSTRUCTIONS FOR EXPERIAN IDENTITYWORKS

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months. This product provides you with identity protection support focused on detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: July 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorksSM online, please contact Experian's customer care team at 833-931-8840 by **July 31, 2024**. Be prepared to provide engagement number **B120427** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorksSM. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorksSM:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-8840. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.¹²

ADDITIONAL STEPS YOU CAN TAKE

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every twelve (12) months, from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one (1) business day. If you request a lift of the freeze, the agency must lift it within one (1) hour. If you make your request by mail, the agency must place or lift the freeze within three (3) business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are 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)

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven (7) years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

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

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

For Texas residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. 3 Rhode Island residents were impacted by this incident.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

CRAFT BEER COMPANY GP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

7 1 1577 *****SNGLP

SAMPLE A. SAMPLE - L02

APT ABC



123 ANY ST

ANYTOWN, US 12345-6789



May 8, 2024

Dear Sample A. Sample:

Re: NOTICE OF DATA BREACH – PLEASE READ CAREFULLY

Craft Beer Company GP (including its subsidiaries Duvel Moortgat USA, Ltd., Boulevard Brewing Company, and Brewery Ommegang, Ltd.) (“CBC” or “we”) is writing to inform you of a cybersecurity incident in which your personal information may have been impacted by an unauthorized third party. This notice provides information concerning the incident, steps we have taken in response, and the services we are offering to help you protect your personal information. Additionally, at the end of this notice, we have included information on additional steps beyond the services we are providing that you may take to help protect your personal information.

What Happened?

On March 5, 2024, we discovered that an unauthorized third party gained access to our network. Upon becoming aware of the incident, we took immediate action to contain the incident and respond to it. Specifically, we promptly isolated all sites, shut down servers, and disconnected our system from the internet. We also launched an internal investigation, contacted law enforcement, and engaged external cybersecurity forensic experts to conduct an external investigation into this intrusion and help to further secure our systems against any additional potential vulnerabilities. Additionally, we promptly implemented the experts’ recommended actions to prevent the disclosure of data as we continued to investigate the situation and while we continue our work on remediating the incident. This work is continuing and while our network has been secured, we are still investigating and remediating the effects of the incident.

As our work continues, we have determined that unfortunately certain personal information of our current and former employees, and their dependents, was impacted during this incident, and thus we are commencing the reporting process for those individuals now.

What Information Was Involved?

Although we are still responding to and investigating the extent of this incident, we have already been able to determine that this incident may have impacted the personal information of CBC’s current and former employees, and potentially that of their spouses and dependents. Thus, we have commenced the reporting process for those individuals.

Unfortunately, we can confirm that your passport was compromised in this incident, and possibly additional personal information, such as your home address, social security number, other government identification such as your driver’s license, your bank account number, and other information such as regarding your health insurance and related life events, like medical leave.

What Are We Doing?

In addition to the immediate actions taken to contain the incident and respond to it as noted above, we are also taking additional appropriate steps in response to it, including re-training our staff to address how the incident occurred and working with them to understand how to avoid similar incidents in the future. We are also reviewing and updating our policies and procedures to further harden our cybersecurity program to hopefully prevent incidents of this nature from occurring again in the future.

Please note that we are still investigating this incident and took steps to notify our affected current and former employees as soon as we learned of the potential impact to their data. We will keep you updated as needed if any relevant information related to your information is learned.

Additionally, while we have no evidence at this time that your information has been misused for purposes of fraud or identity theft, we want to help prevent any such misuse, and thus we are offering you twenty-four (24) months of identity protection services and credit monitoring through Experian IdentityWorksSM. This product provides you with identity protection support focused on detection and resolution of identity theft. You can enroll in these services by following the instructions below. Please note that we strongly recommend that you enroll in Experian IdentityWorksSM, which is free of charge to you and will not hurt your credit score.

What You Can Do

In addition to enrolling in the identity protection services and credit monitoring through Experian IdentityWorksSM as detailed below, we also recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your financial account statements and free credit reports for any unauthorized activity. We also recommend that you remain alert for unsolicited communications involving your personal information.

Please review the “Additional Steps You Can Take” section at the end of this letter, which describes additional precautionary steps you can take to protect your personal information, including contacting the Federal Trade Commission and/or placing a fraud alert or security freeze on your credit file.

More Information

If you have any further questions regarding this incident, please call our dedicated and toll-free response line at 833-931-8840 between the hours of 8am to 8pm Central Time, Monday-Friday. Please reference the engagement number B120427 when calling.

Sincerely,

A handwritten signature in black ink, appearing to read 'Nick Hale', with a stylized, cursive script.

Nick Hale
General Counsel

INSTRUCTIONS FOR EXPERIAN IDENTITYWORKS

To help protect your identity, we are offering complimentary access to Experian IdentityWorksSM for twenty-four (24) months. This product provides you with identity protection support focused on detection and resolution of identity theft. To start monitoring your personal information, please follow the steps below:

- Ensure that you **enroll by: July 31, 2024** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorksSM website to enroll: <https://www.experianidworks.com/credit>
- Provide your **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with identity restoration, or would like an alternative to enrolling in Experian IdentityWorksSM online, please contact Experian's customer care team at 833-931-8840 by **July 31, 2024**. Be prepared to provide engagement number **B120427** as proof of eligibility for the identity restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP:

A credit card is **not** required for enrollment in Experian IdentityWorksSM. You can contact Experian **immediately** regarding any fraud issues, and have access to the following features once you enroll in Experian IdentityWorksSM:

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.*
- **Credit Monitoring:** Actively monitors Experian file for indicators of fraud.
- **Identity Restoration:** Identity Restoration agents are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorksSM ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorksSM membership has expired.
- **Up to \$1 Million Identity Theft Insurance**:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-8840. If, after discussing your situation with an agent, it is determined that Identity Restoration support is needed, then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that this Identity Restoration support is available to you for 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration. You will also find self-help tips and information about identity protection at this site.¹²

ADDITIONAL STEPS YOU CAN TAKE

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, GA 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, TX 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. We remind you to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your financial account statements, you should immediately report any such charges to your financial institution. You may obtain a copy of your credit report, free of charge, once every twelve (12) months, from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator, or have a valid power of attorney, you can get a free freeze for that person too.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one (1) business day. If you request a lift of the freeze, the agency must lift it within one (1) hour. If you make your request by mail, the agency must place or lift the freeze within three (3) business days after it gets your request. You also can lift the freeze temporarily without a fee.

¹ Offline members will be eligible to call for additional reports quarterly after enrolling.

² The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

The following information must be included when requesting a security freeze (note that if you are 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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one (1) year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven (7) years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

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

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

For Texas residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If you are the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. 3 Rhode Island residents were impacted by this incident.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

CRAFT BEER COMPANY GP

Return Mail Processing
PO Box 999
Suwanee, GA 30024

6 1 1352 *****AUTO**ALL FOR AADC 130
PARENT OR GUARDIAN OF SAMPLE A. SAMPLE - L03
APT ABC
123 ANY ST
ANYTOWN, US 12345-6789



May 8, 2024

Dear Sample A. Sample:

Re: NOTICE OF DATA BREACH – PLEASE READ CAREFULLY

Craft Beer Company GP (including its subsidiaries Duvel Moortgat USA, Ltd., Boulevard Brewing Company, and Brewery Ommegang, Ltd.) (“CBC” or “we”) is writing to inform you of a cybersecurity incident in which your child’s personal information may have been impacted by an unauthorized third party. This notice provides information concerning the incident, steps we have taken in response, and the services we are offering to help you protect your child’s personal information. Additionally, at the end of this notice, we have included information on additional steps beyond the services we are providing that you may take to help protect your child’s personal information.

What Happened?

On March 5, 2024, we discovered that an unauthorized third party gained access to our network. Upon becoming aware of the incident, we took immediate action to contain the incident and respond to it. Specifically, we promptly isolated all sites, shut down servers, and disconnected our system from the internet. We also launched an internal investigation, contacted law enforcement, and engaged external cybersecurity forensic experts to conduct an external investigation into this intrusion and help to further secure our systems against any additional potential vulnerabilities. Additionally, we promptly implemented the experts’ recommended actions to prevent the disclosure of data as we continued to investigate the situation and while we continue our work on remediating the incident. This work is continuing and while our network has been secured, we are still investigating and remediating the effects of the incident.

As our work continues, we have determined that unfortunately certain personal information of our current and former employees, and their dependents, was impacted during this incident, and thus we are commencing the reporting process for those individuals now.

What Information Was Involved?

Although we are still responding to and investigating the extent of this incident, we have already been able to determine that this incident may have impacted the personal information of CBC’s current and former employees, and potentially that of their spouses and dependents. Thus, we have commenced the reporting process for those individuals.

While we cannot be sure at this time what personal information of your child was compromised, such information could have included their name, home address, social security number, and other information such as regarding their health insurance and related life events, like their birth or extended illness, if such event impacted the employee (i.e., the employee took parental leave).

What Are We Doing?

In addition to the immediate actions taken to contain the incident and respond to it as noted above, we are also taking additional appropriate steps in response to it, including re-training our staff to address how the incident occurred and working with them to understand how to avoid similar incidents in the future. We are also reviewing and updating our policies and procedures to further harden our cybersecurity program to hopefully prevent incidents of this nature from occurring again in the future.

Please note that we are still investigating this incident and took steps to notify our affected current and former employees as soon as we learned of the potential impact to their data. We will keep you updated as needed if any relevant information related to your child’s information is learned.

Additionally, while we have no evidence at this time that your child's information has been misused for purposes of fraud or identity theft, we want to help prevent any such misuse, and thus we are offering you twenty-four (24) months of identity protection services and credit monitoring through Experian IdentityWorksSM. This product provides you with identity protection support focused on detection and resolution of identity theft. You can enroll in these services by following the instructions below. Please note that we strongly recommend that you enroll in Experian IdentityWorksSM, which is free of charge to you and will not hurt your child's credit score.

What You Can Do

In addition to enrolling in the identity protection services and credit monitoring through Experian IdentityWorksSM as detailed below, we also recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your financial account statements and free credit reports for any unauthorized activity. We also recommend that you remain alert for unsolicited communications involving your personal information.

Please review the "Additional Steps You Can Take" section at the end of this letter, which describes additional precautionary steps you can take to protect your personal information, including contacting the Federal Trade Commission and/or placing a fraud alert or security freeze on your credit file.

More Information

If you have any further questions regarding this incident, please call our dedicated and toll-free response line at 833-931-8840 between the hours of 8am to 8pm Central Time, Monday-Friday. Please reference the engagement number B120428 when calling.

Sincerely,

A handwritten signature in black ink, appearing to read "Nick Hale", with a stylized flourish at the end.

Nick Hale
General Counsel

ATTACHMENT A

To help protect your minor's identity, we are offering complimentary access to Experian IdentityWorksSM for 24 months. This product provides you with superior identity detection and resolution of identity theft. To activate your membership and start monitoring your personal information, please follow the steps below:

- Ensure that you **July 31, 2024** (Your minor's code will not work after this date.)
- **Visit** the Experian IdentityWorks website to enroll: <https://www.experianidworks.com/minorplus>
- Provide your minor's **activation code: ABCDEFGHI**

If you have questions about the product, need assistance with Identity Restoration that arose as a result of this incident or would like an alternative to enrolling in Experian IdentityWorks online, please contact Experian's customer care team at 833-931-8840 by July 31, 2024. Be prepared to provide engagement number B120428 as proof of eligibility for the Identity Restoration services by Experian.

ADDITIONAL DETAILS REGARDING YOUR MINOR'S 24-MONTH EXPERIAN IDENTITYWORKS MEMBERSHIP

A credit card is not required for enrollment in Experian IdentityWorks.

You can contact Experian immediately regarding any fraud issues and have access to the following features once you enroll in Experian IdentityWorks:

- **Social Security Number Trace:** Monitoring to determine whether enrolled minors in your household have an Experian credit report. Alerts of all names, aliases and addresses that become associated with your minor's Social Security Number (SSN) on the Experian credit report.
- **Internet Surveillance:** Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
- **Identity Restoration:** Identity Restoration specialists are immediately available to help you address credit and non-credit related fraud.
- **Experian IdentityWorks ExtendCARETM:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **\$1 Million Identity Theft Insurance^{**}:** Provides coverage for certain costs and unauthorized electronic fund transfers.

If you believe there was fraudulent use of your minor's information as a result of this incident and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833-931-8840. If, after discussing your situation with an agent, it is determined that identity restoration support is needed then an Experian Identity Restoration agent is available to work with you to investigate and resolve each incident of fraud that occurred from the date of the incident (including, as appropriate, helping you with contacting credit grantors to dispute charges and close accounts; assisting you in placing a freeze on your credit file with the three major credit bureaus; and assisting you with contacting government agencies to help restore your identity to its proper condition).

Please note that Identity Restoration is available to your minor 24 months from the date of this letter and does not require any action on your part at this time. The Terms and Conditions for this offer are located at www.ExperianIDWorks.com/restoration.

Additional Steps You Can Take

Contact information for the three nationwide credit reporting companies is as follows:

Equifax	Experian	TransUnion
Phone: 1-800-685-1111 P.O. Box 740256 Atlanta, Georgia 30348 www.equifax.com	Phone: 1-888-397-3742 P.O. Box 9554 Allen, Texas 75013 www.experian.com	Phone: 1-888-909-8872 P.O. Box 2000 Chester, PA 19016 www.transunion.com

Free Credit Report. Regardless of whether you choose to take advantage of the complimentary identity monitoring, it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. If you identify any unauthorized charges on your child's financial account statements, you should immediately report any such charges to your child's financial institution. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

For Colorado, Georgia, Maine, Maryland, Massachusetts, and New Jersey residents:

You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

Security Freeze. Security freezes, also known as credit freezes, restrict access to your credit file, making it harder for identity thieves to open new accounts in your name. You can freeze and unfreeze your credit file for free. You also can get a free freeze for your children who are under 16. And if you are someone's guardian, conservator or have a valid power of attorney, you can get a free freeze for that person, too.

****** The Identity Theft Insurance is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

How will these freezes work? Contact all three of the nationwide credit reporting agencies – Equifax, Experian, and TransUnion. If you request a freeze online or by phone, the agency must place the freeze within one business day. If you request a lift of the freeze, the agency must lift it within one hour. If you make your request by mail, the agency must place or lift the freeze within three business days after it gets your request. You also can lift the freeze temporarily without a fee.

The following information must be included when requesting a security freeze (note that if you are 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.

For New Mexico residents: You may obtain a security freeze on your credit report to protect your privacy and ensure that credit is not granted in your name without your knowledge. You may submit a declaration of removal to remove information placed in your credit report as a result of being a victim of identity theft. You have a right to place a security freeze on your credit report or submit a declaration of removal pursuant to the Fair Credit Reporting and Identity Security Act. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

Fraud Alerts. A fraud alert tells businesses that check your credit that they should check with you before opening a new account. An initial fraud alert stays on your credit report for one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

Federal Trade Commission and State Attorneys General Offices. If you believe your child is the victim of identity theft or have reason to believe your child's personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or avoid identity theft. You may contact the Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

For Connecticut Residents: You may contact and obtain information from your state attorney general at: Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808- 5318, www.ct.gov/ag

For District of Columbia Residents: You may contact the Office of the Attorney General for the District of Columbia, 441 4th Street NW, Suite 1100 South, Washington, D.C. 20001, <https://oag.dc.gov>, 202-442-9828.

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

For New York Residents: You may contact the New York Department of State Division of Consumer Protection, One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1- 800-697-1220, <http://www.dos.ny.gov/consumerprotection>; and New York State Office of the Attorney General, The Capitol, Albany, NY 12224-0341, 1-800-771-7755, <https://ag.ny.gov>.

For North Carolina Residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For Rhode Island Residents: You may contact the Rhode Island Office of the Attorney General, 150 South Main Street, Providence, RI 02903, <http://www.riag.ri.gov>, 401-274-4400.

For Texas residents: You may contact and obtain information from your state attorney general at: Office of the Texas Attorney General www.texasattorneygeneral.gov/consumer-protection/identity-theft or contact the Identity Theft Hotline at 800-621-0508 (toll-free).

Reporting of identity theft and obtaining a police report.

You have the right to obtain any police report filed in the United States in regard to this incident. If your child is the victim of fraud or identity theft, you also have the right to file a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft. You also have a right to file a police report and obtain a copy of it.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

For Rhode Island residents: You have the right to file or obtain a police report regarding this incident. 3 Rhode Island residents were impacted by this incident.

Report Incidents. If you detect any unauthorized transactions in a financial account, promptly notify your payment card company or financial institution. If you are in the U.S. and detect any incident of identity theft or fraud, promptly report the incident to law enforcement, the FTC and your state Attorney General. If you believe your identity has been stolen, the FTC recommends that you take these steps:

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. For more information, please visit <https://www.identitytheft.gov/>.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.