

December 17, 2020

**VIA ELECTRONIC MAIL (ATTORNEYGENERAL@DOJ.NH.GOV)**

New Hampshire Department of Justice  
Office of the Attorney General  
33 Capitol Street  
Concord, NH 03301

Re: **Incident Notification**

To Whom It May Concern:

We write to inform you of a recent data security incident on behalf of our client, Campari America (“Campari”), a distilled spirits importer and producer. Campari, located at 1114 Avenue of the Americas, 19th Floor, New York, NY 10036, is a wholly owned subsidiary of Davide Campari-Milano, N.V. (together with its other affiliates, the “Campari Group”). This recent security incident may have affected the personal information of approximately one (1) New Hampshire resident, who is a Campari employee or former employee.

On or about Sunday, November 1, 2020, Campari learned that the Campari Group was the target of a malware attack where the attacker accessed parts of Campari Group’s network. The Campari Group’s IT team, with the help of cyber security experts, worked quickly to limit the attacker’s access. We do not know with certainty what internal information was exposed or stolen in the course of the breach of our network, but Campari generally does not collect or store consumer information because the bulk of its sales are to a wholesaler.

The types of employee information accessed and exposed through the company’s employee directory include name, surname, work email address, job title, line manager, work phone number, work mobile phone number, and “employee identification code” (an internal number used to identify employees and consultants within the Campari Group’s IT environment). The attacker also appears to have accessed the Social Security Numbers of some employees.

On or about November 12, 2020, Campari mailed written notification to all impacted individuals, including the one (1) New Hampshire resident. Please find enclosed a sample of the notification letter, which was sent to the resident. Campari has also retained a third-party specialist in identity theft protection to provide all impacted individuals with two (2) years of identity protection services, including credit monitoring, free of charge.

# GIBSON DUNN

December 17, 2020

Page 2

If you have any questions or require additional information about the aforementioned data security incident, please do not hesitate to contact me at [asouthwell@gibsondunn.com](mailto:asouthwell@gibsondunn.com) or directly by telephone at (212) 351-3981.

Sincerely,



Alexander H. Southwell

Enclosure

# CAMPARI GROUP

Return Mail Processing  
PO Box 589  
Claysburg, PA 16625-0589

November 12, 2020

F9701-L02-0000002 T00017 P003 \*\*\*\*\*ALL FOR AADC 123



SAMPLE A SAMPLE -L02

APT B

123 ANY ST

ANYTOWN, US 12345-6789



## **RE: NOTICE OF DATA BREACH**

*Please read this entire letter.*

Dear Sample A Sample:

We are contacting you regarding a data security incident at Campari Group that occurred on or around November 1, 2020. Although our investigation is ongoing, it appears the threat actor accessed your Social Security Number. As a result, this information was exposed to others. We sincerely apologize for any inconvenience and stress this may cause you and are taking steps to minimize the risks related to the incident and ensure your information is kept as safe as possible. Please know that we do take protection of your personal information extremely seriously.

### **What happened?**

On or about Sunday, November 1, 2020, Campari Group was the target of a malware attack, which was promptly discovered and addressed. Campari Group's IT team, with the help of cyber security experts, worked quickly to limit the threat actor's access.

### **What information was involved?**

We do not know with certainty at this time what internal information was accessed in the course of the breach of our network, but our current investigation indicates that your name and Social Security number were exposed by the threat actors. Separate from this breach, the threat actors also obtained access to our global directory containing the following data regarding all Campari Group employees, as well as consultants to whom an "ext" Campari email address had been allocated: name, surname, work email address, job title, line manager, mobile phone number (only as registered in such directory for business purposes), and "employee identification code" (an internal number used to identify the employee/consultant within the Campari IT environment).

The information maintained in our servers was collected in the normal course of business by Campari. To our knowledge, only some servers were accessed but our team is continuing to assess the impact.

CAMPARI AMERICA LLC  
1114 Avenue of the Americas, 19th Floor – New York, New York 10036 – USA  
[www.camparigroup.com](http://www.camparigroup.com)

**TOASTING LIFE TOGETHER**

0000002



F9701-L02

## What are we doing?

As soon as Campari learned that its network experienced a cyber-attack, our IT team and external consultants cut off the threat actor's access quickly and have been working hard at recovery of our systems and files. We have also reported the incident to law enforcement, including the Italian cyber police, the Italian Data Protection Authority, and the United States FBI, and we are collaborating with them in their investigations.

We take protection of your personal information extremely seriously and want to ensure you have information that may assist you in continuing to protect your personal information.

## What are we doing to protect your information?

To help protect your identity, we have retained Experian, a specialist in identity theft protection, and are offering you **two (2) years of identity protection services, including credit monitoring, free of charge to you**, through a membership in Experian's® IdentityWorks<sup>SM</sup>. This product provides you with identity detection and resolution of identity theft and will be available to you for a period of 24 months. To activate your membership and start monitoring your personal information please follow the steps below:

- Ensure that you **enroll by: February 28, 2021** (Your code will not work after this date.)
- **Visit** the Experian IdentityWorks 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 online, please contact Experian's customer care team at 833.796.8638 by **February 28, 2021**. Be prepared to provide engagement number **DB23806** 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 IdentityWorks.

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

- **Experian credit report at signup:** See what information is associated with your credit file. Daily credit reports are available for online members only.<sup>1</sup>
- **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 IdentityWorks ExtendCARE™:** You receive the same high-level of Identity Restoration support even after your Experian IdentityWorks membership has expired.
- **Up to \$1 Million Identity Theft Insurance<sup>2</sup>:** Provides retroactive coverage for certain costs and unauthorized electronic fund transfers.

---

<sup>1</sup> Offline members will be eligible to call for additional reports quarterly after enrolling.

<sup>2</sup> 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.

If you believe there was fraudulent use of your information and would like to discuss how you may be able to resolve those issues, please reach out to an Experian agent at 833.796.8638. 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 two years 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](http://www.ExperianIDWorks.com/restoration). You will also find self-help tips and information about identity protection at this site.

**What else you can do.**

We also recommend that you consider monitoring your accounts and free credit reports for suspicious activity, consistent with best practices.

**Other important information.**

You may contact one of the three major credit bureaus listed below and request that a fraud alert be placed on your credit report or request a copy of your credit report:

Experian Security Freeze 1-888-397-3742 <a href="https://www.experian.com/freeze/center.html">https://www.experian.com/freeze/center.html</a>	Equifax Security Freeze 1-800-685-1111 <a href="https://www.freeze.equifax.com">https://www.freeze.equifax.com</a>	TransUnion LLC 1-888-909-8872 <a href="http://www.transunion.com/personal-credit/credit-disputes/credit-freezes.page">www.transunion.com/personal-credit/credit-disputes/credit-freezes.page</a>
---	--	--

In addition, you may contact the Federal Trade Commission (“FTC”) or law enforcement to report incidents of identity theft or obtain information about fraud alerts, security freezes, and preventing identity theft:

Federal Trade Commission Consumer Response Center  
600 Pennsylvania Avenue, NW Washington, DC 20580  
(877) IDTHEFT (438-4338)  
<http://www.ftc.gov/idtheft/>

\* \* \*

We sincerely apologize for any inconvenience this incident may cause you and assure you that we have taken the necessary steps to minimize risk to you and ensure your information is kept as safe as possible. Should you require any further information or have any questions, please feel free to contact at any time your local HR team, the Group Data Privacy Officer (DPO), Daniele Di Maiuta, or your local IT team.

Sincerely,



Ugo Fiorenzo  
Managing Director



## **ADDITIONAL DETAILS FOR RESIDENTS OF MARYLAND, NORTH CAROLINA, OREGON, AND RHODE ISLAND:**

For those of you who reside in Maryland, North Carolina, Oregon, or Rhode Island, you may report incidents of identity theft to, or obtain information about fraud alerts, security freezes, and preventing identity theft from your respective state attorney general:

### **Office of the Maryland Attorney General Identity Theft Unit**

200 St. Paul Place, 25<sup>th</sup> Floor

Baltimore, MD 21202

Tel: 410-576-6491

Email: [idtheft@oag.state.md.us](mailto:idtheft@oag.state.md.us)

### **Office of the Oregon Attorney General Office of Consumer Protection**

Tel: 1-877-877-9392

Email: [help@oregonconsumer.gov](mailto:help@oregonconsumer.gov)

### **Office of the North Carolina Attorney General Consumer Protection Division**

114 West Edenton Street

Raleigh, NC 27603

Tel: 1-877-5-NO-SCAM or 919-716-6000

### **Office of the Rhode Island Attorney General Consumer Protection Unit**

150 South Main Street

Providence, RI 02903

Tel: 401-274-4400

Email: [consumers@riag.ri.gov](mailto:consumers@riag.ri.gov)

## **ADDITIONAL DETAILS FOR MASSACHUSETTS RESIDENTS:**

For Massachusetts residents, please find below additional information on how to request a free credit freeze on your credit report with the three (3) major credit reporting agencies (Equifax, Experian, and TransUnionCorp). When requesting a credit freeze, you should be prepared to provide some or all of the following information, depending on whether you request the freeze online, by phone, or by mail:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. Addresses where you have lived over the prior five years
5. Proof of current address, such as a current utility bill, telephone bill, rental agreement, or deed
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. Social Security card, pay stub, or W2
8. If you are a victim of identity theft, a copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft.

You may also request a credit freeze for a minor child or a dependent, even if they do not have a credit report. Information on how to do so is available from the above credit reporting agencies. For additional information, please see the Massachusetts Attorney General's <https://mass.gov/sevice-details/freeze-your-credit>.