CAMPARI GROUP

Campari Group Press Release

Malware attack- Data security update

Milan, December 4th, 2020-Campari Group announced that it has been the victim of a targeted ransomware attack following unauthorized access to its network. After technical investigations, Campari Group is now able to report that some personal and business data has been compromised.

Campari Group offers its sincerest apologies for any complications and concerns that this may bring to its potentially impacted employees, customers, suppliers, business partners, as well as to its many stakeholders.
As there is an ongoing investigation in place, it is possible that new facts may come to light going forward.

Below is a general summary of what has been confirmed at the date of this public statement.

A - Information verified to have been compromised

(i) Employees Active Directory – containing n. 4,736 employees, n. 1,443 former employees and n. 1,088 consultants' personal information (name, surname, e-mail address, mobile phone numbers (employees and former employees only), job title, reporting lines, personal Campari Network ID number) all as registered in such directory for business purposes;

(ii) some contracts, IDs and other personal data, accounting data mainly relating to our US subsidiary (Campari America LLC).

B - Potentially Compromised Personal and Business Data (exfiltrated, encrypted and/or accessed)

(i) corporate and/or personal data (mainly contact details including name, surname, address, e-mail, telephone numbers), business information and payment details of Campari Group customers, suppliers and other business partners – the estimated global number of active customers is 10,000 and of active suppliers is 8,500. There may be also contact details of journalists (name, surname, address, e-mail, telephone numbers in the range of 1,000) and curricula vitae of candidates;

(ii) personal data of employees and former employees including name, surname, personal address, e-mail address, job description, telephone numbers, payment details, compensation, performance evaluations, IDs, content of documents / files stored by such employees in network folders, content of outlook inbox – maximum global number is estimated in 6,000;

(iii) confidential business documents and information (such as contracts, analysis, presentations, accounting) - 2TB of exfiltrated data which content is not yet possible to determine as a result of the consequences of the attack.

C - Other information
Campari Group does not systematically hold personal credit card or other payments information or credential or any other kind of personal password.
There is no indication that Campari Group websites have been accessed.
All business passwords to access Campari Group network were encrypted.

D- Potential consequences of the breach – Advice for individuals
Potential consequences of the breach resulting from loss of confidentiality are misuse of contact details, phishing attempts, unwanted contacts, fraud attempts (especially if personal IDs and passwords were stored in Campari Group shared folders), alteration of payment details and consequent payment errors by Campari Group or to Campari Group (e.g. change of IBAN codes).
Campari Group has kept informed its employees and stakeholders and has offered identity theft support where customary.
Some simple security advice:

- do not respond to suspicious requests or messages (especially in relation to payments – such as change of payment details, or request for password or bank account information);
- do not open any link unless you are absolutely sure it comes from a reliable source.

E – Defensive Measures and Investigation
Campari Group is implementing all actions deemed appropriate at this stage to further protect its IT estate and, therefore, personal and business data stored therein (checking all servers and end users devices, further raising the IT estate security levels by hardening measures, Multi Factor Authentication Procedures to prevent unauthorized access, acceleration of transfer of IT estate to Cloud).
The investigation into information that has potentially been taken or compromised is continuing and we also are communicating regularly with the data privacy authorities and fully collaborating with police forces.

F – Contact for Information and Support
For individuals who wish to inquire about personal information that has potentially been compromised or need support please contact Daniele di Maiuta, our Group Data Protection Officer at gpdp.office@campari.com.

***

For further information:

Investor Relations

Chiara Garavini Tel. +39 335 5761337 E-mail: chiara.garavini@campari.com

Corporate Communications

Enrico Bocedi Tel. +39 346 5005458 E-mail: enrico.bocedi@campari.com