

- [Risk Management](#)
- [Compliance](#)
- [Privacy](#)
- [Supply Chain](#)
- ▼ [Security Architecture](#)
  - [Cloud Security](#)
  - [Identity & Access](#)
  - [Data Protection](#)
  - [Network Security](#)
  - [Application Security](#)
- ▼ [Security Strategy](#)
  - [Risk Management](#)
  - [Security Architecture](#)
  - [Disaster Recovery](#)
  - [Training & Certification](#)
  - [Incident Response](#)
- [ICS/OT](#)
- [IoT Security](#)

[Home](#) > [Cybercrime](#)



## Recruiting Firm Apparently Pays Ransom After Being Targeted by Hackers

By [Jonut Arghire](#) on September 02, 2021

Share

发推

Recommend 0



Administrative staffing agency Career Group, Inc. this week started sending notification letters to customers who were affected by a data breach that occurred in late June.

Headquartered in Los Angeles, the staffing and recruiting company provides both full-time and temporary placement services, in direct hire and freelance roles at organizations across all sectors.

The data breach, the company says, occurred between June 28 and July 7. The company detected “potential unauthorized access to its network” on July 2 and took the necessary steps to contain it.

The company also informed law enforcement of the incident and started an investigation that revealed unauthorized access to customer data.

“Our investigation determined that the unauthorized party potentially removed certain files and folders from portions of our network between June 28, 2021 and July 7, 2021,” the company says in the notification letter sent to affected individuals.

A redacted copy of the [notification letter](#) that was submitted to the Maine Attorney General’s Office shows that Career Group was able to identify the type of compromised information in early August, but does not reveal the exact type of data that was stolen.

However, the company did share with the Maine Attorney General’s Office the fact that names and other personally identifiable information, such as Social Security Numbers, were impacted. A total of 49,476 individuals were affected by the incident.

Career Group did not share details on the type of cyberattack it fell victim to, but it appears that ransomware might have been used and that the company likely paid a ransom to the attackers.

“We received assurances from the unauthorized party that the data removed from our environment was permanently deleted and not further disseminated,” the company said in the notification letter.

The company also says it took the necessary steps to ensure that it would better protect the data entrusted to it.

**Related:** [Nokia-Owned SAC Wireless Discloses Data Breach](#)

**Related:** [T-Mobile Confirms Data Breach Impacts Millions of Customers](#)

**Related:** [University of San Diego Health Says Personal Information Stolen in Data Breach](#)

Share

发推

Recommend 0



Ionut Arghire is an international correspondent for SecurityWeek.

Previous Columns by Ionut Arghire:

[Facebook Pays Out \\$40,000 for Account Takeover Exploit Chain](#)

[BrakTooth: New Bluetooth Vulnerabilities Could Affect Millions of Devices](#)

[Recruiting Firm Apparently Pays Ransom After Being Targeted by Hackers](#)

[FTC Bans SpyFone From Surveillance Business for Selling Stalkerware](#)

[Cisco Patches Critical Enterprise NFVIS Vulnerability for Which PoC Exploit Is Available](#)

[Virtual Event Series - Security Summit Online Events by SecurityWeek](#)

sponsored links

[2021 Singapore/APAC ICS Cyber Security Conference \[Virtual: June 22-24\]](#)

[2021 ICS Cyber Security Conference | USA \[Hybrid: Oct. 25-28\]](#)

[2021 CISO Forum: September 21-22 - A Virtual Event](#)

**Tags:**

[NEWS & INDUSTRY](#)

[Cybercrime](#)

Search

## Get the Daily Briefing

# BRIEFING

Business Email Address

Subscribe

