THE
NATIONAL LAW REVIEW

High-end Job Recruitment Site Exposes at least 13.7 million Users with Unprotected Server

jackson lewis.
Article By
Catherine R. Tucciarello
Jackson Lewis P.C.
Workplace Privacy Blog

- Communications, Media & Internet
- All Federal

Friday, May 10, 2019

A security lapse has exposed the data of at least 13.7 million user records of the high-end job recruitment site, Ladders. The company left a cloud-hosted search database exposed without a password. Ladders took the database offline less than an hour after the news website TechCrunch alerted the company after learning about the potential breach from a security researcher, Sanyam Jain.

Each record included names, email addresses, addresses, phone numbers, their employment histories and even exact geolocation based off of individual IP addresses. The user profiles also contain information about the industry they're seeking a job in and their current compensation in U.S. dollars.

A data leak of information such as social security numbers, phone numbers, credit history or other more sensitive information "would be a gold mine for cyber criminals who would have everything they need to steal identities, file false tax returns, get loans or credit cards," according to Bob Diachenko, online publisher for TechCrunch. In contrast, most of the information affected in the Ladders' data leak, while personal and sensitive, does not amount to personally identifiable information which could be used for identity theft.

Additionally, an important distinction should be made between data leaks and data breaches: data leaks are usually incidents in which data was unintentionally made public as the result of an accident or misapplication of a system's features, however the data has not actively been accessed or exfiltrated; data breaches are incidents

involving active threats which compromise a database.

The recent abundance of high-profile data leaks as of late emphasize the need for organizations today to be proactive rather than reactive. The legal landscape of the data privacy world also reflects this approach. For example, the General Data Protection Regulation (GDPR) enforces a “Privacy by Design” system, which requires any action a company undertakes that involves processing personal data must be done with data protection and privacy in mind at every step. Similarly the much anticipated California Consumer Privacy Act, requires a business to “implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information”, and similar frameworks are mandates in other states such as Colorado, Massachusetts and Oregon.

This wave of data leaks/breaches, combined with the growing public awareness of data privacy right and concerns, and legislative activity in the area, makes the development of a meaningful data protection program an essential component of business operations.

Source URL: https://www.natlawreview.com/article/high-end-job-recruitment-site-exposes-least-137-million-users-unprotected-server