ICE
TRUSTED IT PARTNER

ICE'S DATA BREACH CASE STUDIES

Ticketmaster

Live Nation, the owner of Ticketmaster, has verified "unauthorized activity" on its database following claims by hackers that they have obtained the personal information of 560 million customers.

ShinyHunters, the group taking credit, has stated that the compromised data comprises names, addresses, phone numbers, and partial credit card information of Ticketmaster users globally.

The hacking group is said to be requesting a $500,000 (£400,000) ransom to halt the sale of the data to third parties.

Live Nation reported to the US Securities and Exchange Commission that a cybercriminal attempted to sell purported user data on the dark web on May 27. Live Nation is actively investigating this incident, but the exact number of customers affected remains undisclosed.

Hackers initially disclosed the Ticketmaster breach by advertising the compromised data on Wednesday evening. Despite this, Ticketmaster chose not to confirm the breach to the public or press, informing shareholders only on Friday.

The Australian government is collaborating with Ticketmaster to address the breach, with the FBI also offering assistance, as confirmed by a US Embassy spokesperson in Canberra. The FBI, however, declined to provide any comments on the matter.

Live Nation stated in its filing that it is taking steps to minimize risks for its customers and is informing users about the unauthorized access to their personal information.

"As of the date of this filing, the incident has not had, and we do not believe it is reasonably likely to have, a material impact on our overall business operations or on our financial condition or results of operations. We continue to evaluate the risks and our remediation efforts are ongoing", it added.

The American website Ticketmaster stands as one of the world's largest online ticket sales platforms. This breach marks a historic scale in terms of global impact, yet the extent of the compromised data's sensitivity remains uncertain in the hands of cybercriminals.

Researchers caution that this incident is part of a broader, ongoing breach involving Snowflake, a cloud service provider utilized by numerous major corporations for cloud-based data storage. Snowflake has alerted its clients to a surge in cyber threats targeting select accounts.

Recently, Santander confirmed that data from roughly 30 million customers was illicitly obtained by the same hacker group involved in the Ticketmaster breach. Notably, Santander reassured customers that UK client data remained unaffected by the breach.

WHAT DO WE KNOW ABOUT SHINYHUNTERS?

The hacking group known as ShinyHunters has gained notoriety for their data breaches targeting numerous companies in 2020 and 2021. Their victims included major platforms such as Tokopedia, Unacademy, Wattpad, AT&T Wireless, and Microsoft. Recently, a key member of ShinyHunters, a French national named Sebastien Raoult, was apprehended and sentenced to three years in a Seattle court. The U.S. Justice Department revealed that from April 2020 to July 2021, ShinyHunters profited by selling hacked data from over 60 companies. Their illicit activities resulted in the theft of hundreds of millions of customer records, inflicting estimated losses exceeding $6 million on the affected companies.

It's thought these hacks are all linked and many others could become public.
An advertisement containing data samples reportedly obtained from a breach has surfaced on BreachForums, a recently relaunched dark web hacking forum where cybercriminals trade stolen data to facilitate illicit activities.

ShinyHunters, known for a series of high-profile data breaches that inflicted significant financial losses on affected companies, notably sold a database with information from 70 million AT&T customers in 2021. Additionally, nearly 200,000 Pizza Hut customers in Australia fell victim to a data breach in September of the same year.

The FBI dismantled the domain in March 2023, apprehending its administrator Conor Brian Fitzpatrick. However, reports from tech media indicate its resurgence.

Hacking forums are notorious for exaggerating the scale of their activities to attract attention. While they often debut substantial stolen databases, they can also propagate misleading information. Some individuals who claim to possess vast data sets have merely recycled previously leaked information.

If ShinyHunters' claims about the data breach's magnitude hold true, it could rank as one of the most significant breaches in history based on the volume and sensitivity of the data compromised.

Ticketmaster's history of security incidents is well-documented. In 2020, the company acknowledged hacking a competitor and agreed to a $10 million settlement. Later that year, it allegedly fell victim to a cyber attack, disrupting ticket sales for Taylor Swift's Era's tour.

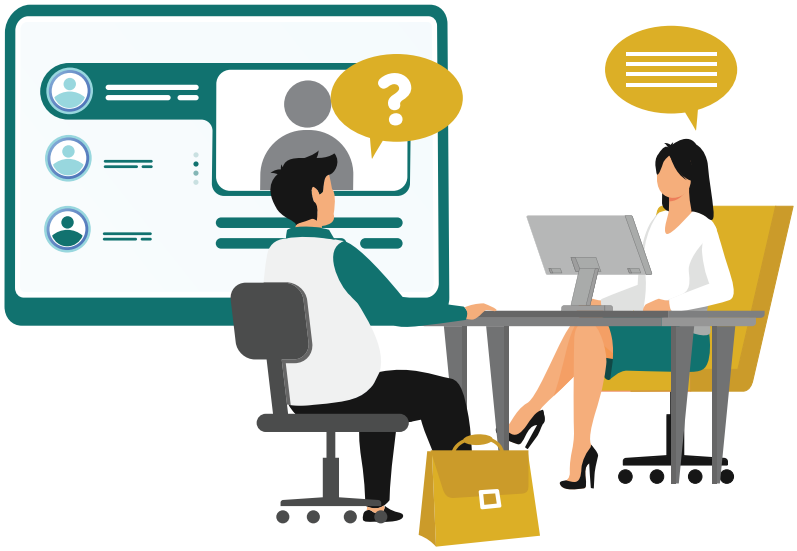
Recently, US regulators filed a lawsuit against Live Nation, accusing the entertainment powerhouse of anti-competitive practices that stifled competition, resulting in inflated ticket prices and subpar customer service in the live music industry.

WHAT TO DO IF YOU ARE WORRIED YOU HAVE BEEN AFFECTED

Following the breach at Ticketmaster, users can safeguard themselves by monitoring accounts, credit cards, and using strong, unique passwords to prevent phishing attempts. While Live Nation and Ticketmaster have not yet addressed the breach publicly, Ticketmaster previously shared advice on securing information and tickets in an April blog post. They advised users to always access contact details from Ticketmaster's official site and to be wary of fake customer service numbers that may pop up in search results.

Experts advise staying calm and vigilant if you suspect you're a target. Beware of fraudulent emails, texts, and calls; hackers may leverage stolen details to deceive victims into divulging more. Scammers might exploit the anxiety from a breach to coerce you into sharing information.

- **Exercise caution with the following:**
  - Official-sounding messages prompting actions like resetting passwords, receiving compensation, scanning devices, or claiming missed deliveries.
  - Emails packed with technical jargon meant to appear more credible.
  - Urgent requests for immediate action within a restricted time frame.



Protecting your business from becoming the next news headline!

ICE Consulting has served as a Managed Cybersecurity Provider for more than 26 years.
Our expertise lies in enhancing businesses' security stance and delivering a range of cybersecurity services including:

1. Security Operation as a Service (24x7 real time cyber threat monitoring and response services)
2. Incident Response Planning
3. Security & Network Vulnerability Scans
4. Penetration testing
5. Cybersecurity Training

As data breaches reach record levels and show no signs of slowing down, it's crucial for every business to regularly evaluate its security stance for weaknesses. We offer this service at no charge to businesses. Reach out today to discover more about this process.

ICE Consulting, Inc
Managed Cybersecurity Provider

ICE
TRUSTED IT PARTNER

888-423-4801
info@iceconsulting.com
www.iceconsulting.com