The Computer & Internet Lawyer

Volume 39 ▲ Number 4 ▲ April 2022

Ronald L. Johnston, Arnold & Porter, Editor-in-Chief

Data Breach at Twitch Exposes Danger for All Businesses

By Tam D. Vu

Recent months have been busy for privacy professionals. From public education institutions and hospitals, to online broadcast and streaming platforms, there has been a surge of data breaches.

One of the more high profile data breach incidents occurred last October[1] when a trove of business-related digital information from a video game live-streaming platform was posted online for all the world to see. What can this incident teach businesses about the need to ensure that their compliance efforts are up to date?

Twitch Suffers Major Data Breach

Twitch – an online interactive streaming platform focusing on eSports and video games live streaming – suffered a data breach that was revealed to the public on October 6, 2021. Among the information hackers obtained and leaked were Twitch's source-code, internal security protocols, and earning records of many streamers. While no usernames or passwords were published, there is no guarantee that they were not compromised; only time will tell whether the breach also implicates such data.

Twitch became a huge target due to its status as a revolutionary interactive entertainment/streaming platform. It sets itself apart from traditional TV and other online streaming platforms by allowing the audience to interact directly with the host/streamer. The platform handles an estimated 9.2 million monthly users and provides lucrative earning opportunities for streamers and brands. With the sheer number of users' data, lucrative earnings, and industry notoriety, it is easy to see why Twitch was an attractive target.

However, businesses must remember that they do not have to be an edgy online-focused business to suffer a data breach. As long as they have customers or employees' data, then they are subject to the same risk. A series of compromised Social Security numbers or banking information, whether of customers or employees, can still be damaging when it falls into the wrong hands.

Tam D. Vu, an attorney in the Irvine, California, office of Fisher & Phillips LLP, represents employers in a variety of employment cases, including claims for harassment, discrimination, retaliation, wrongful termination and wage and hour disputes. He also counsels employers on a variety of workplace issues and assists with the development of employee handbooks, policies, and procedures. He may be reached at *tvu@fisherphillips.com*.

Furthermore, businesses within the European Union ("EU") jurisdictions or states with strict privacy regulations (such as California) may also face hefty administrative fines and costly civil litigation from such data breaches.

With the continued popularity of telework presenting greater security risks, now is a good time for businesses to re-examine their compliance obligations and data security protocols.

Understanding How Data Breaches May Occur

In order to prevent data breaches, businesses must understand ways that a breach may occur. Even if a business does not directly deal with retail consumers or is not an internet-based platform, the implications are all the same. Although not an exhaustive list, businesses should familiarize their organizations with and address the following tactics:

- *Social Engineering Attacks*: A person may call, message, or email an employee and poses as a customer, employee, or an executive to manipulate the employee to reveal confidential information. For example, a caller may pose as an associate of a vendor and ask for the vendor's bank account number to confirm an order.

- *Phishing and Spear Phishing*: A cybercriminal may send an email claiming to be from a reputable entity (i.e., an established third-party vendor) or tailor an authentic-seeming message to a specific recipient, asking for confidential information (i.e., log-ins, bank account number, etc.).

- *Lack of Virtual Private Network ("VPN")*: For businesses with employees working remotely, using an unsecured network at a public place, working on a shared device, or leaving their device unsecured in a public space present risks of data breach and unauthorized access. ImplementingVPN and multi-factor authentication are some ways to establish a secured connection and prevent unauthorized access.

Data Privacy Regulations Implications

While a remote workforce presents more risks for a data breach, the privacy implications for failure to protect confidential and personal information are all the same – hefty fines and penalties – even if a business is non-internet-based or non-tech-focused. Businesses have a duty to protect employees and customers' confidential information such as social security numbers, drivers' license numbers, medical information, and financial account information, among other data. Now is the time for businesses to re-evaluate their compliance obligations and prepare ahead. Even if a business is not retail-centric, its obligations to employees' data alone can land an organization in hot water should a data breach occur.

For example, the General Data Protection Regulation ("GDRP") applies if a business processes the personal data of and monitor EU-based employees, even if the business was incorporated or operates mainly outside the EU. Personal data is broadly defined as "any information relating to an identified or identifiable natural person." Such information may include an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Examples of common identifiable personal information include address, date of birth, phone number, photos, email address, salary information, health records, and severance data. Other "special categories" of data such as racial or ethnic origin, trade union membership, and biometric and health data (i.e., COVID-19 related information) may require enhanced protections.

On top of that, state-specific privacy regulations may impose additional (and complicated) compliance obligations for a business. For example, the California Consumer Privacy Protection Act ("CCPA") applies to businesses operating in California that collect the personal information of one or more California resident and that satisfy one of the following thresholds:

- Generates annual revenue of $25 million or more;

- Collects the personal information of 50,000 or more California residents; or

- Derives 50 percent or more of its annual revenue from the selling of personal information.

Even if a business does not meet any of the above criteria, but it is affiliated with or shares common branding with another business (such as a parent company) that meets the above, then the CCPA also derivatively applies to the business.

As can be seen, both the GDRP and state-specific privacy regulations can be technical and complicated to comply with and follow. For this reason, businesses should begin their auditing and compliance processes early, and re-evaluate them on a regular basis, to allow room for adjustments down the road.

So There's A Breach – Now What?

In data security, prevention is an important duty, but not the only duty. The company's response in cases of breach is just as important. Although not an exhaustive list, at the minimum, businesses should consider the following steps when dealing with data breach.

- *Contact Counsel and Cyber-Insurance Carrier*: Leave it to the professionals. Besides IT professionals, legal counsel can help analyze and comply with applicable data breach notification and other reporting obligations resulting from the breach. Furthermore, mitigating a data breach can be costly. As such, if a business has cyber-insurance, it should notify its carrier in a timely fashion to maximize the likelihood of coverage for costs associated with remediating and responding to the breach.

- *Identify the Type of Information Affected and Initiate the Incident Response Plan*: Mobilize the company's breach response team, and if the company has an incident response plan, be sure to implement it promptly. The company protocols should include procedures to enable prompt investigation and remediation of the breach. Furthermore, the company must determine the nature of the data at issue and how it was impacted by the breach to assess what legal requirements or regulations may apply. It also may want to consider whether to notify law enforcement.

- *Stop the Breach and Take It Offline*: It is already bad, do not let it get worse. Securing the network and changing network access authorization can be part of the business' response protocols should a breach occur. Whether it is to secure a physical area (i.e., where a computer was left unattended), to halt network access until further notice, or to take documents/equipment offline, a business should put in place response protocols that are tailored to its operations.

- *Contact the Service Provider*: If a service provider is responsible for the breach (i.e., web security, website builder, third-party payment processor), review any applicable agreements to determine the obligations of the parties and, as appropriate, ensure that the provider is investigating, remedying, and responding to the breach. Companies should also reassess their access privileges and verify that vulnerabilities were indeed remedied by the provider.

Conclusion

Unfortunately, the key question surrounding a data breach at a business is not a question of "if," but "when." As technology continues to evolve, there are an increasing number of ways for data breaches to occur. The bottom line is that regardless of the industry, businesses must always be prepared to adjust and revise their data security and privacy practices to stay ahead of legal obligations and defend against increasingly sophisticated cyberattacks.

Note

1. *https://www.videogameschronicle.com/news/the-entirety-of-twitch-has-reportedly-been-leaked/*.