Case Study for Jollibee Group Data Breach (June - July 2024)

Group Members:

Arabe, Mark Benjie
Areglo, Dion
Capiña, Christine Mae
Convicto, Hazel Ann
Deonila, Florenz

Case Overview:

A recent report on Jollibee Foods Corporation (JFC), from the Philippines, highlights a significant cyber security breach with Jollibee Foods Corporation being the largest fast food chain in the Philippines. JFC operates a number of fast food brands in the Philippines, and the breach involved their "data lake" which is a centralized repository where data from all of their brands is stored.

- **Date Reported:** June 22, 2024
- **Affected Brands**: Jollibee, Mang Inasal, Red Ribbon, Chowking, Greenwich, Burger King, Yoshinoya, and Panda Express.
- **Victims:** Approximately 11 million data subjects.

Threat & Impact Analysis:

The Threat

- **Threat**: The breach was allegedly carried out by a hacker going by the handle "Sp1d3r". Reports from cybersecurity monitoring groups (like Deep Web Konek) indicated the actor claimed to be

selling the stolen data on a cybercrime forum for approximately $40,000.

- **Attack Vector:** Unauthorized access to the company's central Data Lake. Unlike a typical website defacement, this attack targeted the backend infrastructure where vast amounts of aggregated data are stored for analytics and operations.

- **Motive:** Financial Gain. The hacker explicitly listed the database for sale, indicating a cybercriminal intent rather than hacktivism or state-sponsored espionage.

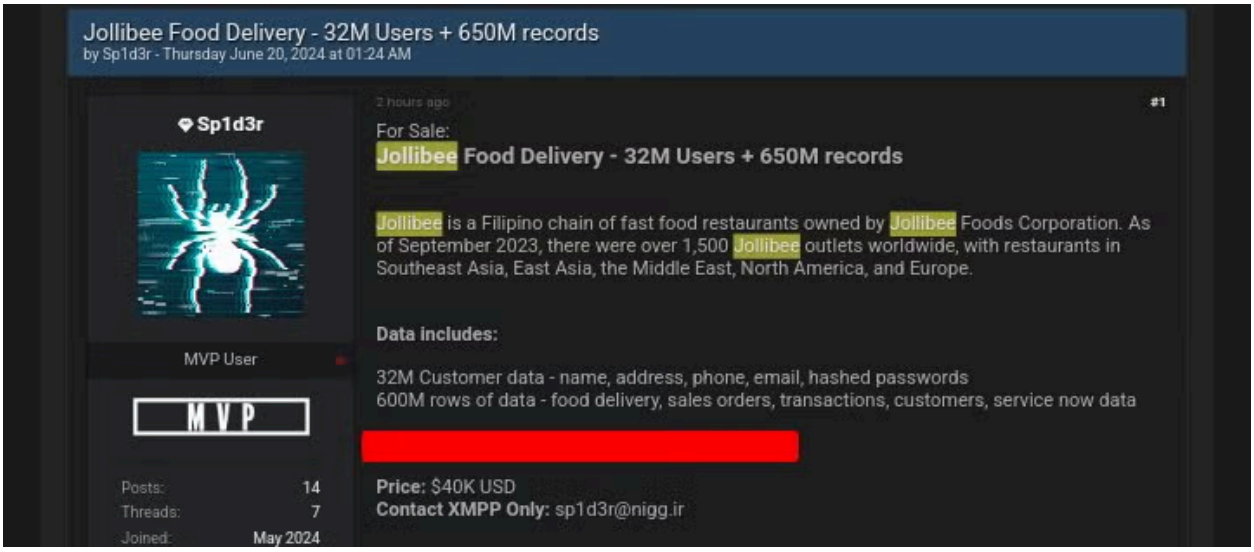
The Impact

- **Data Exposure (Privacy Impact):** The compromise was severe, involving Sensitive Personal Information (SPI).

    - **Confirmed Leaks:** Dates of birth and Senior Citizen ID numbers.
    - **Alleged Leaks:** The hacker claimed to hold 32 million records, including names, addresses, phone numbers, email addresses, and hashed passwords, as well as delivery transaction logs.

- **Reputational Damage:** With 11 million customers who have been loyal customers over many years across multiple brands, public trust has been damaged significantly by this breach. The impact of the exposed Senior IDs has caused an even greater level of concern since this demographic is especially vulnerable to fraud.

- **Regulatory Consequences:** The company has been put under scrutiny by the National Privacy Commission (NPC), and it has required JFC to provide mandated compliance reports and to conduct investigations or face the threat of sanctions.



CIA Triad Mapping

Component	Status	Analysis
Confidentiality	**FAILED**	The core of this breach was a failure of confidentiality. Unauthorized parties gained access to private customer data (Senior IDs, Birthdays) that was supposed to be restricted. The data was not only viewed but exfiltrated and offered for public sale.
Integrity	**AT RISK**	While there were no widespread reports of the hackers *altering* the data (e.g., changing menu prices or customer balances), the unauthorized access proves that the system's integrity controls were bypassed. If they could read the data, they might have had the ability to modify it, rendering the dataset unreliable.
Availability	**MAINTAINED**	JFC has stated that their e-commerce platforms and delivery websites remained operational during the incident, which is the only surprise considering ransomware attacks lock files and stop business operations. Rather, this was a “sleeper” exfiltration operation where data is stolen without disrupting business activities.

Reference:

https://www.sangfor.com/blog/cybersecurity/jollibee-data-breach-philippines-affected-11-million-customers?fbclid=IwY2xjawPUU1JleHRuA2FlbQIxMQBzcnRjBmFwcF9pZAEwAAEej68mfdtEld9j1SfVhNjJpLyQfoiHuClyaV6_kRFA-tD1LpDtLVvlaUCqomk_aem_YFTP4rbtkoi2HNwebMp2Jg