Republic of the Philippines
NATIONAL PRIVACY COMMISSION

LEGAL AND ENFORCEMENT OFFICE

RE: JOLLIBEE FOODS CORPORATION CID BN No. 17-043

x----------x

ORDER

THIS ORDER is being issued under the power of this Commission to compel any entity to abide by its orders on a matter of data privacy, in relation to a data breach report submitted by Jollibee Foods Corporation (Jollibee or JFC) last 12 December 2017.

In the Breach Notification, JFC Group DPO J'Mabelard M. Gustilo informed the Commission that on 8 December 2017, persons unknown to the JFC Group appeared to have been able to gain access to the customer database of the delivery website for Jollibee.

In the course of the investigation, the Complaints and Investigation Division (CID) identified the breach to be a result of a proof-of-concept initiated by a marketing PR team representative of Jollibee, who made representations to a domestic cybersecurity firm.

On 21 December 2017, the CID invited said firm to a meeting wherein one of its members narrated that he, while conducting vulnerability testing for another client, noticed a security gap in the jollibeedelivery.com website. While their group was able to exploit the vulnerabilities, their firm insisted that they did not scrape or exfiltrate any data, because they merely demonstrated their ability to access the data in Jollibee's database if they so desired.

Shortly after the breach, Gustilo decided to handle corrective measures internally and through its third party IT security providers. Gustilo nevertheless clarified that the JFC Group treated the cybersecurity firm responsible for the breach as an uncontracted entity or stranger who had no authority to infiltrate their IT infrastructure.

In a later meeting, Gustilo admitted to the CID that the database protection was not up to date, and some data, including personal information, were unencrypted. Although CID noted some improvements in protecting data privacy on the part of the JFC Group after the suspected breach, more consistent and effective efforts are needed to protect the data. As DPO, Gustilo acknowledged difficulty in effecting the needed data protection and security

measures for various reasons, such as budgetary constraints, low prioritization or outright disinterest within the organization.

Following these meetings, on 20 February 2018, the CID began conducting its own vulnerability assessment of Jollibee's website and found that it remains vulnerable to unauthorized access. Such vulnerabilities may allow malefactors with little to moderate technical knowledge and skill to access personal information of Jollibee patrons through its website.

Considering that smaller systems with more robust security measures have been exposed, there is a very high risk that approximately 18 million people currently on the database will be exposed to harm.

Considering, further, that these vulnerabilities were made known to Jollibee for quite some time, and that their online properties remain vulnerable, urgent action is necessary to protect the personal data of those using the JFC Group delivery service.

WHEREFORE, PREMISES CONSIDERED, this Commission, through its Legal and Enforcement Office, hereby **ORDERS** Jollibee Foods Corporation to:

1. **SUSPEND** *forthwith* the operations of jollibeedelivery.com and all other data processing open to the public through the internet and restrict external access to their networks, for an indefinite time until the site's identified vulnerabilities are addressed, as validated by a duly certified penetration testing methodology.

2. **SUBMIT** a security plan to be implemented in rehabilitating said system to ensure the integrity and retention of the database and its content within ten (10) calendar days upon receipt hereof.

3. **EMPLOY** Privacy by Design in the reengineering of JFC Group data infrastructure.

4. **CONDUCT** a new Privacy Impact Assessment, considering the vulnerabilities exposed in the Commission's penetration tests and in subsequent penetration tests ordered in the next preceding section.

5. **FILE** a monthly Progress Report on this matter until the issues raised in this Order are resolved.

Given in the Meeting dated 4 May 2018 with Jollibee Foods Corporation at this Commission's offices at the Philippine International Convention Center.

SO ORDERED.

4 May 2018, Pasay City, Metro Manila.

For the Commission:

(Sgd.) FRANCIS EUSTON R. ACERO
Division Chief
Complaints and Investigations Division

Approved by:

(Sgd.) GILBERT V. SANTOS
OIC-Director IV
Legal and Enforcement Office