Republic of the Philippines
NATIONAL PRIVACY COMMISSION

In Re: Facebook Forced Logout **CID Case No. 18-J-162**

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

ORDER

THIS ORDER is being issued under the power of this Commission to compel or petition any entity to abide by its order or take action on a matter affecting data privacy,[1] in relation to an ongoing investigation on Facebook Inc. ("Facebook") concerning the exploitation of the "View As" feature to extract a user's access tokens without their consent.

On 25 September 2018, Facebook discovered that there was an unexpected increase in traffic on the use of the "View As" feature. Based on its declaration, it is believed that this was introduced into Facebook's code on 12 July 2017. However, Facebook believes that the attack may have only commenced on 14 September 2018, the date when the spike in traffic commenced.

Three (3) days after the vulnerability was discovered by Facebook, 28 September 2018, the vulnerability was then allegedly fixed and Facebook notified all its users via an in-app update message supposedly on the same date.[2] The Commission was then informed through e-mail at 12:40 a.m. of the next succeeding day, 29 September 2018.

On 2 October, in a conference call with Facebook officials and this Commission, Facebook, through counsel, informed this Commission that individual notification was not deemed ripe as the conditions for individual notification under Circular No. 16-03 were not yet met. At the same meeting, Facebook expressed a commitment to abide by Philippine data privacy laws.

On 13 October, Facebook informed the National Privacy Commission that of the 30 million people with stolen access tokens, they now believe that a total of 755,973 Philippine-based Facebook user accounts may have been compromised that forced Facebook to log out users from their accounts last September 28.

---

[1] Sec. 7(d) Republic Act No. 10173, Data Privacy Act of 2012.

[2] Facebook Letter, Subject: Incident Update from Facebook, Inc., 13 October 2018

Facebook categorizes the affected users into three distinct groups, or "buckets" based on the personal information the perpetrator may have accessed.

The first bucket involves an estimated 387,322 Philippine-based user accounts whose basic profile information may have been compromised. Basic profile information consists of a user's registered full name, email address, and phone number (if one was so associated with the account).

The second bucket affects around 361,227 Philippine-based user accounts. In addition to the basic profile information potentially obtained as with the first group of users, the perpetrator may have also obtained:

a. Username,
b. First name used on the profile,
c. Last name used on the profile,
d. Name (nickname as set by the user on the profile (if any)),
e. Email address (primary email address associated with the account),
f. Phone (confirmed mobile phone numbers associated with account),
g. Gender (as set by the user on the profile),
h. Locale (language as picked by the user),
i. Relationship status (as set by the user on the profile),
j. Religion (as described by the user on the profile),
k. Hometown (as set by the user on the profile),
l. Location (current city, as set by the user on the profile),
m. Birthday (as set by the user on the profile),
n. Devices (that are used by the user to access Facebook - fields include 'os' (e.g., iOS) and hardware (e.g., iPhone),
o. Educational background (as set by the user on the profile),
p. Work history (as set by the user on the profile),
q. Website (list of URLs entered by the user into the website field on the profile),
r. Verified status information (this is a flag for whether Facebook has a strong indication that the user is who they say they are),
s. List of most recent places where the user has checked in (these locations are determined by the places named in the posts, such as a landmark or restaurant, not location data from a device),
t. Recent search queries on Facebook, and
u. Up to the top 500 accounts that the user follows.

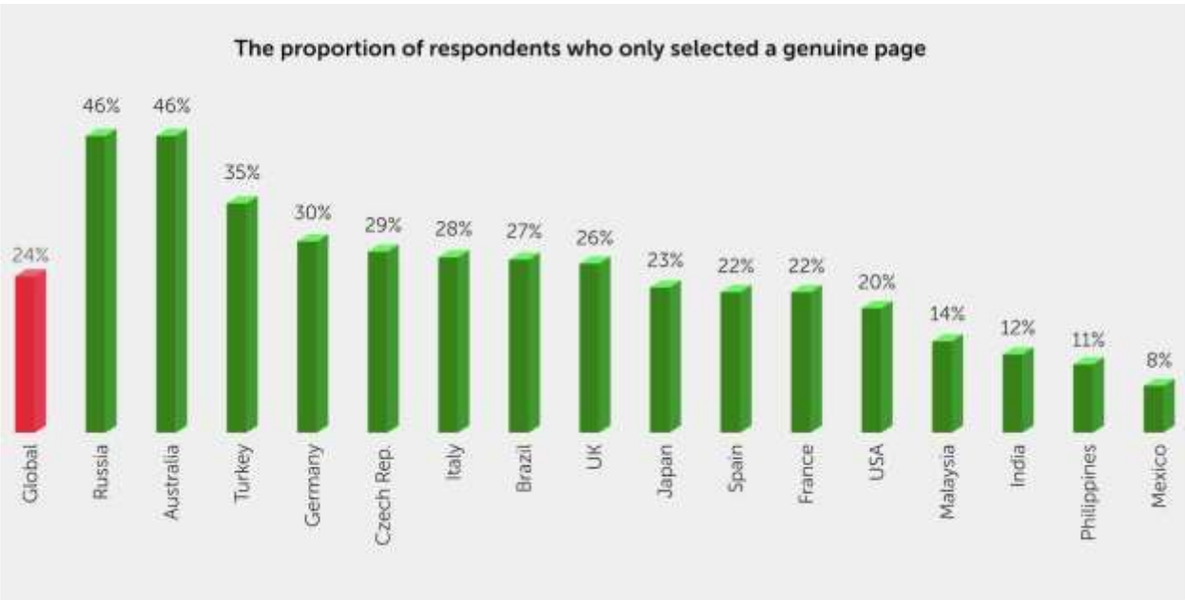
The third bucket involves 7,424 Philippine-based users. In addition to the data potentially obtained in relation to the first two groups of users, further information that may have been exposed include the posts on their

timeline, their list of friends, groups they are members of, and the names of recent Messenger conversations.

From the tenor of the document, we now understand that the breach exposed the personal information of persons with accounts that fall under any of the three buckets, to different degrees. Be that as it may, Facebook contends in its letter dated 13 October 2018 that there is no material risk of more extensive harm occurring.

This Commission does not agree; the risk of serious harm to Filipino data subjects is more than palpable. The conditions for individual notification are present.

As Facebook itself notes, the main potential impact for affected users will be an increased likelihood of getting targeted for professional "spam" operations and "phishing" attacks. However, the risk and vulnerability of Filipinos to spam and phishing are regarded as one of the highest in the world. According to the Are You Cyber Savvy Report from Kaspersky Lab, approximately 9 out of 10 Filipinos are susceptible to phishing attacks.[3]



The level of awareness for spam, phishing and identity theft in the Philippines is not the same as those of the United States and the other developed nations; considerations of risk must always consider the cultural milieu in which the risk is appreciated. For instance, this Commission takes notice that identity verification systems throughout the Philippines are quite weak.

---

[3] https://media.kasperskycontenthub.com/wp-content/uploads/sites/45/2018/03/08234157/Cyber_savvy_quiz_report.pdf (last accessed 18 October 2018).

As a milieu, the increase in risk for phishing and/or identity theft is self-evident for those persons who were exposed through the unauthorized use of the access tokens.

The Commission therefore deems it necessary that Facebook contemplate this cultural gap when notifying the affected data subjects. Facebook should modify its approach and provide a more conducive method that enables affected Filipino data subjects to better grasp the risks they face.

The potential deleterious effects of a breach should not be diluted in the notification to the data subjects. Data breach notifications for data subjects are for their benefit; we must provide as much information as possible to assist the affected data subjects to brace for its impact.

The manner and method of this notification is clearly defined under Section 18 of NPC Circular 16-03.

Facebook is hereby mandated to submit a more comprehensive Data Breach Notification Report and inform the data subjects in compliance with the provisions of NPC Circular No. 16-03 – Personal Data Breach Management.

Due to the nature and exposure of the Filipino data subjects, Facebook must also provide for identity theft insurance or credit monitoring service for free to affected Filipino data subjects; or, in the alternative, establish a dedicated helpdesk/help center for Filipino data subjects who may be adversely affected by this incident, to provide assistance in identity restoration and other related matters.

WHEREFORE, PREMISES CONSIDERED, this Commission, hereby **ORDERS** Facebook to:

1. **SUBMIT** a more comprehensive Data Breach Notification Report to this Commission following rules laid down in NPC Circular No. 16-03;
2. **NOTIFY** the affected data subjects through an appropriate Data Breach Notification following rules laid down in NPC Circular No. 16-03;
3. **PROVIDE** identity theft and phishing insurance for affected Filipino data subjects, or in the alternative, **ESTABLISH** a dedicated helpdesk/help center for Filipino data subjects on privacy related matters concerning Facebook, located in the Philippines and with a local number, within six (6) months from receipt of this Order;

4. **IMPLEMENT** a program in the Philippines or otherwise directed to Filipino data subjects to increase awareness on identity theft and phishing; and
5. **PROVIDE** evidence of compliance with the foregoing.

Given thru electronic mail and by hand, 17 October 2018.

SO ORDERED.

October 17, 2018, Pasay City, Metro Manila.

For the Commission:

(Signed)
RAYMUND E. LIBORO
Privacy Commissioner