Republic of the Philippines
NATIONAL PRIVACY COMMISSION

RMA

Complainant,

-versus-

NPC Case No. 17-065
For: Violation of the Data Privacy Act of 2012

INTERNATIONAL WORKPLACE GROUP PLC/REGUS

Respondent.

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

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by the complainant RMA against the respondent International Workplace Group PLC/Regus, Inc. for an alleged violation of R.A. 10173 ("Data Privacy Act").

The Facts

On 10 December 2017, the complainant filed a Complaint through the official email address of the Complaints and Investigation Division (CID). The complainant stated therein:

> I'm working for International Workplace Group PLC (Regus) as an IT Network Consultant. There was a group of people in our Windows IT department who stole the local database of my personal skype account. This is against our Company's internal policy. They used my private messages against me. They have sent selected conversations to our Human Resource department, then our HR served a Notice to Explain Letter to me and I was suspended for 1 week. The decision was made and the penalty was just a written reprimand as the violation is very minor. After a couple of days, HR sent another Notice to Explain letter with attached fabricated conversations created by those malicious employees. I think they will not stop until I'm dismissed.[1]

[1] Records, Page 2.

On 28 February 2018, the National Privacy Commission (Commission), through the CID, issued an Order to Confer for Discovery that ordered both parties to appear before the Commission on 27 March 2018. The Order stated thus:

> Pursuant to Section 13 of Circular 16-04 of the National Privacy Commission, the Parties shall discuss whether discovery of information and of electronically stored information will be sought; issues relating to preservation of information; period to produce the information; method of asserting and preserving claims of privilege information, confidentiality, and proprietary status of information; appropriateness of allocating expenses of production of information; and any other issue relating thereto.[2]

Only the representatives from the respondent appeared on 27 March 2018.[3] Complainant having failed to attend the Conference, the presiding officer proceeded to discuss with the respondent the purpose of the hearing. It was agreed that the respondent would file a comment with their internal policy and the privacy policy attached in the Comment.[4]

On 25 April 2018, the respondent, through their Data Protection Officer, filed their Answer with the Commission.

Arguments of the Parties

In his Complaint, the complainant alleged that his "private and sensitive conversations" were among the personal information affected, as well as "log-in credentials for very important portals like online banking and other confidential information."[5] Complainant sought dismissal of the "malicious employees" of the respondent.[6] He prayed for damages equivalent to the amount he lost caused by his suspension and all the legal actions he will take. He also prayed for a Cease and Desist Order to be issued directing their Human Resource to stop processing any illegally acquired or fabricated information.

---

[2] *Id.,* at 4-5.
[3] *Id.,* at 10.
[4] I*d.,* pp. 12-13.
[5] Ibid.
[6] Ibid.

Finally, his Complaint prayed for the issuance of a temporary ban on Respondent's processing of his data.[7]

In their Answer, the respondent specifically denies the allegation that they extracted from the complainant's personal Skype account, a series of chat messages between the complainant and the respondent's Head of Network, as well as those with Complainant's friend, RM, who worked for a different company, without his consent.[8]

Respondent asserts that the chat messages were voluntarily forwarded to Respondent's IT Service Operations Director EC, through an anonymous email address [ ]

According to the respondent, it did not violate any right of the complainant under the Data Privacy Act. Rather, they assert that it was the complainant who violated the respondent's company information policy, when, as shown in the chat messages, the complainant provided RM access to the respondent's infrastructure which would enable any external party to access their servers or firewall.[9] They admit that they should have meted out stiffer penalties to the complainant for his violation of the security policy, but only gave him a Written Reprimand.

The respondent asserts that it did not violate any of the rights of the complainant under the Data Privacy Act, and that the complainant failed to demonstrate that the respondent acted in a wanton, fraudulent, reckless, oppressive, or malevolent manner in dealing with the complainant.[10]

Issue

The sole issue to be resolved in this case is whether the respondent committed a violation of the DPA that warrants a recommendation for prosecution.

Discussion

Respondent did not commit a violation that warrants a recommendation for prosecution under the Data Privacy Act of 2012.

---

[7] *Id.,* at 2.
[8] *Id.,* at 29.
[9] *Id.,* at 30.
[10] *Ibid.*

In the Complaint, the complainant claims that there was a group of people in their Windows IT department who stole the local database of his personal Skype account.[11] The Commission notes, however, that the complainant only attached his BIR TIN ID and failed to provide any other supporting document to substantiate his claim that Respondent extracted "private and sensitive conversations, " as well as "log-in credentials for very important portals like online banking and other confidential information."[12]

The Commission further notes that, despite its issuance of an Order to Confer for Discovery to both parties, the complainant failed to appear at the Discovery Conference. Also, despite having been furnished a copy of Respondent's Answer which asserted that his allegations were "totally inaccurate and without basis," the complainant still failed to provide additional information or evidence to support his allegations.

The Complaint shall only be recommended for prosecution if it is supported with *relevant evidence which a reasonable mind might accept as adequate to justify a conclusion*.[13] The allegations in the complaint must be based on substantial evidence that there is a clear and real violation of the law.

In *Morales vs. Ombudsman, et al.*,[14] the Supreme Court explained:

> *The basic rule is that mere allegation is not evidence and is not equivalent to proof. Charges based on mere suspicion and speculation likewise cannot be given credence. When the Complainant relies on mere conjectures and suppositions, and fails to substantiate his allegations, the complaint must be dismissed for lack of merit.*[15]

The Commission's Rules of Procedure also provides:

> **Section 22.** ***Rendition of decision.*** – The Decision of the Commission shall adjudicate the issues raised in the complaint **on the basis of all the evidence presented** and its own consideration of the law.[16]

---

[11] *Id, at 2.*
[12] *Ibid.*
[13] Rules of Court, Rule 133, §5.
[14] 798 SCRA 609. 17 July 2016.
[15] *Id.,* at p. 627.
[16] NPC Circular No. 16-04 dated 15 December 2016 ("NPC Rules of Procedure"), Sec. 22, Emphasis supplied.

As such, on the basis of all the evidence presented, the Commission finds that there is insufficient evidence to support the complainant's claim that the respondent stole the local database of the complainant's personal Skype account, accessing private and sensitive conversations as well as login credentials.

Considering that there is nothing in the Complaint that would reasonably connect the respondent to any of the possible violations enumerated under the DPA, the Commission resolves to dismiss the Complaint for lack of substantial evidence required in establishing cases before quasi-judicial bodies.

WHEREFORE, all the above premises considered, the Commission hereby resolves to **DISMISS** the Complaint of RMA against International Workplace Group PLC/Regus.

SO ORDERED.
Pasay City, 31 January 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

RMA
Complainant

JRB
Respondent's Data Protection Officer

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission