Republic of the Philippines
NATIONAL PRIVACY COMMISSION

CCMC

Complainant,

-versus-

NPC Case No. 18-K-200
For: Violation of the Data Privacy Act of 2012

QUICKLEND, INC.

Respondent.

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

DECISION

AGUIRRE, *D.P.C.:*

Before this Commission is a Complaint filed by Complainant CCMC against Respondent Quicklend, Inc. for an alleged violation of R.A. 10173 ("Data Privacy Act").

The Facts

The facts of this case are not disputed.

On 10 October 2018, Complainant received an email from Respondent with the subject "Early Payment Reminder."[1] It was a mass email sent by KR, an employee from Quicklend, Inc., a financing company to their clients, including Complainant:

> Greetings from Quicklend, Inc. This is to kindly remind you to maintain your loan payment amount in your payroll account which is due for Auto-Debit Deduction on October 15, 2018. Please be informed that there will be a daily P50.00 penalty fee while your Auto-Debit Deduction is unsuccessful due to insufficient funds. Thank you for your due diligence with us and helping us avoid possible collection problems and additional finance charges.[2]

Complainant noticed in the address bar that she was one among 136 recipients of the email and that one of the recipients was her manager

---

[1] Records, pp. 6-8.
[2] *Ibid.*, at p. 15.

at work.[3] The names and email addresses can be seen by all 136 recipients.[4]

On the same day, Complainant replied to the email, stating that they have breached the Data Privacy Act of 2012 as she did not authorize them to show her personal information to every one of their customers.[5]

On 11 October 2018, KR sent an email to Complainant apologizing for the email blast, which stated:

> Hi Ma'am,
>
> We apologize for what happened yesterday and I promise that this would not happen again. I also like to inform you that I'm already the one who's handling your account. Hoping for your consideration.[6]

On 30 October 2018, Complainant filed her Complaint with the National Privacy Commission[7] and sent KR a screencap of the complaint. Complainant approached the Data Protection Officer of Respondent, RBP, about the data breach.[8]

On 31 October 2018, RBP contacted Complainant over Facebook Messenger to apologize for the incident. He informed the Complainant that they imposed sanctions to the one in charge of her account and asked for understanding, asserting it was an honest mistake.[9]

On 5 November 2018, RBP emailed the Commission and explained the situation:

> Unfortunately, through excusable oversight, our staff Ms. KR, instead of placing the email addresses of our clients in the Blind Carbon Copy (BCC) portion of the email, she instead placed around one hundred thirty five (135) email addresses on the "TO" section of the mail.
>
> This is not our practice, we always place on the "Bcc:" the email addresses of our clients when we send them our reminders.

---

[3] *Ibid.*, at p. 7.
[4] *Ibid.* at p. 22.
[5] *Ibid.* at p. 15.
[6] *Ibid.* at p. 24.
[7] *Ibid.* at p. 6.
[8] *Ibid.* at p. 14.
[9] *Ibid.* at p. 27-32

> Therefore our clients, who received the email could see the other recipients. This mistake was unintentional and a mere oversight on the part of the employee.
>
> The Management convened the employees concerned who were in-charge of sending emails and took initial steps to prevent a recurrence of the incident.
>
> a. The assigned employees should be careful and circumspect in sending the email reminders, that when there are several recipients, their email addresses should be placed in the BCC portion; and
>
> b. The DPO and his team should review and recommend procedures to further enhance our data privacy procedure.
>
> c. The DPO and his team will report to Management on or before 25 November 2018 of his recommendations.[10]

On 7 November 2018, Respondent sent an email to the previous recipients of the email complained of, which stated:

> Dear Sir / Madam,
>
> We are writing to inform you of a recent incident that may affect the security of your personal information. We are providing this notice to ensure that you are aware of the incident so that you may take steps to protect your information should you feel it is appropriate to do so.[11]

On the same day, Respondent issued a memorandum of reprimand to KR, following her explanation and apology to Respondent.[12]

Arguments of the Parties

Complainant asserts in her Complaint that having her Manager as one of the recipients of this email will provide her employer, part of the financial sector, an impression that she has debts which may negatively affect her career. She stressed that she did not tell anyone about these debts, not even her family. She also states that she is worried that her personal email address and her name will be used for malicious acts in the future.[13]

---

[10] Records, p. 34.
[11] *Ibid.* at p. 39-41.
[12] *Ibid.* at p. 44.
[13] I*bid.* at p. 2.

She indicates in her Complaint that:

> I lost many hours dealing with this personal data breach, even while I am at work. I don't know what else could happen to my personal information, but it might bring identity theft or fraud against my name which I am taking very seriously.

In Complainant's letter to the Commission, received on 16 April 2019, she states that:

> On the said email, I only realized that my Manager was copied on the email. This gave her an impression that I have debts to which is critical in my career as I work in a BPO-Financial Industry. My reputation, my name and my email address was placed at risk. xxx And since I previously worked in Accenture, some acquaintances were copied on the email as these are work emails. Recently, I received an email from someone I do not know but luring and asking personal information.
>
> xxx
>
> If the Respondent would take full responsibility of this case, I would like to seek the following for breaching my personal information and damage to my reputation at work:
>
> 1. A written apology letter from Quicklend, not from their representative, admitting of the mistake they have done and explanation of process on how will they dispose my information since I am no longer their client;
> 2. Compensation on MORAL DAMAGES worth not more than Php 100, 000;
> - Threat of loss of trust and confidence of the company and my team
> - Potential threat to my work as I work in a financial industry
> - Defamation of my reputation and character was disclosed to 136 recipients of a debt reminder email.

Respondent states in their Comment that it is the company's normal practice to send routine reminders to their clients before their scheduled collection dates. They state that this is a "generic email that divulges no information other than that their payment is due for a particular collection period."[14]

In their Comment, they state that:

> In conclusion, we profusely apologize for the incident. We would like to emphasize that it was a purely clerical error and oversight. No malice

---

[14] I*bid.*, p. 13.

> was intended toward the recipients. We have already implemented measures that this will not happen again.[15]

In their Rejoinder, they stated that:

> The email blast is a gentle reminder to all clients, regardless of credit standing, and that it was not a delinquent notice that was meant to embarrass or harass and there is no personal information divulged.[16]
>
> xxx
>
> We deny the allegation that it caused moral damages because it was a purely clerical error and done in good faith. No malice was intended towards the recipients.
>
> The complainant is not entitled to any form of damages.

Issues

The issues to be resolved in this case are:

1. Whether personal information was involved; and
2. Whether there was a personal data breach.

Discussion

There was personal information involved.

Contrary to what Respondent asserts, personal information was divulged when Respondent's employee sent a mass email of an early payment reminder to 136 recipients, inadvertently copying the email addresses to the "To:" portion of the address bar, instead of "Bcc:" or blind carbon copy, as is supposed company practice.

The Data Privacy Act defines personal information as "any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."[17]

---

[15] Records, p. 15-16.
[16] Ibid. at, p. 15.
[17] R.A. 10173, Sec. 7(b).

In this case, Complainant's entry was "CCMC [email address]". Aside from this, there were other entries containing information that directly ascertained the identity of the other recipients.

The information disclosed did not just consist of the names and email addresses of respondent's clients. In some instances, the entries also contained the clients' middle names, employers, and even birthdates.

The incident is a personal data breach.

A personal data breach is defined in NPC Circular 16-03 as "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed."[18]

It may be in the nature of an availability breach resulting from the loss, accidental or unlawful destruction of personal data; an integrity breach resulting from alteration of personal data or a confidentiality breach resulting from the unauthorized disclosure of or access to personal data.[19]

In this case, her name and email address, both personal information, together with the fact of her loan with Respondent, were disclosed to 135 other individuals. Respondent readily admits when they stated that the mass email placing recipients in the "To:" portion of the address bar instead of the "Bcc" portion was an inadvertence and not the company's regular practice.[20]

This admitted disclosure was not justified by Respondent under any of the lawful criteria for processing personal information under the Data Privacy Act, namely:

> (a) The data subject has given his or her consent;
>
> (b) The processing of personal information is necessary and is related to the fulfillment of a contract with the data subject or in order to take steps at the request of the data subject prior to entering into a contract;
>
> (c) The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;

---

[18] NPC Circular no. 16-03, dated 15 December 2018. Section 3(F).
[19] *Id.*
[20] Records, p. 13.

> (d) The processing is necessary to protect vitally important interests of the data subject, including life and health;
>
> (e) The processing is necessary in order to respond to national emergency, to comply with the requirements of public order and safety, or to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate; or
>
> (f) The processing is necessary for the purposes of the legitimate interests pursued by the personal information controller or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject which require protection under the Philippine Constitution.[21]

Lacking any basis under the law, such disclosure of Complainant's personal information is considered unauthorized disclosure. This incident is in the nature of a confidentiality breach under NPC Circular 16-03.[22]

The fact that such unauthorized disclosure was a "mere oversight on the part of the employee"[23] does not relieve Respondent from the obligations provided by law and the Commission's issuances.

The Commission notes the delay of Respondent in notifying the Commission about the incident on 5 November and in notifying the affected data subjects on 7 November, despite having been informed by Complainant as early as 10 October 2018, when she replied to the email.

This is in contravention of NPC Circular 16-03 which states that the Commission and the affected data subjects shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.[24]

The 72 hour-requirement is not limited to working days, contrary to what Respondent proffers in their Comment. The intention for this period to be uninterrupted is underscored by the fact that it is stated as 72 "hours", which should not be in any way affected by holidays or weekends. Delay for notification to the Commission is only justified to the extent necessary to determine the scope of the breach, to prevent

---

[21] Data Privacy Act, Sec. 12.
[22] NPC Circular 16-03 dated 15 December 2016. Section 3 (f).
[23] Records, p. 34.
[24] NPC Circular 16-03 dated 15 December 2016. Section 17(a).

further disclosures, or to restore reasonable integrity to the information and communications system.[25] On the other hand, personal information controllers may request from the Commission either a delay in or exemption from notification of data subjects when it may hinder criminal investigation, or when it is not in the interest of the affected data subjects.[26] Such grounds were not alleged by Respondent.

The time requirement for notifying affected data subjects is meant to allow them to take the necessary precautions or other measures to protect themselves against the possible effects of the breach.[27]

Respondents assert a supposed company practice of using blind carbon copy or "Bcc" instead of the "To" field when sending mass emails. Nevertheless, incidents such as this, and the protracted response thereto indicate Respondent's lack of policies and procedures for the data breach response team and other personnel. The guidelines issued by the Commission provide that such policies should include, among others:

1. A procedure for the timely discovery of security incidents, including the identification of person or persons responsible for regular monitoring and evaluation of security incidents;
2. Clear reporting lines in the event of a possible personal data breach, including the identification of a person responsible for setting in motion the incident response procedure, and who shall be immediately contacted in the event of a possible or confirmed personal data breach;
3. Conduct of a preliminary assessment for purpose of:
    1. Assessing, as far as practicable, the nature and scope of the personal data breach and the immediate damage
    2. Determining the need for notification of law enforcement or external expertise; and
    3. Implementing immediate measures necessary to secure any evidence, contain the security incident and restore integrity to the information and communications system;
4. Evaluation of the security incident or personal data breach as to its nature, extent and cause, the adequacy of safeguards in place, immediate and long-term damage, impact of the breach, and its potential harm and negative consequences to affected data subjects;
5. Procedures for contacting law enforcement in case the security incident or personal data breach involves possible commission of criminal acts;
6. Conduct of investigations that will evaluate fully the security incident or personal data breach;

---

[25] Id., at Sec. 17(b).
[26] Id., at Sec. 18(b).
[27] Id., at Sec. 18(a).

7. Procedures for notifying the Commission and data subjects when the breach is subject to notification requirements, in the case of personal information controllers, and procedures for notifying personal information controllers in accordance with a contract or agreement, in the case of personal information processors; and
8. Policies and procedures for mitigating the possible harm and negative consequences to a data subject in the event of a personal data breach. The personal information controller must be ready to provide assistance to data subjects whose personal data may have been compromised.[28]

The lack of such policies inevitably lead to inadvertences such as in this case. Respondent must realize the impacts of such personal data breaches to the data subjects.

WHEREFORE, all the above premises considered, the Commission hereby **ORDERS** Respondent to submit, **within thirty (30) days** from receipt of this Decision, their security incident management policy that is compliant with the guidelines stated in NPC Circular 16-03, pursuant to the undertaking in their 5 November 2018 letter to the Commission that a report to management will be made by 25 November 2018 regarding the review and recommendation of procedures by the DPO and his team.

SO ORDERED.
Pasay City, 17 January 2020.

Sgd.
LEANDRO ANGELO Y. AGUIRRE
Deputy Privacy Commissioner

Concurring:

Sgd.
RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

---

[28] NPC Circular 16-03, dated 15 December 2016. Sec. 8.

Sgd.
JOHN HENRY DU NAGA
Deputy Privacy Commissioner

COPY FURNISHED

CCMC
Complainant

RBP
Respondent's Data Protection Officer
Quicklend, Inc.

ENFORCEMENT DIVISION
GENERAL RECORDS UNIT
National Privacy Commission