Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2022-017[1]

20 September 2022

[redacted]

Re: DISCLOSURE OF PERSONAL INFORMATION FOR CYBERSECURITY INVESTIGATIONS

Dear [redacted]:

We respond to your request for an Advisory Opinion on the application of Republic Act 10173 (or the Data Privacy Act of 2012 [DPA])[2] on your client's request for information from a certain corporation for investigation purposes regarding a cybersecurity incident.

We understand that your client, Corporation A, is the owner, operator, and franchise licensor of Brand B stores in the Philippines. Besides being a seller of consumer products, Brand B stores offer e-services such as bills payment, top up, cash-in, and remittance for its accredited merchant partners. One of Corporation A's largest merchant partner is Corporation C which is an e-Money Issuer.

You allege that on 1 December 2020, Corporation A discovered staggering discrepancies between the cash-ins recorded in Corporation A's System and the actual cash received by a Brand B store in Davao City. Corporation A created an investigation committee which learned that during the period 9 November – 1 December 2020, 2,516 unique Corporation C accounts successfully made cash-ins through the Corporation C application amounting to PhP249,011,058.00, all without going through the Point of Sale (POS) system of the Brand B Davao Store and without the latter receiving the money from the account holders. The cash-ins appear to have bypassed the Corporation A's System and POS and, thus, Corporation A has no record of receiving the amounts.

Corporation A immediately notified Corporation C of the incident and requested the latter to block the said 2,516 accounts. Based on Corporation A's investigation, while the cash-ins

[1] Tags: personal data; lawful processing; consent of data subjects; legal claims; Sec. 13 (f), DPA.

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173 (2012).

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1307
URL https //www privacy gov ph Email Add info@privacy gov ph * Tel No 8234-2228

involved 2,516 accounts, the incident appears to have been instigated by a syndicate of approximately 10 people by creating and using the said accounts.

In the course of Corporation A's investigations, it coordinated with Corporation C to request for information and validation of the 2,516 accounts that made the cash-ins. In particular, Corporation A requested for the following information (Requested Information):

1. Number of Corporation C accounts opened after November 2020;
2. Number of top-up transactions that were made through the Corporation C application;
3. Information regarding the accounts, including details on date of creation, manner of KYC, and other pertinent details;
4. Confirmation that the 2,516 accounts were legitimate Corporation C users;
5. Confirmation that the 2,516 accounts have been prevented from further withdrawals;
6. Confirmation that Corporation C has alerted recipient financial and non-financial institutions of the fraudulent activity in order for them to hold the funds;
7. Information regarding the recipient financial institutions that the funds were transferred or withdrawn, and the number of unique accounts in each;
8. Information regarding the withdrawals from ATM machines using the Corporation C ATM card, specifying the date, time, location, and ATM operator/bank;
9. Confirmation that the ATM operator has been notified of possible fraud and instructing them to store CCTV footage from the ATM pending further investigation;
10. Any other details that could aid Corporation A in the investigation.

However, Corporation C responded that any information to be released in relation to the incident was covered by the DPA. According to Corporation C, there must be prior consent from the data subject or a court order compelling it to disclose the information.

You thus ask whether:

a. Item nos. 1, 2, and 4 to 10 of the Requested Information are not considered as personal data, and thus not covered by the DPA; and
b. Even assuming the above information, as well as item no. 3, are considered personal data, that the disclosure of such Requested Information does not require data subject consent prior to disclosure, as claimed by Corporation C.

It is your contention that item nos. 1, 2, and 4 to 10 are not personal data considering that the disclosure will not enable or allow the identification of persons, individuals or data subjects and are not within the purview of protected information under the DPA. In addition, it is your opinion that consent of the data subject and court order are not the only bases for disclosure of personal data.

Information excluded from the scope of the DPA.

Under the DPA, personal information refers to 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.[3] On the other hand,

[3] Data Privacy Act of 2012, § 3 (g).

sensitive personal information is clearly defined under Section 3 (l) of the law.[4] Consequently, information that does not identify an individual are beyond the scope of the DPA.

Nevertheless, there is a need to examine the nature of the information involved item nos. 1, 2, and 4 to 10 to ascertain if they are indeed excluded from the scope of the DPA.

Item no. 1 [number of Corporation C accounts opened after November 2020] and item no. 2 [number of top-up transactions that were made through the Corporation C application] only deal with numbers of accounts and transactions, respectively.

Item no. 4 [confirmation that the 2,516 accounts were legitimate Corporation C users], item no. 5 [confirmation that the 2,516 accounts have been prevented from further withdrawals], item no. 6 [confirmation that Corporation C has alerted recipient financial and non-financial institutions of the fraudulent activity in order for them to hold the funds], and item no. 9 [confirmation that the ATM operator has been notified of possible fraud and instructing them to store CCTV footage from the ATM pending further investigation] merely involve verification of the action mentioned that can be responded to by a simple "yes" or "no" answer.

Item no. 7 [information regarding the recipient financial institutions that the funds were transferred or withdrawn, and the number of unique accounts in each] deal with business information.

Item no. 8 [information regarding the withdrawals from ATM machines using the Corporation C ATM card, specifying the date, time, location, and ATM operator/bank] are information on transaction details of withdrawals using Corporation C ATM card, specifically limited to date, time, location and the ATM operator/bank.

The foregoing reveals that the nature of the information enumerated above are not personal data as these do not identify a unique individual. Thus, such items are indeed outside the scope of the DPA.

However, item no. 10 [any other details that could aid Corporation A in the investigation] is too broad for us determine if it may include personal data as defined by the DPA.

Consent or court order not required for disclosure; information necessary for the establishment, exercise or defense of legal claims

It is your contention that all of the Requested Information, including item no. 3 [information regarding the accounts, including details on date of creation, manner of KYC, and other pertinent details], are not covered by the DPA. You also contend that even if items 1, 2, and 4 to 10 are considered as personal data, such information may still be disclosed without the need for the data subject's consent or a court order, citing Sections 12 (f) and 13 (f) of the DPA in conjunction with the National Privacy Commission's (NPC) Decision in *BGM vs. IPP*.[5]

---

[4] *Id*. § 3 (l).

[5] *See:* National Privacy Commission, BGM vs. IPP, NPC 19-653 (17 December 2020), available at https://www.privacy.gov.ph/wpcontent/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf (last accessed 03 February 2022).

We find merit in your argument.

Sections 12 (f) and 13 (f) of the DPA state:

> SEC. 12. Criteria for Lawful Processing of Personal Information. – The processing of personal information shall be permitted only if not otherwise prohibited by law, and when at least one of the following conditions exists:
>
> xxx
>
> (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.
>
> SEC. 13. Sensitive Personal Information and Privileged Information. – The processing of sensitive personal information and privileged information shall be prohibited, except in the following cases:
>
> xxx
>
> (f) The processing concerns such personal information as is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims, or when provided to government or public authority. (Emphasis supplied)

In NPC Advisory Opinion No. 2021-036,[6] the NPC once again discussed the application of the abovementioned provisions in relation to the processing of personal data necessary for the establishment, exercise or defense of a legal claims out of court, and likewise reiterated its ruling in *BGM vs. IPP*, *viz*:

> In the interpretation of the phrase "establishment, exercise or defense of legal claims," the Commission reiterated its stand in the case of BGM vs. IPP, viz:
>
> > In the case of NPC 17-018 dated 15 July 2019, this Commission held that "processing as necessary for the establishment of legal claims" does not require an existing court proceeding. To require a court proceeding for the application of Section 13(f) to this instance would not only be to disregard the distinction provided in the law but the clear letter of the law as well. After all, the very idea of "establishment … of legal claims" presupposes that there is still no pending case since a case will only be filed once the required legal claims have already been established."
> >
> > …
> >
> > The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.
>
> Given the above, the establishment of legal claims requiring the processing of sensitive personal information is permitted under the DPA. The term establishment may include

[6] National Privacy Commission, Advisory Opinion No. 2021-036 (23 September 2021).

> activities to obtain evidence by lawful means for prospective court proceedings. As such, the DPA does not require the establishment of actual or ongoing court proceedings in the application of Section 13 (f).
>
> …
>
> The Commission's pronouncement in the same case of BGM v. IPP may be applied in the same vein:
>
> > Although Section 13(f) applies to sensitive personal information while the information involved in this case is just personal information, the protection of lawful rights and interests under Section 13(f) by the Respondent is considered as legitimate interest pursuant to Section 12(f) of the DPA.[7]

Similar to the factual milieu of NPC Advisory Opinion No. 2021-036, it is apparent that Corporation A has a legal claim to the PhP249,011,058.00 that were allegedly fraudulently withdrawn from Brand B Davao Store. In order to aid its own investigation and establish its case, Corporation A would have to gather necessary information from Corporation C as the merchant partner involved in the transactions subject of the claim.

Given the foregoing, Corporation C need not obtain consent from its data subjects or wait for a court order to provide Corporation A with the Requested Information, subject to other applicable laws or regulations.

We take this opportunity to remind that while it appears there exists justification for the disclosure of personal data, the DPA mandates that the principle of proportionality should still be adhered to. Proportionality requires that the processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.[8]

Please be advised that this Advisory Opinion was rendered based solely on the information you provided. Any extraneous fact that may be subsequently furnished us may affect our present position. Please note further that our Advisory Opinion is not intended to adjudicate the rights and obligations of the parties involved.

Please be guided accordingly.

Very truly yours,

(Sgd.)
FRANKLIN ANTHONY M. TABAQUIN IV
Director IV, Privacy Policy Office

---

[7] *Id*. Citations omitted.
[8] Rules and Regulations Implementing the Data Privacy Act of 2012, Republic Act No. 10173, § 18 (c) (2016).