Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2020-039[1]

30 October 2020

[redacted]

Re: DISCLOSURE OR SHARING OF BANK TRANSACTION INFORMATION FOR FRAUD INVESTIGATIONS

Dear [redacted]

We write in response to your letter received by the National Privacy Commission (NPC) wherein you disclosed that the Union Bank of the Philippines (the Bank) has initiated several investigations on alleged fraudulent transactions executed through multi-platform transactions wherein said transactions are either triggered from the Bank for transfer to non-bank accounts such as electronic money issuers (EMIs) and vice versa, which culminates in cash withdrawals.

We understand further that fraud transactions can effectively be investigated when transaction details, such as the following, are shared among affected banks and EMIs: 1) destination EMI; 2) destination account number; 3) origin EMI; 4) origin account number; 5) transaction type; 6) transaction date; 7) transaction time; 8) amount; 9) fraud type and 10) reference number.

You now inquire on whether the disclosure or sharing of the above transaction details for purposes of fraud investigation is allowed under the Data Privacy Act of 2012 (DPA), its Implementing Rules and Regulations (IRR) and other relevant issuances of the NPC.

Personal information; lawful processing; legitimate interest

The DPA 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

[1] Tags: personal information; bank transaction details; fraud investigation; legitimate interests.

directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual.[2]

Based on this definition, transaction details such as bank account numbers and transaction reference numbers may be considered as personal information since said details can directly identify a person. In this regard, these transaction details fall within the scope of the DPA.

Note that the processing of personal information shall be permitted if not otherwise prohibited by law, and when at least one of the criteria required by the DPA is met. In particular, Section 12 (f) of the law provides that the processing of personal information is allowed when it is "necessary for the purpose 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."

Under this provision, a personal information controller (PIC) must be able to establish that a legitimate interest in processing the personal information exists. As discussed in our previous Advisory Opinion, legitimate interests are matters that are desired or important to a PIC, which may include business, financial or other reasonable purpose, which are of course not contrary to law, morals or public policy.[3] For this reason, the PIC or third party or parties to whom the personal data is disclosed must clearly identify such legitimate interest, reasonable purpose and intended outcome.[4]

While the DPA does not specifically identify matters to be taken into consideration in the PIC's determination of its legitimate interests, the EU General Data Protection Regulation (GDPR), the successor of the EU Data Protection Directive (Directive 95/46/EC) which highly influenced the DPA, provides some guidance, whereby the processing of personal information strictly necessary for purposes of fraud prevention constitutes a legitimate interest.[5]

Thus, fraud investigation may be considered as the legitimate interest of the Bank and or third parties, and may be used as lawful basis for the disclosure or sharing of personal information.

Legitimate interests test

In the determination of legitimate interest, personal information controllers (PICs) must consider the following:[6]

1. Purpose test - The existence of a legitimate interest must be clearly established, including a determination of what the particular processing operation seeks to achieve;

---

[2] An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and Private Sector, Creating for this Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 3 (g) (2012).
[3] National Privacy Commission, NPC Advisory Opinion No. 2018-061 citing United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis", available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.
[4] Ibid.
[5] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Official Journal of the European Union, Vol. L119, Recital 47 (2016).
[6] See generally, Data Privacy Act of 2012, § 12 (f); United Kingdom Information Commissioner's Office (ICO), What is the 'Legitimate Interests' basis?, *available at* https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/.

2. Necessity test - The processing of personal information must be necessary for the purpose of the legitimate interest pursued by the PIC or third party to whom personal information is disclosed, where such purpose could not be reasonably fulfilled by other means; and
3. Balancing test - The fundamental rights and freedoms of data subjects must not be overridden by the legitimate interests of the PIC or third party, considering the likely impact of the processing on the data subjects.

To reiterate, the Bank must be able to establish that the foregoing conditions are met in order to rely on legitimate interest as a lawful basis in the processing of personal information.

First, it must be established that the investigation is strictly for purposes of resolving previously committed frauds and preventing possible frauds.

Second, only personal information which is necessary and proportionate to facilitate the fraud investigation may be processed pursuant to the said identified legitimate interest.

Lastly, it should be established that the fundamental rights and freedoms of data subjects are not overridden by the legitimate interests of the PIC. Hence, there should be minimal impact on the data subjects and in the exercise of their rights. To determine any potential risks, it must be assessed whether the data subjects had a reasonable expectation at the time and in the context of the collection of personal information that processing for fraud investigation purposes may take place.[7]

Among the factors which may be considered in assessing the reasonableness of the processing are the relationship between the PIC and the data subject and the transparency of the PIC at the time of the collection of data. For a more comprehensive discussion on reasonable expectation, kindly refer to NPC Case 17-047 available at https://www.privacy.gov.ph/wp-content/uploads/2020/10/CID-17-047-JV-v.-JR-Decision-PSD-10Aug2020.pdf.

In the current matter, the data subjects who utilized the facilities of Union Bank for their electronic transactions may reasonably expect that the latter must ensure that all transactions are legitimate, which includes the prevention or resolution of possible and committed frauds, respectively. Moreover, the business of banking is of a fiduciary nature which requires high standards of integrity and performance.[8]

Given the circumstances, the resolution and prevention of fraud may be considered as the legitimate interest of the Bank and the disclosure of its affected clients' transaction details with third parties on such lawful basis may be allowed.

General data privacy principles; reasonable and appropriate security measures

The PIC, although with lawful basis in the processing of personal information, still has the obligation to comply with the other requirements of the DPA.

The processing of information must still adhere to the general data privacy principles of transparency, legitimate purpose, and proportionality. As PICs, the Bank and third parties are also required to implement reasonable and appropriate organizational, physical, and

[7] EU GDPR, Recital 47.
[8] An Act Providing for the Regulation of the Organization and Operations of Banks, Quasi-Banks, Trust Entities, and for Other Purposes [General Banking Law of 2000] Republic Act No. 8791, § 2 (2000).

technical security measures to protect the disclosed personal data. In addition, banks as PICs are also required to regularly monitor for security breaches and take preventive, corrective and mitigating measures against incidents which may lead to security breaches.[9] The PICs involved may also consider entering into a data sharing agreement or a similar contract to document the disclosure or sharing arrangement, as may be necessary and appropriate.

This opinion is based solely on the limited information you have provided. Additional information may change the context of the inquiry and the appreciation of facts. This opinion does not adjudicate issues between parties nor impose any sanctions or award damages.

For your reference.

Very truly yours,

(Sgd.) RAYMUND ENRIQUEZ LIBORO
Privacy Commissioner

[9] Data Privacy Act of 2012, § 20 (c) (4).