Republic of the Philippines
NATIONAL PRIVACY COMMISSION

PRIVACY POLICY OFFICE
ADVISORY OPINION NO. 2021-026[1]

12 July 2021

[redacted]

Re: DATA PRIVACY IMPLICATIONS FOR FINANCIAL SERVICES INDUSTRY INITIATIVES ON DATA SHARING

Dear [redacted]

We write in response to your letter received by the National Privacy Commission (NPC) which sought clarification on two proposed initiatives of the financial services industry on cybersecurity, specifically on data sharing.

We understand that the financial services industry has been shifting to digital financial and payment services in response to the COVID-19 pandemic. You disclosed further that cyberthreat actors continue to exploit the vulnerabilities of the Bangko Sentral ng Pilipinas (BSP) Supervised Financial Institutions (BSFIs) and their clients.

We further understand from your letter that the BSP's surveillance revealed that these cyber attacks and fraudulent schemes affect two or more financial institutions, such as banks and non-bank financial institutions such as e-money issuers, Virtual Asset Service Providers (VASPs) and remittance companies, simultaneously.

With this, the BSP, in consultation with industry associations, developed two key initiatives to prevent fraud incidents and uphold the customers' confidence in digital payment systems.

The first proposal is for a BSP regulatory issuance on data sharing among BSFIs. The said regulation would provide data sharing guiderails including definitions of permissible data

[1] Tags: lawful processing; sensitive personal information; legal claim; law; regulation; BSP; fraud investigation; fraud prevention; blacklists; fairness; lawfulness; accuracy; privacy impact assessment; data subject rights; limitations.

5th Floor, Philippine International Convention Center, Vicente Sotto Avenue, Pasay City, Metro Manila 1308
URL: https//www.privacy.gov.ph Email Add: info@privacy.gov.ph * Tel No. 8234-2228

gathering and sharing and the necessary controls to prevent any possible abuse in the data sharing arrangement. This will enable the open and transparent sharing of information among BSFIs to facilitate investigation and resolution of fraud incidents.

The second proposal is the establishment of a shared database of suspected and blacklisted accounts containing information on verified mule account holders such as customer name, case details, transaction details and online banking credentials, among others. BSFIs shall use the shared database in conducting Know-Your-Customer (KYC) procedures for new depositors/clients and in performing Enhanced Due Diligence (EDD) as part of the regular anti-money laundering (AML) monitoring for existing clients. This mechanism will prevent verified mule accountholders to open accounts and perform financial transactions with BSFIs which would significantly enhance integrity in the financial system

You now ask whether the processing of sensitive personal information for the said proposals may fall under Section 13 (f) of the Data Privacy Act of 2012[2] (DPA) which allows processing of personal data for the protection of lawful rights and interests of natural or legal persons. You further ask on whether a court order is required under the said lawful basis or if a regulatory issuance by the BSP on fraud information sharing guidelines shall suffice.

Data sharing; lawful basis for processing; establishment, exercise, or defense of legal claims; sharing based on laws and regulations

The DPA allows the processing of sensitive personal information provided the requirements of the law are complied with and subject to strict adherence to the basic data privacy principles of transparency, legitimate purpose and proportionality.

Section 13 (f) of the DPA, which may be applicable to the current scenario, recognizes the processing of sensitive personal information when it is necessary for the protection of lawful rights and interests of natural or legal persons in court proceedings, or in the establishment, exercise of defense of legal claims, or when provided to government or public authority.[3]

In the case of BGM vs. IPP,[4] the Commission had the opportunity to clarify Section 13 (f) in this wise:

> "x x x. Its requirement of compelling Complainant to produce a court order prior to the release of the requested information creates a high barrier that effectively impedes the rights vested by the DPA to the latter as a data subject.
>
> Further, Respondent's assertion that the information within its custody can only be disclosed upon data subject's consent or on the basis of a lawful order is misplaced. x x x
>
> 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

[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).
[3] Data Privacy Act of 2012, § 13 (f) (2012).
[4] National Privacy Commission, BGM vs. IPP [NPC 19-653] (Dec. 17, 2020), available at https://www.privacy.gov.ph/wp-content/uploads/2021/02/NPC-19-653-BGM-vs-IPP-Decision-FINAL-Pseudonymized-21Dec2020.pdf (last accessed 9 July 2021).

required legal claims have already been established."

This Commission in the same case went on further and held that: The DPA should not be seen as curtailing the practice of law in litigation. Considering that it is almost impossible for Congress to determine beforehand what specific data is "necessary" or may or may not be collected by lawyers for purposes of building a case, applying the qualifier "necessary" to the second instance in Section 13(f) therefore, serves to limit the potentially broad concept of "establishment of legal claims" consistent with the general principles of legitimate purpose and proportionality. As regards legitimate purpose, the Implementing Rules and Regulations (IRR) of the Data Privacy Act provides that the processing of information shall be compatible with a declared and specified purpose which must not be contrary to law, morals, or public policy. This means that the processing done for the establishment of a legal claim should not in any manner be outside the limitations provided by law. The DPA is neither a tool to prevent the discovery of a crime nor a means to hinder legitimate proceedings.

Based on the foregoing, the disclosure to be made by the Respondent of the information of the recipient of Complainant's personal information, for purposes of identification of the person liable for the alleged fraud, sans the latter's consent, is necessary for the protection of the lawful rights and interests of the Complainant as contemplated by Section 13 (f) of the DPA." (underscoring supplied)

Thus, the sharing of sensitive personal information for the establishment, exercise, or defense legal claims in relation to fraud investigations and fraud prevention may be allowed under Section 13 (f) of the DPA. The same does not require an existing court proceeding, and thus, such processing will not necessarily require a court order.

As we also discussed in Advisory Opinion No. 2021-017,[5] requests for information from online platforms and financial intermediaries by government agencies may come in various forms, i.e., courts orders, subpoenas, officially issued orders, memoranda, letters, and other communication, among others, depending on several factors, such as the stage of the investigation or enforcement action as well as the powers of the particular agency, i.e., some may have subpoena powers and while others do not.[6]

For the general data privacy principle of legitimate purpose, the expectation is that all due process requirements have been complied with in relation to any request for personal data. Likewise, for proportionality, the same requires that the processing of personal data shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

We also wish to emphasize that once the proposed BSP regulatory issuance takes effect, the data sharing may then be based on such issuance, in relation to Section 13 (b) of the DPA which recognizes processing that is pursuant to existing laws and regulations.

Advisory Opinion Nos. 2020-050, 2020-039, 2019-041; credit card fraud; disclosure by online platforms, fintech, digital payment platforms, and telecommunications; sharing of bank transaction information for fraud investigations

[5] National Privacy Commission, NPC Advisory Opinion No. 2021-017 (June 8, 2021).
[6] *Id.*

We reiterate our previous pronouncements on the above captioned Advisory Opinions issued to the Credit Card Association of the Philippines in 2019 and 2020 and the Union Bank of the Philippines in 2020.

Essentially, fraud investigation may be considered as a legitimate interest under Section 12 (f), considering the legitimate interests test:

> "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.
>
> 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."[7]

Hence, the disclosure of personal information, i.e., name, address, delivery address, email address, and mobile or other contact number, by online merchants, financial technology companies, digital payment platforms and telecommunications entities to credit card issuers or banks, or bank transaction details from one bank to another affected bank or electronic money issuer, for purposes of fraud investigation is allowed under Section 12 (f) of the DPA.

As to the disclosure of such personal information to law enforcement, regulatory, or investigative agencies, the same may find basis under Section 12 (c), where processing is necessary for compliance with a legal obligation, and/or Section 12 (e) on processing that is necessary to fulfill functions of public authority which necessarily includes the processing of personal data for the fulfillment of its mandate.

We likewise referred to the provisions of the Philippine Credit Card Industry Regulation Law which recognizes several instances where credit card issuers may disclose data of cardholders.

Shared database of suspected and blacklisted accounts; fair and lawful processing; privacy impact assessment; data subject rights; limitations

Blacklisting was discussed in our Advisory Opinion No. 2017-63,[8] to wit:

> "As a generic approach, blacklists are databases that consist of collected specific

[7] National Privacy Commission, NPC Advisory Opinion No. 2020-039 (Oct. 30, 2020) citing NPC Case No. 17-047.
[8] National Privacy Commission, NPC Advisory Opinion No. 2017-063 (Oct. 9, 2017) citing Article 29 of Directive 95/46/EC "Working document on Blacklists", Adopted on 3 October 2002, available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp65_en.pdf

> information relating to a specific group of persons, which may generally imply adverse and prejudicial effects for the individuals included thereon and which may discriminate against a group of people by barring them access to a specific service or harming their reputation.
>
> That said, blacklisting constitutes processing of personal data and is therefore subject to the general data privacy principles set out in the Data Privacy Act of 2012 (DPA). Thus, the law mandates that a data subject must be properly informed of the nature, purpose and extent of the processing of his or her personal data.
>
> Further, it is mandatory for an organization to clearly establish procedures that allow data subjects to exercise their right to access, rectification, erasure or blocking."

While we recognize that having a shared database for KYC, EDD, and AML purposes may enhance the integrity of the financial system, we also note that this may have significant legal effects on the rights and freedoms of data subjects included in the database.

Hence, there is a need to ensure that personal and sensitive personal information (collectively, personal data) is processed fairly and lawfully.[9] In this particular context, we emphasize that personal data in such database must be accurate, relevant and, kept up to date – inaccurate or incomplete data must be rectified, supplemented, destroyed or their further processing restricted.[10]

We likewise recommend the conduct of a privacy impact assessment (PIA) to identify, assess, evaluate, and manage the risks represented by the processing of personal data in the shared database.[11] Guidance for conducting PIAs may be found in our website at this link: https://www.privacy.gov.ph/wp-content/files/attachments/nwsltr/NPC_AdvisoryNo. 2017-03.pdf.

Finally, we remind the financial services industry that data subjects should be provided mechanism to exercise their rights. Needless to say, these rights are not absolute and may be duly limited when necessary for public interest, protection of other fundamental rights, or when the processing of personal data is for investigations in relation to any criminal, administrative, or tax liabilities of a data subject, among others.[12]

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.) IVY GRACE T. VILLASOTO
OIC – Director IV, Privacy Policy Office

[9] Data Privacy Act of 2012, § 11 (b).
[10] *Id.* § 11 (c).
[11] National Privacy Commission, Guidelines on Privacy Impact Assessments [NPC Advisory No. 2017-03] (July 31, 2017).
[12] National Privacy Commission, Data Subject Rights [NPC Advisory No. 2021-01] (Jan. 29, 2021).