Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/10541
DOI URL: http://dx.doi.org/10.21474/IJAR01/10541

RESEARCH ARTICLE

HOW TO BE RISK-FREE IN DOING ONLINE TRANSACTIONS

Mark Stephen A. Guevara[1], Irene J. Rivera[2] and Charles M. Alano[2]

1. M.H. del Pilar Campus, Valencia St. near R. Magsaysay Blvd. Sta. Mesa, Manila, Philippines.
2. College of Business Administration Graduate School, Polythecnic University of the Philippines.

Manuscript Info

Manuscript History
Received: 17 December 2019
Final Accepted: 20 January 2020
Published: February 2020

Abstract

This paper discussed the in deeper manner the Data Privacy Act 2012. The following sections of the Act have been cited in the paper: its scope, the roles of National Privacy Commission, processing of personal information, implementing guidelines for processing personal information, the penalties and the extent of liability. This also discussed what risk of fraud is when transacting online and the different types of fraud one might possibly experience. Further, some financial institutions and e-wallet in the Philippines who have been practicing Data Privacy have been cited.

Introduction:-

The gradual acceleration of technological innovations empowers the customers more to transact online. From conversing online thru e-mails, messenger, viber, hangouts, social media and the like to purchasing items thru different media, personal information or even the sensitive personal information has to be stored by the system.

Even if this fasten the transactions and saves time, customers should not be at ease if they are not sure of the safety and security of the transaction they are taking. Just like how different establishments such as banks, malls, hotels and need security guards to ensure its safety, customers who are doing online transactions should also be knowledgeable of his/her rights to protect his personal information.

That is why, it is important for consumers to understand what is Data Privacy Act (DPA) 2012 and its importance to the people of the Republic of the Philippines to ensure the security of the information being shared, either online or offline. This paper discusses the different threats and risks when doing online transactions; and the role of Data Privacy Act 2012 in terms of securing one's financial information.

Understanding the Data Privacy Act 2012

Data Privacy Act (DPA) 2012 was passed by the House of Representative and the Senate on June 6, 2012. The Act is a policy of the state that primarily governs the security and the protection of ones' personal information, sensitive personal information, and fundamental human rights. Further, the Act facilitates growth and innovation while ensuring privacy in communication.

Data Privacy Act is majorly ruled by Information and Communications Systems Technology as it has an important role in the safeguarding of the personal information, both from the government and private sector. Information and Communications Technology receives, stores, generates, sends and processes data that has been recorded, or transmitted.

Corresponding Author:- Mark Stephen A. Guevara
Address:- M.H. del Pilar Campus, Valencia St. near R. Magsaysay Blvd. Sta. Mesa, Manila, Philippines.

The following should be considered before accessing the data or processing the information: (1) there should be a consent from the person who owns the information; (2) data should be freely given and there should be a clear indication of one's own volition; (3) the person should have agreed on the process or the means of collecting his personal information; (4) evidence of the consent either thru writing, electronic or recording should be present; and (5) should there be an agent involved, a consent in behalf of the owner should be presented.

As DPA ensures the security and protection of our personal information such as race, origin, health, marital status, education, legal cases, social security system number, bank account numbers, license, tax returns, credit card and loan information and the like, the entity or group handling our personal information must be guided and governed. At the same time, it is also our responsibility to know our rights and responsibility in sharing our information to other entity.

Scope of Data Privacy Act 2012

DPA ensures the protection and security of all types of information processed, either by a private sector or government sector. Furthermore, the Act protects and secures all the information processed using the technologies inside the country. These are being ruled by the National Privacy Commission.

Roles of National Privacy Commission

The National Privacy Commission (NPC) implements and monitors the provisions of the Act. Aside from monitoring, they too, ensure the compliance of the different sectors, groups and even individuals to the implementing guidelines. NPC also initiates investigations once complaints or reports are received.

Aside from the aforementioned, National Privacy Commission also acts as a Collegial Body, which means that it has the power to enforce a permanent or temporary ban, if the group or individual has failed to comply to the provisions of DPA (proven unlawful acts).

Moreover, NPC has the power to evaluate, accept, discard and require entities to amend their privacy codes to ensure the security of the personal information being collected. Lastly, the commission provides support and assistance in addressing issues or concerns associated to privacy.

Processing of Personal Information

It is important to know the do's and don'ts in processing personal information to avoid legal disputes and maintain one's lawful standing. The following sections will discuss more in detail how personal information should be processed, the guidelines in processing personal information, the righs of the owner of the personal information (data subject), security of both personal and sensitive personal information, accountabilities and liabilities, and the different penalties awaiting once defiance or rule infringement.

General Data Privacy Principle

Generally, personal information should be collected because for a valid or authentic reason or purpose. At the same time, personal information, as sacred as it is, should be treated lawfully and be used accordingly.

Data that is incomplete, unncessesary and is inaccurate should be disposed and be destroyed properly. This is so, it will not be the reason for confusion and at the same time, will not cause any issues or concern in the future.

Additionally, data collected should have clear retention rate, to allow more incoming data be safely stored. Collecting and storing data for a very long time may result to shortage in storage, thus, resulting to poor security of information.

Implementing Guidelines or Regulations for Lawful Processing of Personal Information

Any entity or individual should collect one's personal information in accordance to the following criteria : (1) there should be a permission coming from the individual who owns the personal information or data being processed; (2) collected or acquired data has a fundamental role in fulfilling any agreements or contracts made; (3) the processing of the personal information or personal data is necessary in carrying-out any legal measures to address any legal cases or obligation; (4) the processing of the personal data plays a detrimental role in protecting one's life and health; and (5) acquiring or processing of personal information is needed in addressing national issues or emergencies.

Rights of the Owner of the Personal Information
Any rightful owner of any personal information or data being processed should be informed that such is taking place. They have the right to be provided with the copy of the information being encoded on the system, and the purpose of the data collection and gathering should be made known to them.

Also, the ways and means of collecting one's personal information should be disclosed to the person, and the entity or person accountable to the information gathered should also be disclosed to the rightful owner of the data. It is in this manner that the controller give what is due to the owner of the information.

Similarly, the owner of the personal information or also known as data subject should know the existing of such rights.

Security of the Personal Information
Personal information acquired must treated accordingly and used properly to assure the data subject that its in responsible hands. The controller must ensure that there is an implementing guidelines to maitain the confidentiality of the information acquired and protect against the following: (1) unintentional or illegal obliteration; (2) unlawful disclosure; (3) illicit accessing or procesing; (4) forged use; (5) and illegal or unauthorized use of computers to access data or information.

Likewise, personal information controller must have a regular monitoring to protect its systems from illegal breaches. If a third party is involved, they must supervised to ensure their compliance to the provisions of the Act.

Most importantly, once the security has been breached, the National Privacy Commission must be informed immediately by the controller to avoid further casualties.

Accountabilities for Transfer of Personal Information
Personal information controller must make it clear who the accountable person is in terms of securing the personal information. This is important to ensure proper accountabilities and to ensure that each data collected is properly treated. Also, this is to guarantee the compliance to the regulations of Data Privacy Act 2012.

Security of Sensitive Personal Information in Government
With the government sector, each Head of Different Agencies are responsible for securing the safety of the handful of personal information acquired.

It is worth notetaking that any government employee, who doesn't have any aurthorization, shall not be given any acccess to the database of personal information.

Unauthorized access by any individual or entity shall be given a penalty depending on the severity of his/her offense. The latter shows the different types of penalties one can receive if there is a failure in the complying to the provisions of the Act.

Penalties:
The following are the penalties laid by the court and can be given to anyone who will violate the Act.

Unlawful Act	Imprisonment	Fine
1.Unauthorized processing or personal information	Ranges from one (1) year to three (3) years	Not less than five hundred thousan pesos (500,000) but not more than two million pesos (2,000,000)
2.Unauthorized processing of sensitive personal information	Ranges from three (3) years to six (6) years	Not less than five hundred thousan pesos (500,000) but not more than four million pesos (4,000,000)
3.Accessing personal information due to negligence	Ranges from one (1) years to three (3) years	Not less than five hundred thousan pesos (500,000) but not more than two million pesos (2,000,000)
4. Accessing sensitive personal information due to negligence	Ranges from three (3) years to six (6) years	Not less than five hundred thousan pesos (500,000) but not more than four million pesos (4,000,000)
5.Improper disposal of personal information	Ranges from six (6) months to two (2) years	Not less than one hundred thousan pesos (100,000) but not more than five hundred thousand pesos (500,000)

6.Improper disposal of sensitive personal information	Ranges from one (1) year to three (3) years	Not less than one hundred thousan pesos (100,000) but not more than one million (1,000,000)
7.Processing of personal information	Ranges from one (1) year and six (6) months to five (5) years	Not less than five hundred thousan pesos (500,000) but not more than five million (5,000,000)
8.Processing of sensitive personal information	Ranges from two (2) years to seven (7) years	Not less than five hundred thousan pesos (500,000) but not more than two million (2,000,000)
9. Unauthorized acess or intentional breach	Ranges from one (1) year to three (3) years	Not less than five hundred thousand pesos (500,000) but not more than two million pesos (2,000,000)
10.Concealment of security breaches involving sensitive personal information	Ranges from one and a half years (1.5) to five (5) years	Not less than five hundred thousand (500,000) and one million pesos (1,000,000)
11. Malicious disclosure	Ranges from one and a half years (1.5) to five (5) years	Not less than five hundred thousand (500,000) and one million pesos (1,000,000)
12. Unauthorized personal information disclosure	Ranges from three years (3) to five (5) years	Not less than five hundred thousand (500,000) and one million pesos (1,000,000)
13. Unauthorized sensitive personal information disclosure	Ranges from three years (3) to five (5) years	Not less than five hundred thousand (500,000) and two million pesos (2,000,000)
14. Combination of Series of Acts	Ranges from three years (3) to six (6) years	Not less than one million (1,000,000) pesos but not more than five million pesos (5,000,000)

Extend of Liability

First and foremost, any individual or organization who failed to follow the provisions of the Act. Secondly, if the violator is a juridical person, then his/her rights may be revoked. And, if the offender is not a Filipino citizen, he or she will be deported immediately; penalty shall also be imposed to him/her. Lastly, if the violator is a public official, a temporary or perpetual disqualification from his designation may happen.

Online Frauds and How to Address Them

In this fast-paced, technological-driven world, transacting online is what common with most consumers. Saving themselves from the hassle of going to the different establishments (store, banks and others), they can just place their orders and settle the payments online. The following will discuss the different types of fraud happening in the online world, and how some of the leading financial institutions addressed this issue.

Risk of Fraud

Unauthorized personnel can easily have access on one's accounts once they got the right password and were able to answer the security questions provided by the account owner. One danger of online transactions is that no system will verify the person accessing the account as long as the right pieces of information were input to the sytem.

Due to the two (2) major system glitches that happened to the big banks in the Philippines, Bank of the Philippine Islands (BPI) and Banco De Oro (BDO), banking secuirty has been the talk of the town. The representatives from the two banks were even asked to present to the Senate how they can improvise their system security and assure its clients that their personal information are protected.

To fully understand this concept, the following are the different types of credit card fraud one can possibly experience:

Lost Cards – once your card has been stolen, it is a must to report it immediately to avoid major damage.
Account Takeover – the fraudster, who got a hold of the carholder's personal information, could report to the bank that the card has been stolen thus a new card will be released under the victim's name.

Counterfeit Cards – this happen when the card has been cloned, thus giving the fraudester an opportunity to do illegal purchases.

Card-Present (CP) Fraud – this type of fraud is experienced when there is a collusive act between the establishment and fraudesters where the card is being swiped twice – first swipe is to settle the payment and the second swipe is to collet the information of the cardholder.

Card-Not-Present (CNP) Fraud – this type of fraud does not require the presence of the card, but only the card verification code, which make it necessary for everyone to scrutinize closely any transactions he/she is going to take.

Thus, it's important for most e-wallets and banking institutions to improvise their security system to assure the customers of their online security. To name a few, BDO, Security Bank and Paypal have released communication to their clients on how they can protect themselves from online fraud, and how they, as the account holder, can protect one's personal information. The following will discuss how these banks extended their fraud pretection protocol.

Fraud Protection Protocol Banco De Oro (BDO)
Due to the increasing cases of credit card fraud, BDO has called on a first-rate countermeasure that will address the issue. BDO has appointed one of the best leading software that focuses on analytics and decision management to effectively deal with debit cards fraud.

FICO's Falcon Fraud Manager is a software solution that has the capability of protecting accounts from fraudesters by analyzing the different transactions in comparison to the fraud analytics on a real-time basis. In this regard, customers have taken into more consideration the use of online bankings, thus garnering a bigger returns to BDO.

Due to this leap, BDO has stayed true to its commitment in protecting its customers so they can enjoy the privilege it offers such as uncomplicated, undemanding, risk-free manner of both online and store-purchases.

Fraud Protection Protocol of Security Bank
If Banco De Oro has tapped FICO's Falcon Fraud Manager, it is worth notetaking that Security Bank is protected by Tranport Layer Security or TLS. This is the reason why Security Bank customers are assured that their website and online banking are risk-free.

Proof of TLS can be seen in the browser. Thus, customers are highly encouraged to be keen when using browser in transacting online. However, ensuring online security need a collaboration between the financial institutions and of the cardholders. The following are ten (10) key reminders published in the website of Security Bank for their customers to ponder upon:

Passwords must be kept confidential all the time. It is higly recommended to use number that are not associated or has no connection with the customer. Never use TIN, SSS number, birth date, or any User ID as these have bigger possiblity of being generated upon. Also, it is highly advisable to just memorize the passwords than to save it in the mobile due to the threat of being hacked. Lastly, password should be changed regularly.

Don't forget to log off once the session is over. Logging off immediately once the transaction ended will prohibit further transactions from taking place. Also, this will protect your account from unauthorized access from a different personnel.

Never input your personal information to unsecured sites. Don't trust suspected websites to prevent future casualties.

Avoid using less-trusted computer/device. As much as possible, do not use public or shared devices. However, in cases that it cannot be avoided, it is important to always clear the browser cache to make sure that no information or data will be stored.

Don't get used to using public wireless networks. Most consumers are unknowingly becoming victims of fraud because they, most of the time, take advantage of the free wifis in the malls and other establishments that make them vulnerable to malicious attcks.

Always clear the browsing history after every transaction to make sure that no data has been stored in the computer or device used (especially if it is a public or shared computer).

Protect your device with a trusted softward. Installing antivirus or any software that will protect the computer and any device from being attached by malicious softwares will not cost much. Also, by doing so, the level of security of one's personal information will increae.

Regular checking of one's account will also increase the level of security of one's personal information. Keeping track of every transaction made will help one detect any unauthorized transactions that might have taken place.

Always update the bank who holds your account your latest contact details to make it easy for them to get a hold of you. Nobody would want to miss any updates regarding their accounts.

Should there be any unusual changes or unauthorized transactions made, immediately contact the bank that handles your account. In doing so, the hope of reducing any possible casualties may still be avoided.

Indeed, it is important to be knowledgeable with the do's and don'ts of online transactions to ensure the security of one's account. The TLS of Security Bank and its 10 key reminders to its customers have helped them raise the level of security of thousands of accounts they are managing.

Fraud Protection of GCash: A BSP-licensed e-money issuer and remittance agent

Just for a very short time (nine year of existence), GCash has already been awarded by Bangko Sentral ng Pilipinas (2019) with the following awards: (1) Outstanding Partner for Digital Transformation and (2) Outstanding Partner for Innovative Financial Services during the BSP 16th Awards Ceremony. Up to date, it has already over twenty (20) million users with more than sixty-three (63) thousand partner merchants all over the Philippines.

As this is also cater another type of online transaction, GCash has also a program called Customer Protect that promises no user will be held responsible should there be any unauthorized transactions made from the user's account. Here's how it works:

GCash ensures that they have the right system capable of analyzing any transaction taking place and prevent any fraudaulent activity from happening. They make sure that they have the team that closely monitors all of the transactions to avoid risks and promotes friendly-usage.

GCash assures its customers that immediate investigation will take place upon receipt of the report. It's lead time is one (1) day, thus guaranteeing a feedback/solution from the team within 24 hours. Once unusual transacations have been noticed, customers are advised to contact GCash Support team thru their Help Center, hotline or email.

It also guarantees its customers that its money will be given back once unauthorized transactions in one's account has been proved. Any proof such as screenshots or other documentations is needed for faster investigations and problem resolution.

Just like any other financial institutions such as BDO and Security Bank, GCash has made sure that it caters its customers the security and protection they deserve.

Conclusion:-

It is important for anyone to first know whatever it is he/she is getting into before taking any action. This paper has just only discussed some of the financial institutions that has security protocols that ensures the safety of its customers' personal information. As a customer, it is vital to assess if the bank, e-wallet or site you are dealing with is protected to avoid risk of fraud and other threats one may come across with.

More importantly, having deeper understanding of the Data Privacy Act 2012 will allow one to shield himself/herself from different threats concerning data privacy. As this paper aims to give knowledge to its readers the different risks of online transactions, it also hopes to equip them with the individual responsibilities to ensure the safety of his/her personal information.

Lastly, it is important to remember that a cooperation between the cardholder and the account owner greatly increases the security of one's personal information. Knowing will not cost you much, but surely, not knowing will cost you a lot.

References:-

1. Anonymous, (2019). BDO deploys world-class countermeasure vs debit card fraud. Retrieved October 15, 2019 from https://www.bdo.com.ph/news-and-articles/bdo-deploys-world-class-countermeasures-vs-debit-card-fraud
2. Anonymous, (2019). GCash customer protect. Retrieved October 20, 2019 from https://www.gcash.com/customerprotect
3. Gastl, M. (2017). What banks failed to mention about credit card fraud. Retrieved October 15, 2019 from https://www.moneymax.ph/credit-card/articles/banks-credit-card-fraud/
4. Lim, A. (2019). Credit card fraud happens, but don't let it happen to you. Retrived October 20, 2019 from https://news.abs-cbn.com/business/02/25/19/credit-card-fraud-happens-but-dont-let-it-happen-to-you
5. Nikolakopulos, A. (2017). Risks in Eletronic Payment Systems. Retrieved October 15, 2019 from https://bizfluent.com/info-7836297-risks-electronic-payment-systems.html
6. Security Bank Team (2017). Financial Blog. How to Protect Yourself from Online Fraud. Retrieved October 16, 2019 from https://www.securitybank.com/blog/protect-yourself-from-online-fraud/.