International Journal of Innovation, Creativity and Change. www.ijicc.net
Volume 10, Issue 5, 2019

# Implementation of Confidentiality and Data Security in the Execution of the Lending and Borrowing Money Service Based on Information Technology in Indonesia

**Sri Wahyuni[a],** [a]Lecturer in Civil Procedure Law Faculty of Law, University of Bhayangkara, Jakarta Raya, Email: [a]sri.wahyuni@dsn.ubharajaya.ac.id

The development of information technology has had an influence on various fields in Indonesia, especially on developments in the field of information technology lending and borrowing services known as Financial Technology (Fintech). However, many people are unaware that borrowing and borrowing money using these applications actually has a negative impact when the debtor experiences default, so the financier commits defamation, or harassment of women's honour, including violations of human rights. This is contrary to the principle of confidentiality and security of user data. Regarding these principles regulated in Article 29 letter d OJK Regulation 77 / POJK.01 / 2016 concerning information technology lending and borrowing services and Article 4 letter g OJK Regulation Number 13 / PJOK.02 / 2018 concerning digital financial innovation in the financial services sector, and Article 31 OJK Regulation Number: 1 / POJK.07 / 2013 concerning Consumer Protection in the Financial Services Sector, the purpose of this study is the implementation of the confidentiality and data security principles of customers who borrow money through the online platform in Indonesia. This research uses the normative legal research method. The results of the study were to find out about the implementation of the principles of confidentiality and data security of debtors in the operation of lending and borrowing services through Illegal Fintech and settlement of disputes in Indonesia.

**Key words:** *Consumer Protection, Confidentiality and Data Security, Fintech.*

**Background**

The development of information technology currently affects many things in human life, one of which is in the field of information technology based lending and borrowing services[1], the ease of borrowing and borrowing money through online services seems to be one of the trends for obtaining loans through a quick and easy process. This is certainly the main attraction for the community when they need some money to meet their daily needs or other needs.

However, quite a number of people are not aware that loans using online applications actually have a negative impact when the borrower or debtor experiences defaults or breach of contract. The debtor experiences defamation, or harassment of women, including violations of Human Rights (HAM). One example occurred on July 25, 2019, in the case of a woman in Solo with the initial YI claiming to use an online loan because she was in need of money for her children's education. She knew about the online loan information via a short message to her cell phone. The requirements for applying for an online loan are quite easy; among others, they include a photo of yourself and an identity card. Application platform on the smartphone screen appears to give a permission request to access the phone contacts, cameras and galleries. After agreeing to all the Fintech Incash loan terms, YI also tried to apply for an online loan of Rp 1,000,000, but after deducting administrative costs the total loan received was around Rp680,000. The loan must be returned within one week to Rp1,054,000. When it was due, YI apparently could not repay the loan. YI has spoken kindly to the Incash debt collector about her problem. Interval a day later, she began to receive terror by text messages which sent billing to all her contact numbers on her phone. After that, Fintech Incash made a poster that harassed her and distributed it to the WhatsApp group. In the poster was an advert which became viral where a woman named YI gave an offer; which was willing to do sex for Rp. 1,054,000 to repay her debt in a Fintech application called Incash[2]. In the advertisement, YI also guarantees satisfaction for those who use her services. YI very shocked about that

[1] The following is the opinion of the experts: Haag & Keen (1996) information technology is a set of tools that help work with information and perform tasks related to information processing. Martin (1999) information technology is not only limited to IT (Hardware and Software) that is used to process and store information, and also includes communication technology that sends information. Williams and Sawyer (2003) IT is a technology that combines computers with high-speed communication lines that can carry data, voice and video. Lucas (2000) Information Technology is any form of technology that is applied to process and transmit information in electronic form. Oxford Dictionary (1995) Information Technology is the study or electronic equipment, especially computers, to store, analyze, and distribute information, including words, numbers, and images. Gurupendukasi.com, Partasetiawan, Understanding Information Technology - Sorry, Basics, Concepts, Grouping, Experts, https://www.gurupendukasi.co.id/peng understanding-teknologi-informasi/

[2] Merdeka.com - The Financial Services Authority (OJK) ensures INCASH online loan company (Fintech) suspected of defamation of customers is illegal. OJK Confirms Illegal INCASH Online Loan Companies, Thursday, July 25 2019 17:51 Reporter: Arie Sunaryo, https://www.merdeka.com/peristiwa/ojk-certain-company-lending-online-incash-ilegal.html

hoax advertisement. Then, she asked her friend who were in the whatsapp group to leave the group. YI immediately called her friends to leave the group. Meanwhile YI's attorney from LBH Solo Raya, I Gede Sukadewana Putra has reported the case to the police. Not only that, she also reported the case to the Ministry of Women's Role, Ministry of Communication and Information, Ministry of Law and Human Rights and YLKI. That it is not true if YI offered sex service for money. Source Liputan6.com, Solo.

Another case occurred on July 29, 2019, SM borrowed money through various online applications for Rp. 5 million. The money was to be used for business. But because of not having a permanent job, SM finally went into arrears to pay the loans for up to 2 months. The loan is only Rp. 5 million from several applications, 2 months later it becomes Rp. 75 million. The details consist of fines, fees for extending the tenor and interest. In addition to debt and interest rates to swell, they also get terror for being late in making payments. LBH Solo Baru, Sukoharjo has reported the case to the Surakarta Police. It also includes a number of online loan evidence tools. A number of pieces of evidence included in the form of screenshots of defamation, blasphemy, recordings, pictures that are related to the case and others. Source Merdeka.com, 29 July 2019.

The imposition of high loan interest rates does not match the loan interest rates set by Bank Indonesia, the imposition of high fines when debtors experience delays in repayment payments, collection time that does not have the limitation plus the threat of terror, violence, humiliation, defamation, spreading personal photos or videos, some of these things are the confidentiality of personal data of customers or debtors because these online loans do not have official permission from the Financial Services Authority (OJK) which is an independent institution free from interference from other parties that have functions, duties and supervision, inspection and investigation of all activities in the financial services sector from the banking sector, capital market and non-bank financial services sectors such as insurance, pension funds, financial institutions, Fintech and other financial service institutions. This is of course detrimental to the debtor and is contrary to the principles of confidentiality and user data security.

Through the principle of confidentiality and data security, information technology-based loan lenders and users in accordance with Article 29 letter d OJK Regulation 77 / POJK.01 / 2016 concerning information technology-based loan services and Article 4 letter g OJK Regulation Number 13 / PJOK.02 / 2018 concerning digital financial innovation in the financial services sector and Article 31 of the OJK Regulation Number: 1 / POJK.07 / 2013 concerning Consumer Protection in the Financial Services Sector, in addition to that, it needs a rule in the form of a law regarding Fintech which is an integral part of the conventional banking system and sharia-based information technology by taking into account also the prudential aspects, data security, consumer protection and good corporate governance (Bank Indonesia

Regulation (PBI) number 8/4 / PBI / 2006)[3] and how the system of supervision of the implementation of Fintech activities. This will provide business actors and financial service users with protection (POJK No. 1 / POJK.07 / 2013).[4]

Some of the previous studies written by Basrowi, his research on the first forms of consumer protection in the use of Fintech through two ways namely Preventive and Refressive, which is meant by preventive legal protection. This is legal protection that aims to prevent disputes by applying the basic principles of legal protection for users of Fintech services, regarding these principles which are regulated in Article 29 POJK Number 77 / POJK.01 / 2016 concerning Information Technology based lending and borrowing services, including the principles of transparency, fair treatment, reliability, confidentiality and security of data and simple user dispute resolution, fast and affordable cost. Whereas Refressive protection is protection whose purpose is to resolve disputes. If the lender as the injured party has the right to receive compensation from the borrowing party, but if it does not reach an agreement, the lender can carry out the settlement of the dispute outside and in court as regulated in Article 39 paragraph 1 POJK Number 1 / POJK.07 / 2013 concerning Protection financial service consumers that dispute resolution outside the court can submit their requests to OJK to facilitate the resolution of consumer complaints that have been harmed by financial service actors, namely the Fintech service providers.

Second, prevention efforts that can be done so that Fintech organisers do not misuse applications by giving an obligation to report to OJK, this is in accordance with Article 5 of Law Number 21 Year 2011 concerning the Financial Services Authority which states that OJK functions to organise a regulatory and supervision system which integrates all activities in the Financial Services sector.

The three roles of BI, OJK and Kemenkominfo, BI plays the role of Regulator and Supervisor of the payment system, OJK plays the role of supervising the marketing of Fintech products and services through online media, the Ministry of Communication and Information conducts supervision in terms of Information Technology Specifically the protection of consumer personal data (cybersecurity) and markings digital signature payment (Basrowi, 2019).

---

3 Based is a bank governance that applies the principles of transparency, accountability, responsibility, independence, and fairness. fairness). Whereas for sharia banks, the terms and regulations are stipulated through PBI Number 11/33 / PBI / 2009, which covers Sharia Commercial Banks and Sharia Business Units. These basics are used as a guide in carrying out the duties and responsibilities carried out by the Board of Commissioners, Directors, Committees and work units of a bank institution.

4 This provision especially applies to PUJK which has been monitored by OJK and implemented Fintech services. The PUJK must pay attention to all aspects of consumer protection by applying the principles stipulated in article 2, namely the principles of transparency, fair treatment, reliability, confidentiality and security of Consumer data / information, and handling complaints and resolving Consumer disputes simply, quickly, and costly affordable.

Previous research was conducted by Iswi Hariyani and Cita Yustisia Serfiyani. This study examined the legal protection and resolution of business disputes "Loan-based on Financial Technology" (PM-Tekfin). This research includes three things: OJK's role in PM-Tekfin's business development, forms of legal protection for PM-Tekfin's service users, and forms of PM-Tekfin's business dispute resolution. The results showed the OJK was authorised to regulate and supervise the PM-Tekfin business. OJK has also issued OJK Regulation number 77 / POJK.01 / 2016 as a form of legal protection for PM-Tekfin service users. PM-Tekfin's business disputes are expected to be resolved through Alternative Dispute Resolution (ADR) by forming an online Dispute Settlement institution (PSD) (Iswi and Cita, 2017).

Svetlana Saksonova and Irina Kuzmina-Merlino, (2017) in researching about the phenomenon of Fintech in the Latvian country, showed the results that respondents were generally unaware and did not understand about Fintech services in Latvia and their relationship with innovation and new financial products.

Arner, Barberis, and Bukley (2015) researched the development of financial technology since 2008 in developed and developing countries. The latest evolution of Fintech led by start-ups faces a variety of challenges for regulators, market participants, especially in balancing the potential benefits of innovation and the risks that may arise from new approaches. They analysed the evolution of Fintech over a period of more than 150 years and the basis of that analysis was against rules that were too early or rigid at the moment. The development of the Fintech sector attracted the interest of regulators who are currently evaluating the best way to support market development and ensure developments in the contributing, non-threatening sectors, core mandates such as systemic stability, consumer protection, and market competition.

With several cases of lending and borrowing through Illegal Fintech experienced by YI and SM debtors in Indonesia related to personal data protection of the debtor as the borrower when there is a delay in payment or default, the debtor experiences unfavorable treatment of defamation. Then the harassment and violation of human rights (HAM), so this research focuses on the Implementation of the Principles of Confidentiality and Data Security in Providing Money Lending and Borrowing Services[5] through Fintech in Indonesia.

[5] Regulation of the Financial Services Authority Number 77 / POJK.01 / 2016 2016 concerning Information Technology Lending and Borrowing Services and Bank Indonesia Regulation Number 19/12 / PBI / 2017 2017 concerning Financial Technology Implementation. Application-based loan services or information technology is one type of Financial Technology Implementation (Fintech) Other Financial / Financial Services category. In conducting its business, the organizer must submit registration and licensing to the Financial Services Authority (OJK).

The purpose of this study is to determine the implementation of the principles of confidentiality and data security in the provision of technology-based money lending and borrowing services in Indonesia.

The problems that will be raised in this study are:

1. How is the implementation of the principle of confidentiality and data security in the operation of lending and borrowing services based on information technology in Indonesia?
2. What is the protection for personal data of the Debtor when experiencing defaults on illegal or non-registered Fintech institutions in the OJK?

The research methods used in this study include the law approach (statue approach) and conceptual approach (conceptual approach). The statue approach is carried out by examining all laws and regulations related to the research focus. Conceptual approach (conceptual approach) departs from the views and doctrines that develop in the science of law.

**Discussion**

***Implementation of the principle of confidentiality and data security in the operation of information technology-based lending and borrowing services in Indonesia***

Financial Technology (Fintech) is a form of application of information technology in the financial sector. Juridically, the understanding of Fintech is found in Fintech's Bank Indonesia Regulation (PBI). Based on Article 1 paragraph (1) PBI No.19 / 12 / PBI / 2017 Concerning the Implementation of Financial Technology (hereinafter referred to as PBI Fintech):

> "Financial technology is the use of technology in financial systems that produces new products, services, technology and / or business models and can have an impact on monetary stability, financial system stability, and / or the efficiency, smoothness, security and reliability of payment systems."

The Government through the Bank of Indonesia and the Financial Services Authority as the authority to regulate Fintech in accordance with technical regulations in regulations related to Fintech, including POJK No. 77 / POJK.01 / 2016 concerning Financial Technology-Based Lending and Borrowing Services (POJK Fintech), PBI No. 19/12 / PBI / 2017 Regarding the Implementation of Financial Technology (hereinafter referred to as PBI Fintech), PBI No. 18/40 / PBI / 2016 Regarding the Implementation of Payment Transaction Processing, PBI No. 11/12 / PBI / 2009 Regarding Electronic Money, which has been amended in PBI No. 16/8 / PBI / 2014.

***Acquisition and Collection of Personal Data***

Acquisition and collection of personal data by electronic system providers must be limited to relevant information and in accordance with the objectives. It must also be done accurately. Electronic system operators need to respect personal data that is privacy.[6]

Acquisition and collection of personal data is carried out in accordance with the consent of the owner of the personal data or the provisions of the legislation. When the owner of personal data does not give consent to disclose the confidentiality of personal data, then everyone who acquires and collects personal data and organisers of electronic systems must maintain the confidentiality of personal data.

Personal data[7] obtained and collected directly must be verified to the owner of personal data based on various data sources. The data source must have a legal basis. Electronic systems that are used to collect the acquisition and collection of personal data must have interoperability and compatibility capabilities and use legal software.

***Processing and Analysing Personal Data***

Personal data can only be processed and analysed according to the needs of the electronic system provider, which has clearly been stated when obtaining and collecting personal data. Then, the processing (Minister of Communication and Information Regulation No. 20 of 2016)[8] and analysis must be done with approval, except if the personal data comes from personal data that has been displayed or publicly announced by the electronic system for public services. Personal data that is processed and analysed must have verified its accuracy.

***Storage of Personal Data***

[6] Privacy is the right of individuals to control the use of information about personal identity either by themselves or by other parties. According to the ITE Law, Article 19

[7] The definition of personal data in article 1 point 22 of Law No. 23 of 2006 concerning Population Administration (UU-Adminduk), while the details of the definition of personal data according to the Law-Adminduk are as follows "Personal Data is certain personal data that is stored, maintained, and protected by the truth and protected by confidentiality." Regarding its protection, regulated in Article 2 of the Law and Administration. While the scope of personal data is regulated in article 84 of the Law-Adminduk, which is included in the personal data, among others: "Family card number (KK), NIK, date / month / year of birth, information about physical and / or mental disability, maternal NIK biological father, NIK, and some contents of the record of important events. In addition, article 84 of the Law and Administration imposes obligations on the state to protect and store personal data.

[8] Minister of Communication and Information Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems (PM 20/2016) in force since December 2016, protection of personal data includes protection of the acquisition, collection, processing, analysis, storage, appearance, announcement, transmission, dissemination, and destruction of data personal.

Personal data must be stored in an electronic system: in accordance with the provisions of the laws and regulations governing the obligation to store personal data for each supervisory agency and sector regulator; or no sooner than 5 years, if there are no statutory provisions that specifically regulate it.

Data centres and disaster recovery centres that provide electronic systems for public services used in the process of protecting personal data must be located within the territory of the Republic of Indonesia. Data centre is a facility that is used to place electronic systems and related components for the purpose of placement, storage and data processing.

A disaster recovery centre is a facility used to recover data or information and important functions of electronic systems that are disrupted by disasters caused by nature and or humans. If the personal data storage time has exceeded the time limit, personal data in the electronic system can be deleted unless the personal data will still be used or utilised in accordance with the original purpose of its acquisition and collection.

***Appearance, Announcement, Delivery, Dissemination and or Opening of Personal Data Access***

Displaying, announcing, sending, distributing, and / or opening access to personal data in the Electronic System can only be done: 1) upon approval unless otherwise specified by statutory provisions; and, 2) after being verified the accuracy and suitability of the purpose of the acquisition and collection of personal data. The sending of personal data managed by the Electronic System Provider to government agencies and regional governments as well as to the public or private parties domiciled within the territory of the Republic of Indonesia outside the territory of the Republic of Indonesia must: 1) coordinate with the Minister or the official / institution authorised for that and 2) apply the provisions of the regulations legislation concerning the exchange of personal data across national borders. Whereas for the purposes of the law enforcement process, the organiser of the electronic system is required to provide personal data contained in the electronic system or personal data generated by the electronic system at the request of law enforcement officials based on statutory provisions.

***Destruction of Personal Data***

Destruction of personal data in an electronic system can only be done if it has 1) passed the provisions of the period of storage of personal data in the electronic system based on the regulation or in accordance with the provisions of the legislation that specifically regulates in each of the supervisory agencies and sector regulators for that; or at the request of the owner of personal data unless otherwise specified by statutory provisions.

***Rights and Obligations of the Parties***

The owner of personal data has the right: 1) to the confidentiality of his personal data, 2) submit complaints in the context of resolving personal data disputes over the failure of protecting the confidentiality of his personal data by the electronic system provider to the Minister, 3) get access or opportunity to change or update his personal data without disturbing the personal data management system, 4) obtaining historical personal data that has been submitted to the electronic system provider, unless otherwise stipulated by statutory regulations and requires the destruction of certain personal data of his own in the electronic system managed by the electronic system provider.

Each Electronic System Operator must: 1) certify the electronic system it manages in accordance with regulatory requirements, and, 2) safeguard the truth, validity, confidentiality, accuracy, relevance and conformity with the objectives of acquisition, collection, processing, analysis, storage, appearance, announcement, delivery, distribution and destruction. personal data.

Then notify the owner of personal data in writing if there is a failure to protect the confidentiality of personal data in the electronic system under its management, with the provisions of the notification as follows: 1) it must be accompanied by reasons or causes of failure of personal data confidentiality protection, 2) it can be done electronically if the owner of the personal data[9] has given approval for that which is stated at the time of the acquisition and collection of personal data; 3) it must be ensured that it has been received by the owner of personal data if the failure contains potential losses for the person concerned; 4) written notice is sent to the owner of personal data no later than 14 days after the failure is detected; 5) have internal rules related to personal data protection in accordance with statutory provisions; provide a track record of audits of all electronic system implementation activities that it manages; 6) gives an option to the owner of personal data[10] regarding the personal data that he manages about can / cannot be used and / or displayed to third parties with the agreement as long as it is still related to the purpose of the acquisition and collection of personal data further provides access or opportunity to the owner of personal data to change

[9] Protection for personal data are regulated in legislation and regulations, namely Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law 2008) and Act Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Transactions Electronic (ITE Law 2016) Article 26 Paragraph 1 that unless otherwise stipulated by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the approval of the person concerned.

[10] protection for personal data are regulated in legislation and regulations, namely Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE Law 2008) and Act Number 19 of 2016 concerning Amendments to Law Number 11 of 2008 concerning Information and Transactions Electronic (ITE Law 2016) Article 26 Paragraph 1 that unless otherwise stipulated by statutory regulations, the use of any information through electronic media concerning a person's personal data must be carried out with the approval of the person concerned.

or update the data personal without disturbing the personal data management system, unless otherwise stipulated by statutory provisions; 7) destroy personal data in accordance with the provisions in this regulation or other statutory provisions that specifically regulate in each supervisory agency and sector regulator for it; and provide contacts that are easily contacted by the owner of personal data related to the management of his personal data.

***Dispute resolution***

Every owner of personal data and the organiser of the electronic system can submit complaints to the Minister for the failure to protect the confidentiality of personal data.

Complaints are handled according to the procedure, as follows: complaints are made no later than 30 working days since the complainant knows the information on the failure to protect the confidentiality of personal data; complaints are submitted in writing and must be supplemented with supporting evidence, officials / dispute resolution agencies must respond to complaints no later than 14 working days since the complaint was received that at least contained a complete or incomplete complaint, the incomplete complaint must be completed by the complainant no later than 30 working days since the complainant received the response then if it exceeds the deadline, the complaint is considered cancelled, and the official / the dispute resolution agency that handles complaints can provide recommendations to the Minister for imposing administrative sanctions on the Electronic System Operator even though the complaints can or cannot be resolved by deliberation or through alternative resolution efforts.

If efforts to resolve disputes by deliberation or through other alternative resolution efforts have not been able to resolve disputes, every owner of personal data and the electronic system providers can file a civil claim for failure to protect the confidentiality of personal data. If in the process of law enforcement by law enforcement officials in accordance with the provisions of the legislation the authorities must confiscate, then only Personal Data related to legal cases can be confiscated without having to confiscate the entire electronic system.

***Administrative Sanctions***

Every person who obtains, collects, processes, analyses, stores, displays, announces, sends, and / or disseminates personal data without rights or does not comply with the provisions in this regulation or other legislation is subject to administrative sanctions in accordance with statutory provisions in the form of: (a) verbal warning; (b) written warning; (c) temporary suspension of activities; and / or (d) announcements on sites in the network.

***Protection of personal data when the debtor experiences defaults on an Illegal Fintech institution or not registered with the OJK***

In Indonesia, Fintech is divided into two types, first Fintech Legal, namely Fintech registered with the Financial Services Authority, and secondly, there is Illegal Fintech, which is not registered with the Financial Services Authority. Relating to the protection of debtor's personal data when experiencing defaults on Fintech Legal institutions it is clearly regulated in the regulations of the Financial Services Authority, Bank Indonesia and the Ministry of Communication and Information. However, if there is a default on Illegal Fintech, then it has not been clearly regulated in the Financial Services Authority regulations or other regulations. This can lead to legal uncertainty for people who experience defaults in the Illegal Fintech case, this is caused due to lack of public knowledge and information about legal and illegal Fintech, so it needs serious support from various parties in order to form a regulation or legal umbrella to protect data personal debtor as a borrower so that there is legal certainty and the implementation of the principle of confidentiality and data security which is one of the human rights that must be protected.

**Conclusion**

The implementation of the principle of confidentiality and data security in the operation of information technology-based lending and borrowing services in Indonesia has been regulated in Financial Services Authority regulations and Bank Indonesia regulations. Protection of Debtor personal data when experiencing defaults through Illegal Finteches or those not registered with OJK does not yet have arrangements that need to be made a rule that regulates personal data in order to protect human rights.

## REFERENCES

Act Number 19 of 2016 concerning Amendments to Act Number 11 of 2008 concerning Information and Electronic Transactions.

Arner, Barberis, and Bukley, (2015). The Evolution of Fintech: A New Post Crisis Paradigm ?. University of Hongkong Faculty of Law.

Bank Indonesia Regulation (PBI) number 8/4 / PBI / 2006 concerning the definition of GCG in Banking.

Bank Indonesia Regulation Number 19/12 / PBI / 2017 2017 concerning Implementation of Financial Technology.

Basrowi, (2019). STEBI Lampung, Indonesia. Analysis of Aspects and Efforts to Protect Consumer Fintech Sharia, Lex Librum: Journal of Legal Studies, http://www.lexlibrum.id, Volume 5 Number 2 June 2019.

Financial Services Authority Regulation Number 77 / POJK.01 / 2016 2016 concerning Information Technology Based Lending and Borrowing Services.

Iswi, H. and Cita, Y. S. (2017). Legal Protection and Dispute Settlement of PM-TEKFIN Service Businesses, Journal of Indonesian Legislation, Volume 14 Number 03 September 2017.

Kausarian, H., Sri Sumantyo, J. T., Kuze, H., Aminuddin, J., & Waqar, M. M. (2017). Analysis of polarimetric decomposition, backscattering coefficient, and sample properties for identification and layer thickness estimation of silica sand distribution using L-band synthetic aperture radar. *Canadian Journal of Remote Sensing*, *43*(2), 95-108.

Kausarian, H., Sumantyo, J. T. S., Kuze, H., Karya, D., & Panggabean, G. F. (2016). Silica Sand Identification using ALOS PALSAR Full Polarimetry on The Northern Coastline of Rupat Island, Indonesia. *International Journal on Advanced Science, Engineering and Information Technology*, *6*(5), 568-573.

Kausarian, H., Batara, B., Putra, D. B. E., Suryadi, A., & Lubis, M. Z. (2018). Geological Mapping and Assessment for Measurement the Electric Grid Transmission Lines in West Sumatera Area, Indonesia. *International Journal on Advanced Science, Engineering and Information Technology*, *8*(3), 856-862.

Law Number 11 Year 2008 concerning Information and Electronic Transactions.

Minister of Communication and Information Regulation No. 20 of 2016 concerning Protection of Personal Data in Electronic Systems.

POJK No. 1 / POJK.07 / 2013 concerning Protection, Consumers of the Financial Services Sector.

Saksonova and Merlino, (2017). Fintech as Financial Innovation - The Possibilities and Problems of Implementation. European Research Studies Journal. Volume XX. Issue 3A. Pages 961-973. 2017.