Asia Pacific Fraud Journal
E-ISSN: 2502-695X, ISSN: 2502-8731
Volume 5, Nomor 1 (January-June) 2020
http://apfjournal.or.id/index.php/apf

ANALYSIS OF THE READINESS OF INDONESIAN PEOPLE AND REGULATIONS IN HANDLING FRAUD ON TECHNOLOGY EXPLOITATION

✉[1]Mustika Prabaningrum Kusumawati, [2]Ari Nur Rahman, [3]Panzi Aulia Rahman,
[4]Henry Adrian Sumule, [5]Endrojoyo Sigit Triyono
[1]Universitas Islam Indonesia
[2]Indonesia Eximbank (Lembaga Pembiayaan Ekspor Indonesia (LPEI)), Indonesia
[3]PT. PLN (Persero), Indonesia
[4]Alumni of Institut Teknologi Sepuluh Nopember Surabaya and
Institut Teknologi Bandung, Indonesia
[5]Head of the Inter Bank Transfer Reconciliation Departement, Indonesia

ARTICLE INFORMATION
Article History:
Received June 14, 2019
Revised July 03, 2019
Accepted June 18, 2020

JEL Classifications:
D73; E44; L32

DOI:
10.21532/apfjournal.v5i1.134

ABSTRACT
The development of information technology has a big influence in supporting business continuity among producers, consumers, distributors, and financial service institutions. The development of Financial Technology (Fintech) has now become a trend in modern society that follows the current developments. The positive side of technological development, especially in supporting fast and smooth financial services, can actually create a large gap in the readiness of the use of technology in the industrial revolution 4.0. Without strong preparation, this will increasingly create a big gap in the formation of the Fintech technology-based fraud chain. This paper discusses how a qualitative research using the grounded research model can find out the use of recht vacuum loopholes to commit fraud in the exploitation of technology. In addition, it also encourages the establishment of a regulation that supports the creation of a healthy Fintech ecosystem which is the main key in increasing Indonesia's economic growth. Factors influencing the occurrence of fraud include the lack of public knowledge about how to transact using Fintech, the looseness of applicable regulations, the arrogance of Fintech consumer in utilizing bug software Fintech to get profit as much as possible without thinking about legal consequences, the arrogance of the Fintech company in minimizing the large risks that will occur, and not maximum formation of the Fintech ecosystem with other traditional financial service institutions. The situation is exacerbated by the unavailability of the Whistleblowing System (WBS) through a complaint channel specifically for Fintech. The establishment of the Fintech ecosystem, with the adoption of an anti-fraud system as one of the factors that drive Indonesia's economic growth, can be done by creating a technology-savvy community, especially Fintech; making an integrity pact to support anti-fraud and anti-money laundering among regulators, the Fintech association, and the Fintech companies at the time of making official registration with the regulator; Regulators need to get rid of egotism between institutions by synchronizing verbally or nonverbally through technology channels that are automatically integrated between state institutions and preparing special channels for whistleblower systems or consumer complaints channel specifically for Fintech.

Keywords: *Fintech, Grounded Research Model, Recht Vacuum, Anti-Fraud, Whistleblowing system*

✉ Corresponding author :
Email : mustika.praba@gmail.com

1. INTRODUCTION

The development of information technology has a big influence in supporting business continuity among producers, consumers, distributors and financial service institutions. The development of financial technology (Fintech) has begun in the banking world since 1866, known as the Real Time Gross Settlement System (RTGS). Along with the growing business needs, there was a transition period of change from the era of analog technology to the era of digital technology from 1967 to 2008 which was marked by the emergence of automatic teller machines (ATMs) and SWIFTs which made it easier to transfer abroad. It was then followed by the era of internet banking along with the increasingly widespread internet network.

In the two eras of technological development, banking was still a pioneer in financial technology (Fintech) innovation. Since the increasingly widespread fiber optic and cellular internet networks, however, financial service institutions other than banking have begun to emerge and help smooth payment transactions within one country or between distant countries. The era began with the increasing use of smartphones which was then supported by financial product and service innovations such as *PayPal* and *Payoneer* which were still based on *Visa* and *MasterCard* network, and then followed by mobile phone and *user-friendly applications* such as *Venmo*, *Skrill*, *Stripe*, and *2 Checkout*. The internet giant like *Google* and e-commerce giant *Amazon* even issued similar applications called *Google Wallet* and *Amazone Payments*. In Asia, it began with the slogan of the e-commerce giant *Alibaba* from China, namely "*Embracing Secure, Multiple Use Cases, Anywhere, Reward, Technology (SMART) Living*" by issuing an *Alipay* payment application which was then followed by *Tencent* which started focusing on online communication services *WeChat* which then developed and presented *WeChat Pay*.

In Indonesia, the Fintech 3.0 and 4.0 began with increasingly heard slogans promoted by banking book IV such as "*Digital Banking*" and competing to make mobile phone banking applications in order to transact and make payments through the palm of the hand. In this era, however, banking has not become a major player in the payment sector. Even in Fintech sector with Online Lending type, banking is relatively slow compared to the growth of Fintech companies that are increasingly developing and in demand by consumers or the public in general. This condition is inseparable from the many regulations that supervise banking performance so as not to cause systemic losses.

Existing regulations in Indonesia refer to regulations issued by Bank Indonesia, the Ministry of Communication and Information, and the Financial Services Authority (OJK) as Fintech supervisors. One effort to provide a legal umbrella for the development of Fintech is the existence of the Regulation of Financial Services Authority (POJK) No.13 / POJK.02 / 2018 concerning *Digital Financial Innovation* (IKD). With the existence of this regulation, there are several Fintech registration mechanisms for startup companies (Non-Financial Services Institutions) and Financial Services Institutions in each of the banking, capital market, and Non-Bank Financial Industry sectors.

In fact, there are still some conditions that are the subjects of discussion in the developing Fintech service sector at this time. One of them is the impact or readiness perceived by banks that are classified in Book I and Book II as well as Rural Banks (BPR). In addition, special attention needs to be paid to Finyech consumers or the general public regarding the existing conditions and regulations for Fintech. It is necessary to consider the dangers or consequences that will be received by consumers when transacting at Fintech service providers, both registered and not registered with Bank Indonesia and the Financial Services Authority (OJK).

Another phenomenon is the lack of a complaints channel or Whistleblowing System (WBS) specifically for Fintech.

During this research, only 1 complaint channel related to Fintech was found since November 1, 2018, which was pioneered by the Legal Aid Institute (LBH), while the institutions or state institutions or associations still relied on consumer complaints channels in general. Based on information obtained by researchers in collaboration with several Legal Aid Institutions (LBH), the information obtained was approximately 3,400 complaints of Fintech violations in Jakarta, 30 complaints in Yogyakarta, 650 complaints in Surabaya until February 2019.

The current condition of Fintech development is like a diamond showing its beauty without seeing the being sacrificed. Therefore, it is necessary to add a Whistleblowing System (WBS) or consumer complaints channel specifically for Finyech into a Fintech ecosystem. Widespread offers to join a Fintech company with income above the average of other companies become a concern for employees who work at Fintech companies to report fraud acts that occur. According to Kusumawati et. all (2018), company employees are lazy to become whistleblowers because they are already in the comfort zone and are afraid of losing their jobs. So reports from whistleblowers or consumers as Fintech users are very reliable.

In creating security for customers and reducing the risk of loss to Fintech companies without obstructing the development of Fintech that has participated in supporting the rise of the Indonesian economy, there is a need for in-depth research that goes down directly to the field and interacts directly with Fintech customers personally. In addition, the research should include technology so as to be able to provide input to encourage the growth of the Indonesian economy through a healthy Fintech that is accommodated by new regulations or strategies that have been and will be issued by regulators in Indonesia.

This study aims to determine 1) The aspect of consumer awareness in utilizing the recht vacuum gap or the consumer's indifference toward applicable regulations is a major factor in the continued development of Fintech in Indonesia. 2) The level of behavior of Fintech companies and marketing employees who are trying to find a vacuum recht gap raises the intention to commit fraud. 3) Whistleblowing system or consumer complaints channel for Fintech can be effective in identifying fraud cases created by the Fintech ecosystem.

2. LITERATURE REVIEW AND HYPOTHESIS

Financial Technology (Fintech)

According to Amer et.all. (2016), financial technology (Fintech) is the use of information technology that aims to provide financial solutions by using innovation in improving services in the financial services industry. While the word "Fintech" itself has entered the Oxford Dictionary, that is, a computer program used to support or activate banking and financial services. The term fintech was first introduced by CitiGroup in the 1990s through the Financial Technology Services Consortium project in introducing the use of faster technology in banking financial services.

According to Arner (2016), Fintech has evolved in 3 periods: Fintech 1.0 from 1866 - 1967, Fintech 2.0 from1967-2008, and Fintech 3.0, 3.5 and 4.0 from 2008 to the present time. Fintech 3.0, 3.5 and 4.0, according to Rojko (2017), was the beginning of the industrial revolution in 2012 which was introduced by General Elektric by combining Big Data analysis with the Internet of Things (IoT). The types of Fintech are increasingly diverse such as *E-Commerce Payments, Mobile Banking, Mobile and Online Wallets, Peer to Peer (P2P) Lending, Crowdfunding, Supply Chain Finance, Digital / Virtual Currencies, Blockchain* and others.

Radio Frequency Identification* (RFID), *Near Field Communication* (NFC), and *Cyanogen Mod

RFID is a technique to identify an object using radio frequency spectrum which is then explained in detail in ISO / IEC 18000. The RFID technique can be used if an RFID frequency spectrum reader is available. A more modern technique that is becoming a trend among millennials is the use of smartphones that support NFC. NFC is a development or evolution of RFID technology. NFC is a two-way wireless interface device and is often referred to as contactless transaction technology. On smartphones that support NFC there are antenna and controller of the use of electric current as needed. On another occasion, the NFC antenna can still receive radio analog signals with a slight change in the algorithm through the system installed on the smartphone. In the active mode, NFC can be communicated with other NFC devices even with a barcode scanner and several Electronic Data Capture (EDC) devices that already support charging digital currency cards and debit cards as well as credit cards in the use of payments without *swipe magneting strips*. Based on the Regulation of the Director General of Resources and Postal Devices and Information Technology No. 1 of 2019, NFC spectrum is in the range from 13,553 to 13,567 MHz with a maximum transmit power of 10 meters.

Cyanogen Mod is a smartphone operating system that is open source and can be installed together with the Android smartphone system. *Cyanogen Mod* itself was officially stopped and renamed Lineage OS. Researchers still use the term *Cyanogen Mod* because the XDA Developers Android Forums are still familiar with the name of *Cyanogen Mod* which is then abbreviated as CM. CM itself was developed for non-profit by utilizing ideas from android developers across the world. The development is based on software such as the *kernel and firmware* which are open source and official from Android released by Google.

With a little creativity and intermediate knowledge about the use of Cyanogen Mod, someone who has a smartphone that supports RFID and NFC technology can easily commit fraud in getting information about credit card, debit cards, as well as transfer digital currency card balances without being read by PoS terminal core banking system of a bank. Such a condition creates fraudulent behaviors, in this case skimming and cloning, committed traditionally using a reader which is placed at an ATM. And it has been said to be a traditional act of fraud. Skimming and cloning have become easy to do. Even based on experimental results using an official smartphone from Android, someone can do it with a distance of 30 centimeters.

Financial Technology (Fintech) Ecosystem

The term ecosystem in Indonesian Dictionary means a special condition of the community of a living organism and the components of non-living organisms from an environment that interact with each other and the interaction of a reciprocal relationship. Thus, Fintech ecosystem will discuss about the various elements that interact with each other and provide mutual relations to support the growth of a healthy Fintech.

According to Welchek (2015) in Lee and Shin (2018), there are 5 elements that can support the formation of the Fintech ecosystem: Fintech Starups, Government, Technology Developers, Traditional Financial Institutions, and Financial Customers. Within the scope of financial services technology, a healthy and dynamic Fintech ecosystem which is anti-fraud culture can stimulate the growth of various sectors and be one of the supporting elements in local economic growth. It can also attract talented, ambitious people to generate creative and innovative thinking in supporting financial services business processes.

Recht Vacuum

Enforcement and application of law often collide with the development of society.

The development of society is always faster than the development of laws and regulations. The principle of legality is defined as a principle that can provide legal certainty, but the fact is that the sense of justice of the community cannot be fulfilled because it is the development of the society itself that is moving rapidly along with technological advances and the times. This is the reason why law and regulation cannot possibly regulate all aspects of people's lives so that it is inevitable that sometimes a law is unclear or incomplete which results in the recht vacuum in the community.

According to the Law Dictionary, recht (Dutch) objectively means law. Grotius in his book "*De Jure Belli ac Pacis (1625)*" states that "*the law is the rule of moral conduct that guarantees justice*". Whereas Van Vollenhoven in "*Het Adatrecht van Ned. Indie*" reveals that law is a symptom in the association of life that is constantly turbulent in a state of collision and banging endlessly with other symptoms.

Wignjodipuro (1971), in "*Pengantar Hukum*" (Introduction to Law) provides an understanding of the law that "*Law is a set of life rules that are coercive, containing an order, prohibition or permission to do or not do something and with a view to regulating order in people's lives*.". The life rules are both written rules in the legislation and unwritten rules in custom.

The Indonesian Dictionary (1989), provides the definition that emptiness is a matter (condition, nature, etc.) of emptiness. The definition of Vacuum (Dutch) based on the Law Dictionary is "empty or vacant". Narrowly, the "legal vacuum" is defined as a state of the absence of statutory regulations that govern, or it could also be said that this legal vacuum occurs because the things or conditions to be regulated by the regulation have changed or even if it has been regulated in a statutory regulation, it is still unclear or even incomplete. This is actually in line with the slogan which states that "the formation of a statutory regulation is always lagging or underdeveloped compared to events in the development of society.

Rect Vacuum (legal vacuum) has an impact in the form of *rechtsonzekerheid* (legal uncertainty) which will further lead to *rechtsverwarring* (legal chaos) in the sense that as long as it is not regulated it means that it is permissible, as long as there is still no clear procedure it means that it is not prohibited.

The Implementation of Anti-Fraud Culture through the Whistleblowing System (WBS) or Consumer Complaint Channels in the Formation of the Financial Technology (Fintech) Ecosystem.

The issue of the availability of a Whistleblowing System (WBS) channel or a consumer complaints channel has again become a concern in the development of the business world, especially the development of Fintech in financial services. Many literatures or studies have touched on the importance of the Whistleblowing System (WBS) in the formation of sound business processes. The benefit of the Whistleblowing System (WBS), as proposed by KNKG (2008), is that WBS can be an early warning system for fraud.

According to Kusumawati et. all (2018), until now the Law on Whistleblowing System (WBS) is still partial, so that it still refers to several legal umbrella of witness and victim protection, protection of reporters and witnesses in Money Laundering Crime as well as other regulations. The phenomenon of the absence of a special legal umbrella was answered again after the case of the dismissal of a private employee due to terror from the way of collecting loans online to the supervisor of the employee. But there was a case that became a major concern, in which a taxi driver at one of the leading taxi companies committed suicide because he was unable to repay his loans online and held back the shame because the people around him already knew and continued to get terror due to his loans.

3. METHODS

Research Method and Design

The research method used in this study is a qualitative method. The approach used by researchers is based on a grounded approach that sees a condition directly from the field, historical approach, and ethnographic approach.

Grounded Theory was first introduced by Glasser and Strauss (1965, 1967) in the social world, especially health. According to Fuady (2018), grounded research is a research model that determines generalization of empirical data based on field data so that concepts and categories are formed in determining the theory. In this grounded research, the first thing to look for is data in the field, and then a theory is found that is directly sourced from the data that has been found. Therefore, grounded research is qualitative in nature which seeks to describe and formulate a theory acquired (not to verify speculative theories or verify existing theories) but based on analysis and interpretation of facts and real data in the field which directly intersects social problems happening in society.

According to Liusvaara (2015), in order to guarantee that there is a match between the data and the theory produced, the grounded research process must meet four criteria: validation of real empirical field data, the researchers' overall mastery of the phenomenon under study, the process of generalization of the findings with other supporting contexts of the phenomenon under study, and controlling process by anticipating findings that may not be in accordance with the findings or previous theories of other parties. In supporting the fulfillment of these criteria, it is necessary to do a technique or a series of tiered research such as open coding data, axial coding data, selective coding data, the process of memoing, theorizing, integrating, conceptualizing, shorting which will produce categories, and data-based or big data based-concepts and theories.

Grounded research that produces theories based directly from the real life of Indonesian people is likely to solve the recht vacuum gap problem in Indonesia.

Type and Source of Data

The types of data used in this study are primary data and secondary data as supporting data. The data source is obtained from the grounded research model, with the following figure:

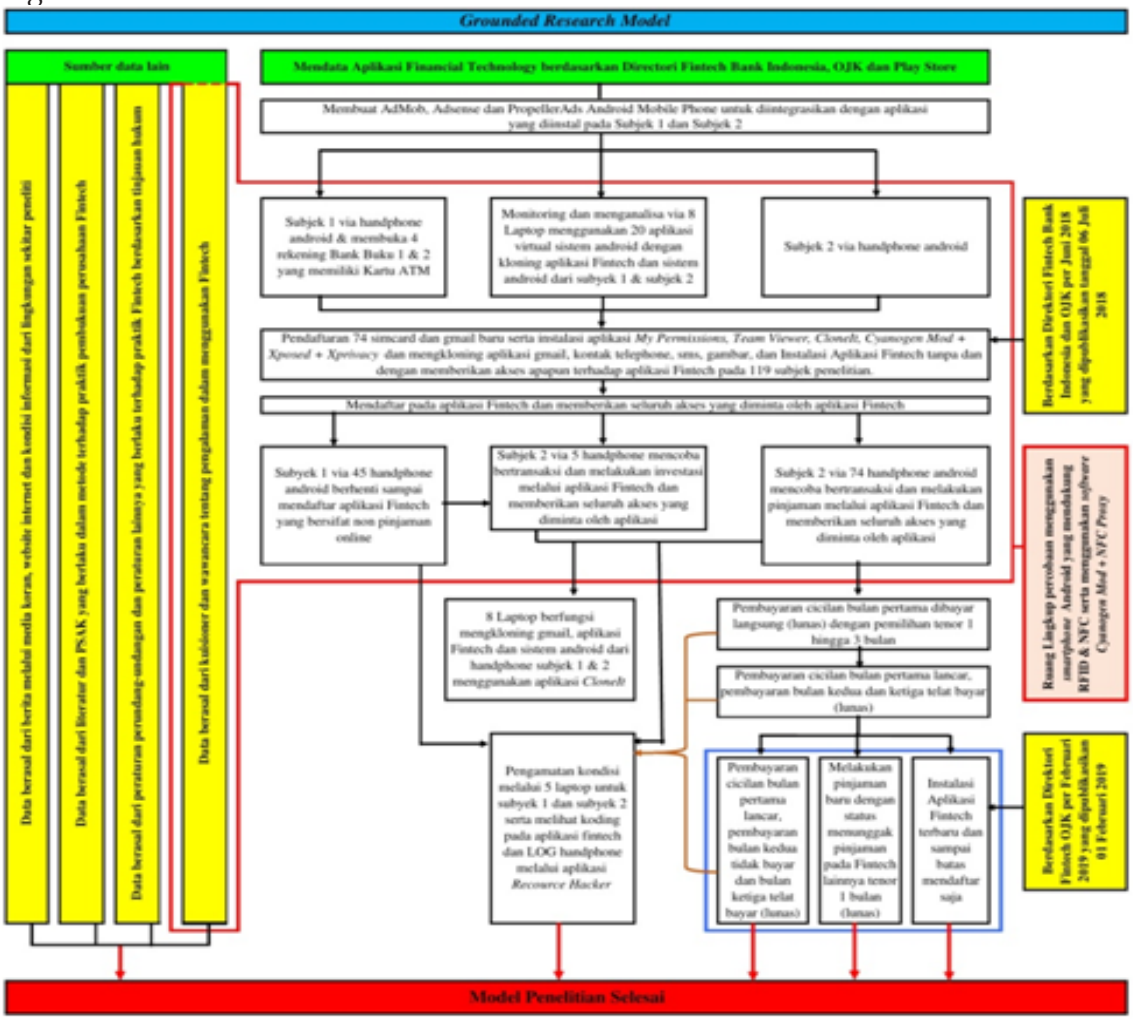
Data Collection Technique

Data collection technique used in this study is a grounded research model that adopts questionnaire techniques, telephone interviews, in-depth interviews face to face with several respondents who meet the criteria and are willing to provide information, literature review based on applicable legal regulations, and the use of online data search techniques. Population, according to Sugiyono (2009), is an area that has been determined by researchers consisting of research subjects or objects (respondents) who have certain qualities and characteristics to be studied, understood and then obtained conclusions. In this study the researchers use a population of 259 respondents divided into 3 groups. The first group consists of 140 respondents who fill open questionnaires via Google Form, the second group consists of 45 respondents who make online non-loan Fintech transactions, and the third group consists of 74 respondents who make online loans Fintech transactions. The second group is mostly students of the Faculty of Law at the Universitas Islam Indonesia, while the third group is mostly online motorcycle taxi drivers and office drivers who are members of a number of online motorcycle taxi communities in Jakarta and Yogyakarta as well as several entrepreneurs who are members of agricultural cooperatives around the area of Region 3 Cirebon and around the area of Buton Regency.

The steps taken in the grounded research model are as follows:

1. Make an agreement between the researchers and subject 1 and subject 2 to follow the instructions of the researchers during the study and will be given incentives in the form

Figure 1. **Grounded Research Model**



Source: Descriptive Analysis, processed (2019)

of interest payments from Fintech loans or administrative costs during transactions using Fintech.

2. Install and integrate *AdMob, Adsense and PropellerAds Android* as a source of income for researchers on Android smartphones of subject 1 and subject 2.
3. Researchers provide 74 new simcards and new gmail for subject 2.
4. Researchers install the *My Permission, Team Viewer, CloneIt, Cyanogen Mod + Xposed + Xprifacy* applications on 119 research subjects. In addition, researchers also clone the gmail application, smartphone contacts, SMS, images on Android smartphones of the subjects.
5. Researchers clone the Android system on 119 research subjects through 20 virtual system Android applications on 8 laptops.
6. Phase 1 is trying to install the Fintech application that has been selected in advance by the researchers without giving any access rights.
7. Phase 2 is again trying to install the same Fintech application in step 1 for subjects 1 and 2 by giving the requested access rights as a whole.
8. A total of 4 people on subject 1 open 2 savings accounts at Bank of Book 1 and 2 savings accounts at Bank of Book 2.
9. All subjects 1 carry out normal transactions in general using the Fintech application and specifically 4 people in subject 1 make transfers via ATM on a newly opened account into 3 times namely normal time, high season

time, and the end of day / month of the banking system.

10. Researchers divide 3 phases on subject 2 namely:
    - Phase 1: Subject 2 makes online loans through the Fintech application with a tenor from 1 to 3 months with smooth payments and is accelerated in the 1st month.
    - Phase 2: Subject 2 again makes online loans through the Fintech application with a 3-month tenor through a smooth payment for the 1st month and late payment scheme for the 2nd and 3rd months.
    - Phase 3: Subject 2 again makes online loans through the Fintech application with a 3-month tenor through a smooth payment sheme for the 1st month, while the 2nd month is paid together with the payment for the 3rd month with late payment scheme. In addition, subject 2 also makes an online loan to another Fintech application with a tenor of one month, which is paid smoothly. And subject 2 installs the latest Fintech online loan application that is registered in the Fintech OJK Directory.
11. All processes are analyzed and recorded on a scheduled basis through the cloning of the Android system of 119 subjects found on 8 laptops.
12. During the research stages on subject 1 & 2, the researchers also conduct a review of the applicable regulations and conduct interviews with sources and victims who have direct contact with Fintech. And the researchers try to use an Android smartphone that supports NFC and RFID and have been installed with *Cyanogen Mod + NFC Proxy*.

All results described on the grounded research model are then analyzed using the Pivot Table Microsoft Excel Professional Plus 2016 application and the Nvivo v12 Pro application based on field data based or big data obtained.

4. RESULT AND DISCUSSION

Demography, according to Kotler & Keller (2016) in ACFE (2017), is a science that studies population, such as density, location, age, gender, ethnicity, type of work and various other types of statistics.

This demographic analysis serves as supporting information and provides an overview of respondents used in research in the form of primary or secondary data. Demographic distribution of respondents can be seen in in Appendix 1.

When the data were analyzed, many respondents did not understand how to distinguish between illegal and official Fintech applications registered with regulatory authorities in Indonesia. Respondents assumed that the Fintech applications appeared on the Google play store were all official applications registered in Indonesia. Surprisingly, there were only a few respondents who knew what authorities that had the right to oversee Fintech's activities in Indonesia.

In addition, 3 different conditions were found about respondents who were willing to be whistleblowers or to report on consumer complaints channels about fraud that occurred when interacting using the Fintech application. The first condition was seen by respondents who interacted with online non-loan Fintech applications, such as e-commerce and digital wallets. Despite the act of fraud, respondents assumed that even if they made a complaint to a Fintech service provider, it would not significantly influence the satisfaction they would receive. The efforts they made would not be worth with the results obtained, especially if the nominal loss was immaterial. However, this was different when respondents interacted with Fintech online loans. They were willing to be whistleblowers or reported fraud on the consumer complaints channel for fraud that occurred. This was motivated by the taking of various information contained on the respondent's smartphone which then disrupted the respondent's daily life.

Other conditions occurred for respondents working as marketing who

were not willing to be a whistleblower for fraud that occurred around their environment. This was motivated by the rational thinking of respondents who assumed that the exchange of consumer information they had with consumer data from other marketing employees was one of the easiest ways to support the achievement of targets every month.

This condition was inseparable from the existence of a recht vacuum which formed a condition to be utilized by certain people to gain profit. Recht vacuum conditions found by researchers can be seen in Table 1.

Based on the review of researchers, there are 9 points of Recht Vacuum in supporting government programs to create positive economic growth through technology, especially Fintech:

- The absence of a regulation, specifically the Law governing the Protection of Personal Data. Researchers consider that the existing regulations and legislation are still lacking to be used as a basis to strengthen the argument

Table 1. **Recht Vacuum Conditions**

No	Recht Vacuum occurring	Rescent Condition & Regulations
1	Protection of personal data	UU No. 1 / 1998 POJK No. 1/POJK. 07/2013 PBI no. 16/PBI/2014 UU No. 19/2016
2	Accelerated repayment mechanism, online loan restructuring, regulations on billing, online loan limits or digital credit cards (pay later), settlement of losses or minus e-wallet balances due to bug software	Not available
3	Data access request restrictions on the fintech application including a maximum of emergency contacts	Lmited to Regulator's appeal only
4	The use of Network, proxy or NFC spectrum in electronic transactions and Smart SIM Card and security features	PerMenKomInfo No. 16/2018 PerMenKomInfo No 1/2019 PBI No. 20/6/PBI/2018
5	Protection of whiltleblower on Whistleblowing System (WBS)	UU No. 31/2014 Guidelines of KNKG (2008) as Non-Regulator concerning Violation Reporting System-Whistleblowing system
6	Taxes for Fintech online loans	Article 21 & 23 of UU No. 36/2008 PMK No. 251/PMK.03/2008
7	Fintech online loan checking integrated via SLIK or similar with BI checking integrated with the national blacklist of banking and other financial services institutions.	Limited to the Regulator's appeal regarding SLIK with a deadline until 2002 and the development of the Fintech Lending Data Center
8	All Fintechs are required to use the QR code issued by Bank Indonesia in the payment transaction mechanism	Development of QR Code by Bank Indonesia
9	Explanation from the Indonesian Accountants Association through ISAK (Interpretation of Financial Accounting Standards) related to Fintech that will be exposed to the adoption of PSAK 71	Not available

Source: Books and Legislation and its derivatives, processed (2019)

about the theft of personal data while in court. The proposal regarding the Personal Data Protection Act has been submitted since 2017 after the National Police Headquarters managed to reveal the sale of nearly 2 million personal data on the internet. The mode used in theft of personal data is usually through phishing. Even at this time the theft of personal data is very easy with the development of RFID and NFC technology installed in a smartphone.

- Regulations that are not yet available are the Mechanism of Early Repayment and Online Loan Restructuring, the Regulations on Billing and Online Loan Limit or Digital Credit Card (pay later), as well as the settlement of losses or minus e-wallet balances due to bug software. Despite the Regulation of Financial Services Authority (POJK) No. 1 / POJK.7 / 2013 concerning Consumer Protection of the Financial Services Sector and the Regulation of Bank Indonesia (PBI) No. 16 / PBI / 2014 concerning Consumer Protection of Payment Services which requires consumers to obtain clear and detailed information when entering into a loan agreement, the researchers consider that the regulations have not been able to accommodate these needs. From the Fintech companies, as research objects, it is found that an explanation of the agreement in online loans related to fees to be obtained by the Fintech company, the amount of interest on loans, the amount of arrears penalties, the early repayment mechanism and the request for loan restructuring, it is not more than 5 Fintech companies which explain in the loan agreement. In addition, researchers also think that there have been standard rules regarding online loan limit and dispute resolution related to the minus e-wallet balance due to the Fintech bug software. This condition makes it easy for customers to borrow on several Fintech Online Loans without limit, and consumers are faced with a loss condition if there is a bug software that causes the balance to be minus. The condition that is most detrimental to consumers is the billing procedure of the Fintech company which is still hiring a group of debt collector that presents a condition of intimidation and even makes customers become depressed due to being late paying online loans. Although this problem can be overcome with Article 368 of the Criminal Code and Article 29 Jo. Article 45 of the ITE Law concerning threats to billing, Article 378 of the Criminal Code for fraud in billing or marketing Fintech, Article 311 paragraph (1) of the Criminal Code concerning Fintech in billing, and Article 27 paragraph (1) Jo. 45 paragraph (1) of the ITE Law concerning sexual harassment through electronic media when billing, the researchers think that there need special regulations that are more in-depth related to the mechanisms and sanctions that will be faced in online loan billing.
- Determining the provision of access to emergency numbers to Fintech is important because it reduces excessive intimidation toward customers due to late payment of their online loans. Until this research taking place, what the researchers know is that there is only an appeal from the Regulator to the Fintech companies to request a maximum of 2 emergency contact numbers in the event of a delay in loan repayment. The condition that becomes the main concern of researchers is the customer data retrieval in the form of minimal access to telephone contacts and short messages when new customers try to install the Fintech application. With the condition of the Indonesian people who are still in the stage of trying something new in technological developments, this has become a huge loss experienced by the customers. Without knowing the existence of personal data retrieval by the Fintech application that is embedded in the

smartphone and subconsciously the customer gives legal access rights for the granting of permission (agreement between the application provider and the customer) to be able to access telephone contacts, short messages and so on. The researchers hope that there will be a written regulation issued along with the sanctions for granting access to 2 emergency contacts, and not allowing access to telephone contacts when the customer has not registered to enjoy the services that the Fintech application has.

- The next Recht Vacuum is the absence of regulations that can accommodate the progress of RFID and NFC technology on smartphones. This condition will make it easy for unscrupulous people to do creativity by using a minimum smartphone to do skimming. Researchers expect that there are special regulations for the use of network services, proxies or spectrum of RFID and NFC technology on smartphones that can be used as electronic payment transactions on e-wallets or even using debit card or credit card algorithms, for example, MasterCard which accommodates NFC technology stored on a smartphone application. Researchers see that Regulators need to look at Japan's Act on the Protection of Personal Information (APPI), Japanese Penal Code, Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and Canada's Criminal Code (NFC) which are closely related to point number 1 in the establishment of a law on personal data protection. Researchers propose collaboration between Regulators in Indonesia and cellular operators in Indonesia to be able to issue Smart SIM Cards, known as Universal Integrated Circuit Cards (UICC). The Smart SIM Card can be used as a Big Data Transaction Electronic that is stored securely and can only be accessed by official applications installed on the smartphone. The Smart SIM Card will later be connected and also become the basis for activating NFC devices or RFID devices on smartphones. With the Smart SIM Card, operators can find out contactless transactions through NFC technology which will then be recorded on Point of Sales (PoS) or national accounts of electronic transactions in Indonesia. The application of Smart SIM Card that is integrated with NFC technology needs security features embedded in official applications installed on smartphones such as supported by 4 digit code security features or biometric code security features such as fingerprints, faces, or eye sclera.
- The attention of researchers is focused on the importance of legally binding regulations on the Whistleblowing System (WBS). At present the Whistleblowing System (WBS) merely sticks to the Witness & Victim Protection Act and the agreement of several related agencies to protect a Whistleblower or also a Justice Collaborator. This regulation is necessary because with the continued development of the technological era, there must be someone who has a mental and clean intention to help people with the frauds he knows. The need for a Fintech employee, who is aware of fraud committed at his company or at a similar company that is considered to have become a common culture at the company, can be the basis for making new regulations that are more relevant with the main goal to protect customers.
- The researchers see the need for an in-depth study related to taxation on the Fintech online loan scheme, because Article 21 & Article 23 of Law No. 36 of 2008 and PMK No. 251 / PMK.03 / 2008 are still considered to be able to accommodate the taxation on the Fintech online loan scheme. However, what happens in the field is that business actors such as funders, recipients of

funds and Fintech companies are still confused in applying or cutting Income Tax (PPh) 21 on object for receiving loan interest to individuals or PPh 23 for receiving loan interest to companies (non-individuals). Researchers see the need for confirmation from the Director General of Taxes to be able to issue DGT regulation or DGT Circular Letter related to the imposition of tax objects on online loans and even fees obtained by Fintech companies. In general, interest on loans between non-bank companies and those not exempted in the Regulation of Minister of Finance (PMK) No. 251 / PMK.03 / 2008 will be the object of tax which is subject to a 15% rate on gross interest. However, the rates for receiving loan interest earned by individuals may vary, bearing in mind that the income tax rate for individuals applies a progressive rate principle. The progressive rate is between 5% and 30% depending on the income received by the individual. The question is who will make the tax deduction? The tax payment mechanism will be carried out by the recipient of the loan interest. In addition to this affirmation, researchers see the need for relaxation of tax regulations related to the imposition of tax objects on the Fintech online loan scheme. Because in general, this condition can be one of the factors causing the high interest of Fintech online loans today apart from the high risk of online loans without collateral. In addition, researchers see that in the future there will be a problem when there is tax audit on funders, recipients of funds, and Fintech companies due to lack of ease in depositing taxes so that it will result in aggressive tax planning that might even lead to tax avoidance and tax evasion.

- Checking Fintech Online Loans that are integrated via SLIK, or similar to BI Checking, that is integrated with the National Black List (DHN) of banks and other Financial Services Institutions (LJK) is one of the recht vacuum that is of concern to researchers. Researchers think that if the regulation related to point number 7 is not immediately enforced, fraud will often occur, such as money laundering and excessive use of loans (beyond real ability) by the customer. In this recht vacuum phase, researchers see the awareness of the Fintech Association to develop the Fintech Lending Data Center (Pusdafil) as a step forward to minimize fraud. It is expected that in the future the Fintech Lending Data Center (Pusdafil), SLIK or a similar system of BI Cheking in the Fintech application can be integrated automatically with DHN and collectibility of banking customers and other Financial Services Institutions.
- Issuance of regulations regarding the obligation to all Fintech companies to use the QR Code issued by Bank Indonesia in the payment transaction mechanism is a recht vacuum that Bank Indonesia seeks to close through its QR Code development system. Because if every Fintech company has its own and diverse QR Code, it will make Fintech customers confused in scanning the QR Code of a Fintech application. It also can be one of the tools to minimize non-recording of Point of Sales (PoS) or national accounts of electronic transactions in Indonesia.
- Explanation by the Indonesian Institute of Accountants through the Interpretation of Financial Accounting Standards (ISAK) regarding Fintech's exposure to the implementation of Statement of Financial Accounting Standards (PSAK) 71 in preparing financial statements. The ISAK is needed because of the statement on Fintech Online Loan risk disclaimer which states that the risk of default or credit risk is fully borne by the lender, and there is no state regulator responsible for the risk of default. The statement seems to show that Fintech companies are independent or free

from credit risk so that it does not meet the accounting going concern principle in knowing the condition of Fintech's financial statements from time to time.

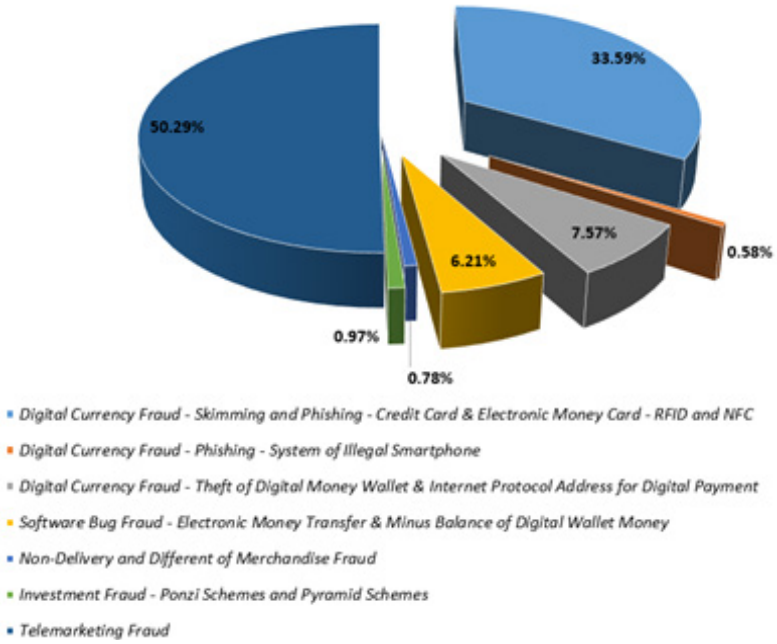
Based on the recht vacuum gaps that have been described, the researchers find fraud during research process through the grounded research model due to the recht vacuum gap. The distribution of respondents which is based on the frequency of fraud that occurs when using Fintech when the grounded research model takes place is shown in Figure 2.

The latest demographics based on our questionnaire, interview and grounded research model are done by the researchers based on the frequency of fraud that occurs when using Fintech. As many as173 activities or 33.59% are Digital Currency Fraud - Skimming and Phishing - Credit Cards & Electronic Money Cards - RFID and NFC, 3 activities or 0.58% are Digital Currency Fraud - Phishing - System of Illegal Smartphones, 39 activities or 7.57% are Digital Currency Fraud - Theft of Digital Money Wallet & Internet Protocol Address for Digital Payment, 32 activities or 6.21% are Software Bug Fraud - Electronic Money Transfer & Minus Balance of Digital Wallet Money, 4 activities or 0.78% are Non-Delivery and Different of Merchandise Fraud, 5 activities or 0.97% are Investment Fraud - Ponzi Schemes and Pyramid Schemes, and the most fraud or 259 activities or 50.29% are Telemarketing Fraud

The results obained from the questionnaire, interview and grounded research model are as follows:

1. *Digital Currency Fraud - Skimming and Phishing - Credit Cards & Electronic Money Cards - RFID and NFC.* This condition occurred during the process of grounded research model involving several respondents face to face. During the meeting, researchers activated Android smartphone with RFID and NFC support which had already been installed with Cyanogen Mod + NFC Proxy and brought it closer to where the respondents put their wallet. Then the researchers told the respondents that the electronic money balance had been reduced including information from the credit cards they have. Most respondents did not trust the information provided by researchers. The summary of the respondents'

Figure 2. **Data Grounded Research Model**



Source: Primary Data, 2019

responses are as follows:

> *"It is impossible. Just bringing closer or attaching a smartphone, then in a short time, it can take credit card data and electronic money card balances, more over at the same time making payment transactions."*

With 197 times of experiments on respondents with activity frequency more than 2 times on 1 respondent produced data of 173 times of activity. Then researchers considered that exploiting technology for digital currency fraud succeeded in retrieving information data on credit cards, debit cards, and electronic money cards of respondents. These actions make it easy to skimming to make a new credit card or attach it to a barcode machine to make transactions directly and can be used without requiring an OTP password from a credit card when making transactions via the internet network. Whereas for electronic money taken on e-money cards can be transferred directly to other e-money cards or accommodated and used during transactions. However, it is surprising that the theft using NFC and RFID technology can be done by setting the smartphone's IMEI number, IP Address and it is possible to encrypt NFC and RFID networks so that the transaction terminal's Point of Sales (POS) on the Bank system cannot detect this condition. When looking at the era of e-commerce goes to contactless, researchers found 2 international e-commerce that have applied NFC technology to their payment methods to make it easier for customers in making transaction, where they do not need to re-type the card number, card active period, cardholder's name, and other information needed in making transactions, especially through cards that are integrated through the MasterCard network. Even when researchers tried to make NFC payments using data that has been skimmed through the NFC Proxy application, it can be recorded on the NFC payment service to the 2 e-commerce sites.

2. Digital Currency Fraud - Phishing - System of Illegal Smartphones. This condition occurred when there were 3 respondents' smartphones that entered Indonesia illegally or without going through the Domestic Component Level (TKDN) process. With the default Android software when buying a smartphone, through an analysis of the smartphone LOG, it was found that there was already *an adsense pop up* advertisement and with the activity behind the smartphone screen that sent smartphone user data information, such as passwords, credit card numbers stored on the android system, to IP Address outside Indonesia.
3. Digital Currency Fraud - Theft of Digital Money Wallet & Internet Protocol Address. This condition is closely related to theft carried out without the knowledge of the smartphone owner. It is possible that the company providing the Fintech application regularly takes digital money in a small scale. What happens in reality is that the resources owned by the Fintech provider company, even though it has followed the relevant authority regulations that must use the IDR currency and only intended for certain citizens who are becoming foreign tourists in Indonesia, this can occur with experiments conducted by researchers by transacting through the Fintech QR Code application but not through the IP Address of sending transaction data in Indonesia, which can be seen from the smartphone LOG when transacting using an IP Address outside of Indonesian territory. It is feared that this condition will not be recorded in the national account of electronic transactions in Indonesia.
4. *Software Bug Fraud - Electronic Money Transfer & Minus Balance of Digital*

Wallet Money. This condition occurs when there are bugs in the software with 3 different conditions as follows:

a. The first condition occurred in one of Fintech which caused the digital currency balance in the Fintech application to be minus when used by consumers. In this condition, many consumers were contacted via e-mail or text messages (SMS and Whatsapp). Settlement of the minus balance was then charged to consumers with intimidation that if the consumer did not immediately top up the digital currency balance in accordance with the specified time, it would be resolved through the applicable legal channels. Some respondents said that when the error of the system occurred, respondents only transacted to buy food through QR Code payment 1 times, but the balance was reduced 8 times which caused the balance to be minus.
b. The second condition occurred in one of the Fintech which caused the Fintech company to experience a substantial loss. The loss was due to one of the features offered by Fintech e-wallet to buy Google Play vouchers (GPC). The bug software e-wallet was found on the purchase of GPC worth IDR 500,000, which then consumers of e-wallet users only paid IDR 22,000. The solution made by the Fintech e-wallet company was by withdrawing from a balance on the account belonging to consumer who had utilized the bug software. Withdrawing balances at some consumers made the account balance minus. In addition, the Fintech company also billed customers via text message and through email registered on the account.
c. The third condition occurred when researchers tried to make transactions in the banking accounts book 1 & 2 which already had an ATM at the time of the *end of day or month core banking system*. Of the 4 banks that were tested, 2 banks used the same core banking and 1 bank used core banking as a product of the development of its Technology Information Department. The results showed that there was an indication of bug when making transactions through the ALTO and Union Pay networks, with the time limits when transacting at an ATM approaching the time limit of the transaction which was then followed by clicking the transfer button at the end of day or month core banking system that became an experiment bank, and several transactions entered the bank account. However, for transactions on bank accounts (Banks books 3 and 4), these transactions were considered as void transactions and did not reduce the account balance. The condition was a little difficult to trace if it did not examine in detail the journals formed on the transaction, due to identical reference numbers that were formed from the results of data sent by companies providing interbank transaction services with reference numbers from transaction recipient banks. Based on the results of the recipient bank's opinion, the situation was due to the limited costs incurred to use all the features contained in the third-party core banking system and the non-existence of bug algorithm from the development of the core banking system.

5. Non-Delivery and Different of Merchandise Fraud. This condition occurred when respondents were buying goods from e-commerce applications in the country and abroad. The goods purchased were sent not in accordance with the purchase agreement and even no item was sent, or only the cardboard folds received

by the respondent. The action taken by the respondent by reporting the seller of goods through the e-commerce application did not produce any results and sometimes there were no substitutes commensurate with the items purchased.

6. Investment Fraud - Ponzi Schemes and Pyramid Schemes. This condition was closely related to the existence of the Fintech application which admitted to being affiliated with an international investment broker. The mechanism used was by issuing illegal digital certificates that were embedded in the Fintech application to convince consumers to invest by providing high investment returns. Examples that were indicated using Ponzi Schemes in investing through Fintech were GCG Asia and MIA FintechFX.
7. Telemarketing fraud. This condition occurred when there was arrogance from marketing employees to the algorithm contained in the Fintech application. This condition occurred with 2 different conditions:
    a. Telemarketing through the Fintech application that had a feature to request access rights, even without asking for access rights from the smartphone owner. Some conditions that occur are as follows:
        - When installing the Fintech Loan Online application, only 2 of the 74 Fintech applications researched that could be installed without giving access rights to a cellphone contact or others. The data transmission for the installation mostly took place prior to an agreement to make a transaction with the customer, so that at least the telephone and LOG contact data on the hand phone had been sent. Even for the illegal Fintech application, it was found access to a smartphone camera and the installation of *malware ghost push* without the permission of the smartphone owner. The malware was aimed at smoothing the takeover or known as keylogging smartphone to access smartphones secretly. The data retrieval will increase if there is a delay in the payment due for the loan. Another thing that was not explained in the cooperation agreement in the loan was the repayment mechanism that was faster than the actual maturity, until there was no solution to do the restructuring of the online loan agreement.
        - An e-commerce application that is a part of Fintech is the discovery of Adware that infiltrates smartphone systems. The adware acts on the background of the android system which will display pop up ads, display ads when reading online news.
        - It was found 1 application of international banking and 1 application of national banking that provided convenience in viewing transactions on credit cards, requesting the right of access as a whole to telephone contacts.

    b. Telemarketing through marketing employees is in the following ways:
        - Offering product in a timeless manner. The offer was made via telephone, SMS, or Whatsapp. Even during the research process, there were offers via SMS and whatsapp that included a link that contained malware. And in the algorithm contained in the instant message was found a spouseware attachment which automatically sent instant messages to various contacts and groups on whatsapp.
        - Based on the results of the questionnaire and in-depth interviews which were

then practiced by one of the respondents, it was found that there was a practice of exchanging and even buying and selling cellphone numbers of IDR 500,000 for every 200 cellphone numbers.

- Based on information from one respondent with a marketing background in a Financial Services Institution (LJK), it was found that there was customer who was included in the National Black List (DHN) from Bank Indonesia and had loans that were included in the NPL category at one of traditional Financial Service Institutions but was still free to conduct transactions by investing as a funder for Online Fintech Loans.
- In the telemarketing procedures for billing, it was found intimidation to the research respondents using high-pitched sentences or abusive sentences, threats to billing, and the distribution of personal data to 119 contact groups that were given access. The distribution of personal data was in the form of slander for acts of sexual harassment committed by respondents in arrears on loans.

The factors that affect the chances of fraud as explained above are the lack of public knowledge of the procedure for transactions using Fintech, loosening of applicable regulations, and the arrogance of Fintech customers to take advantage of the Fintech bug software to get the maximum profit without thinking about the impact of the law behind it, and the arrogance of the Fintech company to minimize the big risks that will occur. In addition, there is indication that the formation of the Fintech ecosystem with other traditional financial services is not yet maximal. The situation is exacerbated by the unavailability of the Whistleblowing System (WBS) through the special complaint channel related to Fintech, which is only available at the Legal Aid Institute (LBH) in Jakarta but OJK and Bank Indonesia still provide a channel for consumer complaints in general.

The results of research on RFID and NFC technology support the the results of research conducted by Ariansyah (2012) that NFC technology on smartphone technology devices needs to have binding standards as well as increased socialization and education to the public about NFC technology as one of the payment instruments.

Researchers illustrate that the formation of a healthy Fintech ecosystem and an anti-fraud culture should be done like in the division of sea area ownership between the territorial sea zone and the free sea zone. Where territorial sea zone means the use of internet access to support financial services quickly but still has territorial zone ownership limits based on imaginary lines, namely the use of IP Address, in the sovereign territory of a country every time conducting financial transactions, while the free sea zone means a free zone in the use of IP Address to provide internet benefits in addition to financial services.

5. CONCLUSION

Based on the observations, the very rapid development of technology to support fast and unhindered financial services can create a large gap in the readiness of the use of technology era 4.0 in the country. Without strong preparation, it will increasingly create a big gap in the formation of the Fintech technology-based fraud chain. The four main factors are the large recht vacuum gap, the unpreparedness of the Indonesian people who are still engulfed in a culture of lazy reading the terms and conditions required by Fintech and regulators, arrogance of customers who understand the existence of the Fintech bug software to gain profit as much as possible without thinking about the legal impact behind it, and the arrogance of using technology resources owned by Fintech companies and marketing employees.

The researchers assume that the arrogance of the technology resources owned is used to create a big data in minimizing the risk of the Fintech company and the opportunity in the pressure perceived by marketing employees to achieve the specified targets. This is also the arrogance in the use of errors / bugs in the Fintech system and the inability of the Indonesian people to understand the use of Fintech which only follows social trends and high levels of trial and error over Fintech. It is also complemented by the non-maximum consumer complaints channel or the Fintech special whistleblowing channel system which is shown by the high number of complaints by Fintech customers to be the main spotlight that has not been resolved to date. Other conditions that influence the high interest rate of Fintech online loans, one of which is the imposition of an income tax object on loan interest as explained in Law No. 36 of 2008 concerning Income Taxes.

Therefore, researchers provide suggestions in the formation of the Fintech ecosystem by implementing anti-fraud as one of the drivers of Indonesia's economic growth as follows:

1. Creating a society that understands technology, especially Fintech and not following the trend of a certain Fintech only. It can be done by establishing an educational curriculum from an early age about technological knowledge, making more intense socialization by regulators, or by follwing trends in the technology era by inserting ad content using adware that aims to educate Indonesian society.
2. Making an integrity pact to support anti-fraud and anti-money laundering among regulators, Fintech associations, and Fintech companies when making official registration with regulators.
3. Regulators should get rid of egoism between institutions by synchronizing verbally or nonverbally through technology channels that are automatically integrated between state institutions, such as Bank Indonesia, the Financial Services Authority (OJK), Ministry of Communication and Information, PPATK, and the Ministry of Finance which focuses on the Director General of Taxes and others in making better Fintech regulations that can be a driver of economic growth in Indonesia. As for the new regulations or the updates can at least accommodate the following conditions:
   - Rules regarding prohibition on requests for access right of the collection of consumer information data before the customer agrees in accordance with the agreement to transact through the Fintech application.
   - Rules regarding billing procedures and the upper limit of online loans or digital credit cards (pay later).
   - Rules regarding the mechanism for accelerated repayment and online loan restructuring.
   - Rules regarding the settlement of customer or Fintech company losses for the existence of Bug Software.
   - Closing all illegal download paths of the Fintech application registered in the Google Play Store by requiring all Fintech company IP Address channels through a special channel.
   - Collaborating with operators of communication service providers to make the algorithm for using non-Indonesian IP Addresses which is automatically blocked and unable to make transactions through Fintech.
   - Rules regarding NFC and RFID proxies on smartphone companies which can be seen in the PoS terminal banking system financial transaction flow.
   - Collaborating between regulators and telecommunications service operators to make regulations regarding the use of NFC that is connected to the Smart SIM Cards that are supported by 4-digit code

security features or biometric code security features such as fingerprints, faces, or eye sclera.

- Rules regarding the use of QR Code that have been issued by Bank Indonesia to all Fintech service providers.
- Accelerating rules, similar to BI Checking, for loans or Fintech funders integrated with BI Checking and the national blacklist of banks and other financial service institutions.
- Rules regarding the establishment of the Fintech online loan company in running the online loan distribution business to be the subject to tax or not on PPh 23 or PPh 21 for interest on the loan.
- The assertion about the operation of online loans or online investments that will be exposed to the application of PSAK 71
- Rules that forbid Fintech companies directly or through the Indonesian Fintech association not to act arrogantly in carrying out its financial services.

4. Setting up a special channel for the whistleblower system or a special Fintech consumer complaint channel for regulators and requires all Fintech service providers to provide a whistleblower system channel or consumer complaint channel openly and readable by consumers.

REFERENCES

ACFE Indonesia Chapter dan E&Y. (2017). *Survai Fraud Indonesia*. ACFE Indonesia Chapter.

Allan Richarz (____). Near-Field Communication Technology: Regulatory and Legal Recommendations for Embracing the NFC Revolution. Canadian Journal of Law and Technology. Vol. 12.

Andreja Rojko. (2017). Industry 4.0 Concept: Background and Overview. iJIM – Vol. 11, No. 5.

Ariansyah Kasmad (2012). Studi Kesiapan Penyelenggaraan Layanan Near Field Communication (NFC) Komersial di Indonesia. Buletin Pos dan Telekomunikasi Vol. 10 No. 3.

Aurora & Francisca. (2011). Grounded Theory of Generating Theory in The Study of Information Behavior.

Bambang Setioko. (2011). Penggunaan Metoda Grounded Theory Dibawah Payung Paradigma Postpositivistik Pada Penelitian Tentang Fenomena Sosial Perkotaan.

Berry *et. all.* (2017) Perkembangan Financial Technology Terkait Central Bank Digital Currency (CBCD) Terhadap Transmisi Kebijakan Moneter dan Makroekonomi.

Crowe Horwarth. (2011). Putting The Freud in Fraud: Why The Fraud Is No Longer Enough IN Howarth, Crowe.

D. W. Arner, *et. all*. (2016). The Evolution of FinTech: A New Post-Crisis Paradigm?

Douglas, Janos & Ross. (2016). The Emergence of RegTech 2.0 from Know Your Customer to Know Your Data. CFA Institute Research Foundation.

Douglas, Janos & Ross. (2017). Fintech and Regtech in a Nutshell, and The Future in a Sanbox. CFA Institute Research Foundation.

Ernest & Young. (2018). Fintech Ecosystem Playbook.

Fitri Amalia. (2016). The Fintech Book: The Financial Technology Handbook for Investors, Entrepreneurs and Visionaries.

Financial Services Ireland. (2018). A Fintech Strategy for Ireland.

Gredha & Cholichul. (2012). Kebosanan Kerja Pada Karyawan Radio Sonora Surabaya.

HM Tresury. (2018). Fintech Sector Strategy: Securing the Future of UK Fintech.

I Gusti Ayu. (2014). Metode Grounded Theory dalam Riset Kualitatif.

In Lee & Yong Jae. (2018). Fintech: Ecosystem, Business Models, Investment Decisions, and Challenges. Journal of Business Horizons Vol. 61: 35-46.

James & Adam. (2019). Technological Innovation and Economic Growth: A Brief Report on the Evidence.

Kamus Hukum (Edisi Lengkap).____.

Kamus Besar Bahasa Indonesia (KBBI). (1989). Balai Pustaka Jakarta.

Kaushik *et. all.* (2016). Unlocking Indonesia's Digital Opportunity. McKinsey.

Kevin & Dr. Robert. (2002). Case Study and Grounded Theory: Sharing Some Alternative Qualitative Research Methodologies with System Professionals.

KNKG. (2008). Pedoman Sistem Pelaporan Pelanggaran – SPP (Whistleblowing System –WBS), KNKG.

Kusumawatiet.all.(2018).ThePhenomenon of Leadership in Conglomerate Subsidiaries in Creating Anti-Fraud Culture. Volume 3, No.2nd Edition Asia Pasific Fraud Journal.

Liusavara, leena. (2015). Grounded Theory in a Case Study – Questions of Generalizing Outcomes. Finlandia: Oikeus-ja kaulutuspalvelu Law Point avoinythio.

McKinsey Global Institute. (2019). Digital India: Technology to Transform a Connected Nation.

Otoritas Jasa Keuangan. (2017). Perlindungan Konsumen pada Fintech : Kajian Perlindungan Konsumen Sektor Jasa Keuangan.

Oxford Research. (2018). CPH Fintech Hub: Study and Recommendations for Making Copenhagen a Nordic FinTech Hub.

Munir Fuady (2018). Metode Riset Hukum: Pendekatan Teori dan Konsep. Rajawali Press.

PBI No. 16/1/PBI/2014 tentang Perlindungan Konsumen Jasa Pembayaran.

PBI No. 20/6/PBI/2018 tentang Uang Elektronik.

Peterson K. Ozili. (2017). Impact of Digital Finance on Financial Inclusion and Stability.

PerMenKomInfo No. 1 Tahun 2019 tentang Penggunaan Spektrum Frekuensi Radio Berdasarkan Izin Kelas.

PerMenKomInfo No. 16 Tahun 2018 tentang Ketentuan Operasional Alat dan/ Atau Perangkat Telekomunikasi.

PMK No. 251/PMK.03/2008 tentang Penghasilan atas Jasa Keuangan yang Dilakukan oleh Badan Usaha yang Berfungsi Sebagai Penyalur Pinjaman dan/atau Pembiayaan yang tidak Dilakukan Pemotongan Pajak Penghasilan PPh 23.

POJK No. 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan.

Surojo Wignjodipuro. (1971). Pengantar Ilmu Hukum (Himpunan Kuliah), Bandung: Alumni.

Tiko Huizinga. (2018). Using NFC Enabled Android Devices to Attack RFID Systems. Radboud University.

Tim Pustaka Buana (2017). Kitab Lengkap KUH Perdata, KUHA Perdata, KUHP, KUHAP. Pustaka Buana.

UN Environment. (2017). Fintech, Green Finance and Developing Countries.

UN Environment. (2018). Green Digital Finance: Mapping Current Practice and Potential in Switzerland and Beyond.

Undang-Undang No. 1 Tahun 1998 tentang Perbankan.

Undang-Undang No. 19 Tahun 2016 tentang Perubahan Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik.

Undang-Undang No. 31 Tahun 2014 tentang Perubahan Undang-Undang Nomor 13 Tahun 2006 tentang Perlindungan Saksi dan Korban.

Undang-Undang No. 36 Tahun 2008 tentang Pajak Penghasilan.

Yuliansyah *et. all.* (2015). Manajemen dan Analisis Data Kualitatif dengan Perangkat Lunak NVivo. Salemba Empat.

Appendix 1. **Demographic Distribution of Respondents**

No.	Types of Demography	Respondents Questionnaire		Respondents Grounded Research Model			
				Fintech Non-Online Loans		Fintech Online Loand	
1	Gender						
	Male	72	51%	29	64%	64	62%
	Female	68	49%	16	36%	28	38%
	Total	100	100%	45	100%	74	100%
2	Age						
	< 21 years	21	15%	38	84%	0	0%
	21 – 30 years	39	28%	5	11%	22	30%
	30 – 40 years	65	46%	0	0%	44	59%
	40 – 50 years	12	9%	2	4%	8	11%
	50 – 60 years	3	2%	0	0%	0	0%
	Total	140	100%	45	100%	74	100%
3	Last Education						
	< = Senior High School	21	15%	38	84%	32	43%
	Associate's degree	9	6%	0	0%	16	22%
	Bachelor's degree	87	62%	2	4%	26	35%
	Master's degree	21	15%	5	11%	0	0%
	Doctoral degree	2	1%	0	0%	0	0%
	Total	140	100%	45	100%	74	100%
4	Community Status						
	State Civil Apparatus	3	2%	0	0%	0	0%
	SOE/ROE's employee	26	19%	7	16%	0	0%
	General employee	37	26%	0	0%	58	78%
	Entrepreneur	53	38%	0	0%	16	22%
	Univesity student	21	15%	38	84%	0	0%
	Total	140	100%	45	100%	74	100%
5	Occupation						
	Head of division (equivalent)	2	1%	0	0%	0	0%
	Head of Department (equivalent)	4	3%	2	4%	0	0%
	Staff	68	49%	5	11%	0	0%
	Lecturer	6	4%	0	0%	0	0%
	Marketing of Bank, leasing, financing, fintech, and the like	21	15%	0	0%	0	0%
	Online motorcycle taxi driver	0	0%	0	0%	58	78%
	University Student	21	15%	38	84%	0	0%
	General public	18	13%	0	0%	16	22%
	Total	140	100%	45	100%	74	100%

6	Experience using the fintech application						
	Yes	111	79%	45	100%	74	100%
	Yes, feel like a victim of fintech	29	21%	0	0%	0	0%
	No	0	0%	0	0%	0	0%
	Total	140	100%	45	100%	74	100%
7	Willingness to be interviewed						
	Yes	98	70%	45	100%	74	100%
	No	42	30%	0	0%	0	0%
	Total	140	100%	45	100%	74	100%
8	Willingness to be a whistleblower or report fraudulent act						
	Yes	37	26%	18	40%	56	76%
	No	103	74%	27	60%	18	24%
	Total	140	100%	45	100%	74	100%

Source: Questionnaire Data & Graounded Research Model Data processed (2029)