Research on the Abuse of Fintech in Crime

Ji-Heng Lin[*] & Yueh-Ping Yang[**] & Kai-Ju Lee[***]

Abstract

FinTech (Financial Technology) has sped up the development of payment services and promoted the use of electronic payment instruments to transfer funds online/offline in both daily consumption and investment. In addition, backed by blockchain and cryptography technologies, cryptocurrency provides the public with a new option to store and exchange value, prompting many countries to rethink not only their currency policies and supervision but also to consider the issuance of digital currency (Central Bank Digital Currency, "CBDC"). These developments have deep impacts on modern ways of payment, and the impact is wide and rapid.

Electronic payment instruments, including electronic payments and third-party payments, have five general characteristics: anonymity, speed, difficult to track, non-face-to-

[*] Managing Partner of Lin and Partners; College of Law, National Chengchi University, Doctor in Law, Taiwan.

[**] Association Professor of College of Law, National Taiwan University; Doctor in Law, Harvard Law School.

[***] Director, Banking and Capital markets department, Lin and Partners; New York University School of Law, Master of Laws.

face, and cross-border. These characteristics provide criminals with a new instrument to commit crimes. There have been many criminal cases in Taiwan that have employed electronic payment instruments as part of the crime. Through a comprehensive empirical analysis and typology, we have found that criminals often use electronic payment instruments to commit fraud, gambling, theft of electronic payment account for consumption, theft of personal information to create fraudulent payment account, and others. The number of such cases and the monetary amount involved are also considerable, showing that the current electronic payment instrument structure contains significant loopholes in terms of regulations and anti-money laundering supervision. As a result, electronic payment instruments have gradually become an instrument for crimes.

Cryptocurrency itself also experiences high price fluctuation, resulting in a relatively high investment risk. In addition, in recent years, some fraud cases involved the collection of public money in the name of blockchain and/or cryptocurrency. However, except for Security Token, which is a security regulated by the Securities and Exchange Act, and Money Laundering Control Act, the current laws and regulations do not directly regulate cryptocurrency; as a result, the Financial Supervision Commission recently released a press release to remind the public of the potential risks of cryptocurrency investments. In this study, we analyzed all the related court

judgements and summarized six major types of crimes related to cryptocurrency, including cryptocurrency as a medium for transaction, delivey of personal data, delivery of cryptocurrency account, payment instrument, money laundering of illicit income, and theft of electricity for mining. The number of such cases grows each day.

Recent regulatory amendments have affirmed the AML obligations of both third-party payment businesses and cryptocurrency businesses. That said, related competent authorities still face challenges when supervising the businesses to implement their said obligations in this regard. This research proposes that investigation authorities may establish communications with competent authorities and report to the latter the businesses that fail to implement AML obligations as observed during the investigation. Based on this information, competent authorities may designate certain business as top priority for inspection to implement the risk-based approach supervision. Besides, the investigation authorities may further establish a FinTech criminal database that collects investigation data for the analysis of FinTech-related crime. Through the assistance of technology, investigation authorities, with limited supervisory resources, can more comprehensively and timely supervise this complex system and identify the businesses for which enhanced supervision is appropriate. Finally, to reduce the crimes using FinTech as a criminal instrument, this research

proposes to introduce a provision under the Criminal Law penalizing the counterfeits of digital payment instruments to fill the loophole under the current Article 201-1 of the Criminal Law that applies only to card payment instruments. In this way, the authenticity and trustworthiness of digital payment instruments may be enhanced.

Keywords: Electronic Payment, Third-party Payment, Cryptocurrency, Virtual Asset, Money Laundering, Fintech, Legal Compliance, Criminal Investigation

Chapter 1. Research Background

FinTech (Financial Technology) has sped up the development of payment services and promoted the use of electronic payment instruments to transfer funds online/offline in both daily consumption and investment. In addition, backed by the blockchain and cyptography technologies, cryptocurrency provides the public with a new option to store and exchange value, prompting many countries to rethink not only their currency policies and supervision, but also to consider the issuance of digital currency (Central Bank Digital Currency, “CBDC”). These developments have deep impacts on modern ways of payment, and the impact is wide and rapid. On the other hand, payment instrutments derived from such emerging financial technologies have gradually become criminal instruments or money laundering instruments used by criminals in committing crimes, causing challenges to criminal investigations. The main purpose of this research is to sort out the types and practices of abuse of emerging financial technology in crimes in Taiwan, including electronic payment instrutments and cryptocurrency, and then propose feasible policy responses. As far as "electronic

payment instruments" are concerned, this research adopts a broad definition, including the businesses referred to in paragraph 1 of Article 4 of the Act Governing Electronic Payment Institutions, and also includes two types of narrowly defined electronic payment and third-party payment, as defined below:

1. Narrow definition of electronic payments

In a narrow sense, electronic payment institutions refer to institutions that handle the collecting and making of payments for real transactions as an agent, receive stored funds, engage in domestic and foreign small-amount remittances business, engage in buying and selling foreign currencies and currencies issued by Mainland China, Hong Kong, or Macao (hereinafter referred to as foreign currencies) related to the aforementioned businesses.

At present, there are 5 exclusive electronic payment institutions, 4 electronic ticket institutions under the old law, and 23 concurrent electronic payment institutions, such as: JKOPAY, GAMA PAY, O'Pay, Pay2go, ezPay, etc.

2. Third-party payments

This refers to only the business of collecting and paying substantive transaction funds as an agent, where the

average daily balance of the collection and payment items in the custody of the agent does not exceed NT$2 billion. Popular providers are LINE Pay, ECPAY, NewwbPay, PChomePay Payment, Yahoo Easy Pay, HyPocket, Swipy, SmilePay, etc.

The electronic payment instrutments referred to in this research does not include the following common mobile payment instrutments:

A. Mobile Payments

This refers to the cooperation between the credit card issuer and the coded service provider and the use of coded technology to enable the cardholder to convert the physical credit card number into a code and load it into a mobile device such as a mobile phone for consumer transactions after the completion of application and identity verification procedures. Popular providers are Google Pay, Apple Pay, Samsung Pay and Taiwan Pay.

B. Mobile Banking Card

This refers to downloading personalized data to mobile devices through cloud-based transmission, and issuing financial cards with mobile transaction functions. A popular provider is Taiwan Pay "Financial Card Cloud Payment".

C. Mobile Point of Sale (mPOS)

Also known as mobile credit card machine, this refers to using an APP on a mobile phone or tablet that allows the device to act as an acquiring device, and then through the card swiping or chip card method, allows the store to accept payments by credit card at any time.

3. Cryptocurrency

As far as cryptocurrency is concerned, the term " cryptocurrency " in this research is defined under the laws of Taiwan, which means "using cryptography and distributed ledger technology or other similar technologies, which recognized the value that can be stored, exchanged or transferred digitally and used for payment or investment purposes.” At present, most advanced countries in the world have not regarded the pure use of cryptocurrency as a criminal act. However, because cryptocurrency has the function of commending a certain asset value when used as an investment instrutment or a means of payment, this has led to incidents of domestic and foreign investment fraud, money laundering, violations of the Securities Exchange Law and illegal deposit. According to its nature, it can be divided into:

A. Payment Tokens

These are only used for payment, and has no further functions or connection to other uses.

B. Utility Tokens

These are tokens that provide digital access rights for other applications or services.

C. Asset Tokens

These are used to reflect the underlying value of a physical entity or a company's surplus or dividends, or other financial products (stocks, bonds, and derivatives) including but not limited to Bitcoin, Ethereum, USDT or other cryptocurrency used as the objects or instruments of crime.

Chapter 2. Difficulties for Law Enforcement Agencies to Detect Crimes Related to Emerging Fintech

1. The characteristics of crimes related to electronic payment instruments

Theoretically, electronic payment instrutments have certain characteristics that are conducive for use as criminal tools, which may constitute obstacles or challenges for criminal investigation. They have been the subject of attention of the Financial Action Task Force (FATF) and international academic research literature. Based on the empirical data of judicial judgments in Taiwan, this research summarizes the use of electronic payment tools in crimes in Taiwan, and then concludes that the challenges brought by electronic payment instrutments to criminal investigations in Taiwan are mainly related to the following characteristics: anonymity, multi-layered, speed, non-face-to-face contact, and cross-border nature.

A. Anonymity

As a result of the use of Internet technology in

electronic payment instruments, such instruments carry with it the anonymity that is common in the Internet world, thereby increasing the difficulty of criminal investigation. What needs to be emphasized is that the anonymity referred to here is not limited to absolute anonymity where no real name is used at all, but also includes anonymity where the identity is easier to hide, resulting in more complicated procedures required to trace the real identity of the individuals involved.

Specifically, the results of the second chapter of this research show that many crimes involving electronic payment tools involve the use of so-called "virtual accounts", which can be seen in the following judgments: the Taipei District Court 109, Yi Zi No. 783 Criminal Judgement, the Taipei District Court 107, Sen Jien Zi No. 643 Criminal Judgmen, and the Taichung District Court Su Zi No. 2311 Criminal Judgment. The crime is the use of electronic payment or third-party payment to conduct transactions. This type of payment transaction will generate a set of corresponding virtual accounts for the purpose of receiving funds when the transaction occurs. After the criminal obtains the virtual account, the criminal provides the virtual account number for the victim to remit money.

The original function of the virtual account was to protect consumers. It was hoped that the virtual account can serve as a temporary relay point for the transaction between the buyer and the seller. After the seller confirms the order and the buyer obtains the goods, the amount remitted by the buyer into the virtual account will be transferred to the seller's physical account. However, in practice, the application for a virtual account can be completed with simply personal information such as ID card number and physical account number, which is relatively convenient and easy. Therefore, criminals in Taiwan commonly steal other people's personal information to create virtual accounts. Compared with physical bank accounts, virtual accounts have a relatively loose connection with the real identity of the account owner due to the fact that such accounts can be created easily. Therefore, such accounts have a certain degree of relative anonymity. It takes a significant effort for law enforcement to uncover the real identity of the owner of the virtual account, thus increasing the difficulty of criminal investigation.

In addition, in practice, virtual accounts are mostly for single use; that is, they usually become invalid after the conclusion of the online transaction. This also increases the

relative anonymity of electronic payment instruments and the difficulty of criminal investigation. Although the inspection agency can theoretically identify the physical bank account linked to the virtual account, and then the bank to which the account belongs can retrieve the information to know the identity of the physical account owner linked to the virtual account, the difference between physical and virtual accounts is that when the criminal uses a physical bank account, the prosecuting agency can quickly freeze the physical account and identify the holder of that account when it learns of the crime; in contrast, further investigation is required to discover the identity of the virtual account holder, which can easily cause delays and difficulties for the police when tracing crimes.

This study also found that many crimes (especially fraud) using electronic payment tools occur in shopping transactions on online platforms. In this type of transaction, the buyer usually does not know the seller's real identity, and only knows the payment account or virtual account to which the payment should be made; in practice, the buyer even often goes to the convenience store to use the super merchant code to pay in cash. The virtual account, therefore, in addition to the relative anonymity of the

seller's use of the virtual account, even the victim (the buyer) has anonymity. In the case that both the offender and the victim have a certain degree of anonymity, a certain degree of investigative burden may be placed on the notification, investigation, evidence collecting, or even the use of resources in the investigation and trial of related cases.

B. Multi-layered

One of the characteristics of electronic payment instruments is that they increase the flow of funds to intermediaries, thereby increasing the layers and complexity of the flow of funds. Take electronic payment and third-party payment as examples, when a user applies to create his payment account, he usually binds his existing bank entity account, and the payment company itself also needs to set up a special account in the bank. Therefore, a multi-layered payment system of "payer bank → payment provider → payee bank" is formed. The Hsinchu District Court's 106 Yi Zi No. 1114 Criminal Judgment, and the Taoyuan District Court 106 Yi Zi No. 2293 Criminal Judgment are good examples of this complexity.

The direct effect of the payment industry's

intermediary cash flow is that both the payer's bank and the payee's bank only handle the cash flow with the payment service provider, so the payer's bank will not have access to the payee's information, and the payee's bank will not have access to the payer's information. When the investigating agency conducts investigations, it is not easy to obtain a full picture of the cash flow directly from the bank records, and it must rely on the payment service provider that acts as an intermediary to grasp the complete information about the cash flow.

What is more complicated is that, in practice, third-party payment providers and electronic payment providers also cooperate, thus forming a more complicated payment relationship. For example, the electronic payment company Oupay must comply with the real-name system and other anti-money laundering regulations, so it requires both buyers and sellers to be its members before Oupay can conduct payment transactions. However, in order to expand its business, it has started to cooperate with its third-party payment company in September 2016. Green World Technology has reached a technical cooperation with Oupay, so that the cash flow collection from non-Oupay members will be handled by Green World Technology. In

this case, the electronic payment industry may not have direct dealings with either the payer or the payee, so there is no relevant information about the payer or the payee, and the third-party payment industry does have direct dealings with the payer or payee. However, because the money laundering prevention and control requirements it is required to comply with are relatively confusing, it may not have fully implemented such requirements. In such a situation where a third-party payment company and an electronic payment company participate in the transaction at the same time, the cash flow is actually more complicated, and the investigator may face greater challenges in determining the flow of funds when investigating crimes.

C. Speed

Electronic payment instrutments have the convenience of fast account creation, and the fund transfer process is more convenient and faster than traditional financial institutions such as banks, and the required verification procedures are also simpler. Especially with mobile devices, payment and collection procedures can be completed quickly, which is also an advantage of electronic payment tools compared to traditional payments. Precisely due to

this characteristic of speeding up transactions, electronic payment tools are, at the same time, more likely to be used as criminal instrutments.

For example, in the case of creating virtual accounts as described above, since virtual accounts are convenient to create and are often only used for a single transaction as described above, criminals can create a large number of virtual accounts in a short period of time for fund collection purposes. When the prosecuting agency receives a report and requests payment companies or related banks to obtain physical account information, criminals can commit more crimes with a large number of virtual accounts. Therefore, even if the prosecutorial agency can finally track down the offender, the number and scale of victims may continue to expand during the investigation process due to the speed of electronic payment instruments.

In fact, as the empirical study of judicial judgments in this study shows, electronic payment tools are widely used in small-value fraud cases. However, many small-value fraud cases have a large number of victims, and the crime can span many years. For example, the case of Taitung District Court 108 Yuan Jin Su Zi No. 47 Criminal Judgment spanned from 2018 to 2019, and Taichung

District Court's 108 Jianshang Zi Criminal Judgment No. 445 spanned from 2015 to 2016. The number of victims and the time distribution of such cases show that the speed of electronic payment instrutments may aggravate the overall degree of victimization of related crimes and increase the time pressure for investigation by the prosecuting agency.

D. Non-face-to-face contact

Electronic payment instruments rely on the internet to provide payment services. Therefore, payment institutions do not directly contact payment service users face-to-face. Instead, the server determines the correctness of the account and password through identification to determine whether to grant access to or use of a specific account. In this context, not only users of electronic payment tools such as transaction counterparties will not know the real identity of each other, but the payment institutions themselves face the challenge of user identification when users apply to set up an account or initiate a specific transaction. Criminals may fraudulently use the identity of the payment account holder to conduct transactions, thereby causing harm to the account holder.

For example, in the case of stealing the identity

information of others and using the payment platform for consumption, the criminal may steal the victim's credit card information in the victim's payment account for online consumption payment, causing the victim's property loss. At this time, the electronic payment industry acts as a collection and payment service and facilitates the cash flow settlement of credit card transaction funds. In this process, the electronic payment industry connects to the credit card authentication center to obtain authentication from the bank. Therefore, as long as the card number and authorization code are filled in correctly, the payment will be approved, so that it is not easy to identify that the consumer is not actually the credit card holder or payment account holder, and it is not easy to prevent theft from happening in the first place. It is true that the above-mentioned hacking methods may also occur when physical credit cards are used, such as stolen credit cards. However, the non-face-to-face contact feature of electronic payment tools allows criminals to perform authentication procedures through account numbers and authorization codes without the need to steal or forge physical cards, thereby greatly reducing the cost of stealing credit cards, and allows for the more efficient commission of crimes.

Another common criminal tactic is that the criminal uses social networking sites to post specific auction information as a seller to induce the victim to place an order, and simultaneously, he purchases equivalent products from unrelated sellers as a buyer, and then obtains a set of virtual account from the seller. The criminal then passes the virtual account provided by the seller to the victim to instruct payment to the virtual account, but the criminal does not in fact ship the goods to the victim after obtaining the goods he purchased from the seller. The victim essentially pays the seller on behalf of the offender, and the victim does not actually obtain the goods purchased from the offender. This is the case in the New Taipei District Court 107 Jien Zi No. 103 Criminal Judgment and the New Taipei District Court Shen Su Zi No. 2352 Criminal Judgment. The establishment of this criminal method is also due to the non-face-to-face contact nature of electronic payment tools, which allows criminals to easily embezzle others' virtual accounts for their own use and hide their identity behind the Internet.

In addition to the above-mentioned theft of other people's electronic payment accounts, the nature of non-face-to-face contact has also caused a common practice in

Taiwan in the form of "stealing other people's information to set up electronic payment accounts". Covered by non-face-to-face contact, criminals can create an electronic payment account that appears to belong to others by setting a series of account and password information as long as they obtain the basic personal information of others, and then can use the account and password for criminal purposes. By completing all transactions through authentication, the offender can use the electronic payment account of this unknowing person to cover his crime. Under such criminal methods, the prosecuting agency may only detect the person whose personal funds have been stolen for the purpose of setting up an account during the investigation, but if there is no evidence that the person was involved in committing the crime, the prosecuting agency will not be able to prosecute. Therefore, it increases the difficulty of criminal investigation by prosecutors.

E. Cross-border

Electronic payment instruments use the Internet to provide payment services. Due to the far-reaching nature of the Internet, payment services supported by payment companies can cover users outside Taiwan and can be

spread across numerous countries. Therefore, they have a certain degree of cross-border nature and may be used for cross-border crimes. The investigation agency, therefore, faces the challenge of cross-border investigations.

The empirical study of judicial judgments in this research shows that although the proportion of electronic payment tools used in cross-border crimes in Taiwan is not very high, it is still worthy of attention. In the cases collected in this study, the criminals involved in cross-border crimes include illegal operation of online gambling platforms, illegal operation of exchange business, violation of multi-level marketing management measures and other large-scale crime types. From this we can see that the amount of electronic payment instrutments used in cross-border crimes in Taiwan is relatively large, and most of them are long-term crimes that last for a long period of time. The foreign country or region involved is mainly mainland China, but there are also other countries such as Thailand or South Korea. As such, it is clear that criminals have also taken advantage of the cross-border nature of electronic payment tools to commit crimes in Taiwan.

2. The Characteristics of Crimes Related to

Cryptocurrency

Crpytocurrency can also be used as a digital payment tool, using the blockchain network to provide the same payment service. Therefore, virtual currency-related crimes may also have the aforementioned five criminal characteristics, and there are other obstacles or challenges in related criminal investigations, as described below.

A. Illegal activities on the darknet

One of the challenges in detecting cryptocurrencies is illegal activities on the darknet. The illegal activities of the dark web are closely related to virtual currency. Virtual currency enables criminals to engage in underground illegal operations (such as the sale of drugs) and escape money laundering investigations. Criminals want to avoid being survielled by others in the process of paying for virtual currency or data transmission. As such, many anonymous networks such as the Onion browser (Tor) have gradually received attention, and many illegal websites have also begun to flourish. Darknet transactions are prevalent with crytocurrency as the means of payment, of which Bitcoin is the largest. Since cryptocurrency can hide the real identity of users, it can also evade government and bank

supervision. According to a study by Chainalysis, a blockchain analysis organization, the average Bitcoin transaction volume in the darknet market in 2018 was as high as US$2 million per day. As in the aforementioned "Silk Road" money laundering case, the website also provides the provision of crimes such as contract killing and human trafficking in addition to drug dealing.

The use of Bitcoin for third-party payment is an online payment method that has gradually been widely valued by the world in recent years. This method combines both virtual currency (Bitcoin) and existing online payment technology, and uses the CNC server (Command & Control Server) and the Internet bot virus, to create a new "complex criminal behavior" and method to “hide criminal cash flow”. However, when the criminal perpetrator uses Bitcoin to launder money quickly and frequently, it may also be the criminal's "fatal weakness". Although cryptocurrency transactions are secret, the blockchain they use allows law enforcement agencies to track criminal activities based on the data recorded on the blockchain. This actually provides law enforcement agencies with tools that can identify "users"; that is, most law enforcement agencies actually hope that these criminals will continue to use

cryptocurrency to fund illegal activities, as this will make investigations easier. The Global Ledger on the blockchain also provides good clues for investigators: government departments and others can view the information without subpoenaing any banks.

FATF regulatory guidelines suggest that countries should ensure that virtual asset service providers (VASPs) must retain the necessary and accurate user information of the sender and the payee when transferring funds, and submit these information to the payee’s institution. The main features of cryptocurrency, however, seem to conflict with these regulatory guidelines. Most privacy coins emphasize that they are "completely anonymous and untraceable", which makes it almost impossible for privacy coins to meet FATF's requirements for retaining user information on virtual asset services. However, according to data from the United States Drug Enforcement Administration (DEA), although privacy coins other than Bitcoin are more attractive alternatives, they are currently too small in scale, and the world’s current major virtual currency exchanges have all delisted privacy coins. The current market for privacy coins other than Bitcoins is not sufficiently liquid to be a viable payment instruments for

criminals.

There have been numerous cases of crimes related to Bitcoin in Taiwan. For example, taking Bitcoin as an example of criminal crimes, criminals who use Bitcoin as the subject of fraud to obtain property, instead of using legal currency as the subject of illegal money collection, commit the crime of fraud and profit. This is very different from the traditional method of illegal fundraising (the Taiwan High Court 107 Jin Son Zi No. 83 Criminal Judgment); the Taipei District Court also ruled in 2013 in case about a suspect who used the Internet to download the anonymous Internet browser package software Tor, and then opened an account on the Mt.Gox bitcoin trading website, transfered a considerable amount of U.S. dollars into that account, and then logged on to the "Silk Road" website to pay Mexican and Italian sellers, in Bitcoin, for the purchase of cannabis and had them delivered to designated locations within Taiwan. As a result, he was convicted of the ordinances on the prevention and control of drug harm (the Taipei District Court Su Zi No. 222 and No. 644 Judgments). In addition to the problem of dummy accounts, in order to avoid being surveilled by others in the process of payment of encrypted currency or data transmission, many

anonymous networks like the Tor network have gradually received the attention of drug traffickers. Many illegal websites have also begun to flourish. For example, in the aforementioned "Silk Road" money laundering case, this website also provides the provision of crimes such as contract killing and human trafficking in addition to drug dealing.

B. The flow of illegal income from Cryptocurrency is difficult to grasp

In recent years, due to the prevalence of cross-border transactions in virtual currencies (which have the same five characteristics as mentioned previously), criminals have used virtual currencies to launder money as such currencies are easily used by criminals to avoid tracking. Analysis using the three stages of typical money laundering behaviors shows that virtual currencies are clearly used for money laundering. Illegal funds (placement) are transferred to virtual currency wallet addresses (layering), and finally transferred to other virtual currency trading platforms or businesses to be used to purchase other services, commodities, and even legal currency (integration). For money laundering, the currency flow of the above-

mentioned multi-layered virtual currency is usually extremely complicated, which makes it difficult for law enforcement agencies to grasp the flow of criminal proceeds.

However, crytocurrency is not as unmanageable and invisible as imagined. The reason is that although crytocurrency is anonymous (there is no real-name requirement for opening a crytocurrency wallet), another feature is that all transaction records are recorded in the blockchain. The blockchain distributed ledger has the "transparency" of the transaction process. This feature has also become an opportunity for investigating money laundering crimes.

Taiwan Money Laundering Control Act announced an amendment bill on November 7, 2018. According to Article 5, Item 2 of the law, cryptocurrency platforms and trading businesses are subject to the provisions of the law on financial institutions, including the establishment of internal money laundering prevention systems, control and audit system, conduct confirmation of customer identity, record keeping, declaration of currency transactions above a certain amount, and declaration of suspected money laundering or terrorist transactions. In addition, FATF has

required virtual asset (cryptocurrency) service providers to follow FATF's 15th recommendation and other anti-money laundering regulations.

On November 7, 2018, the Executive Yuan designated the Financial Supervisory Commission as the authority in charge of money laundering prevention for this industry, and on April 7, 2021, the scope of this industry was designated. In consideration of the recommendations issued by the FATF, the Executive Yuan formulated the "Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction" (hereinafter referred to as the "Regulation"). The virtual currency platform and transaction business enterprises specified in Article 2 of the Regulation refer to the following:

1. Exchange between virtual currencies and fiat currencies, such as New Taiwan Dollar (hereinafter referred to as NTD), foreign currencies, and currencies issued by Mainland China, Hong Kong, or Macao.

2. Exchange between one and more forms of virtual currencies.

3. Transfer of virtual currencies.

4. Safekeeping or administration of virtual currencies or instruments enabling control over virtual currencies.

5. Participation in and provision of financial services related to an issuer’s offer or sale of virtual currencies.

In other words, virtual currency companies outside the scope of this business (typically wallet software companies that "do not provide safekeeping of private keys") and those who are not part of Taiwan's money laundering prevention law system may have the possibility of creating loopholes in the money laundering prevention system. The research conducted a focused discussion to understand the relevant virtual currency investigation practices, the illegal proceeds of related financial technology crimes, and concluded that, indeed, the above-mentioned loopholes were used to launder money or transfer the illegal proceeds to the dummy accounts to complete the concealment of the illegal proceeds. Due to the lack of currently available investigation tools, the flow of virtual currency is difficult to be grasped by investigative agencies.

In addition, Article 7 of the Regulation[ie "Travel Rule"] stipulates“” that, "If this business acts as the transferor of virtual currency transfers, it shall obtain

necessary and correct customers who transfer cryptourrency (hereinafter referred to as "transferor"). The information and necessary customer information for receiving virtual currency shall be kept, and the previous information shall be kept, and the previous information shall be provided immediately and safely to the business acting as the receiving party. When requested by the prosecutors and judicial police agencies to provide them immediately, should cooperate with the handling...; if this business acts as the recipient of virtual currency transfers, appropriate measures should be taken to identify whether the virtual currency transfers lack the necessary information, and appropriate follow-up actions should be taken, and information about the originator and receipient of the acquired transfers should be kept." Therefore, if the statutory obligations of the travel rules are implemented, the real-name system and virtual currency cash flow information such as the transferor and recipient of the virtual currency can be controlled by the judicial investigation agency.

In October 2018, FATF revised and approved the 15th recommendation, mentioning that countries should ensure that virtual currency service providers (VASPs) are

supervised to prevent money laundering and terrorism financing. In June 2019, the FATF issued the 15th recommendation which contained specific guidelines for supervising virtual currency service providers. Subsequently, the FATF issued a review report in June 2020, promising to further revise the guidelines and evaluate and amend the proposal for Article 15; FATF also issued the draft guidelines for the prevention of money laundering by virtual currency operators in March 2021 (hereinafter referred to as the "FATF Draft Guidelines"), and just ended the public comment process in April of the same year. FATF is expected to discuss and announce the final version of the draft guidelines in October 2021, including the revised definition of virtual currency, the scope of applicable industry, specific recommendations for preventing money laundering, and whether to establish a "Travel Rule", etc. After the FATF issued the above draft FATF guidelines (including the Travel Rule), due to the considerable range of amendments to the existing money laundering prevention standards and measures, and the related obligations of virtual currency operators have been greatly increased, industry associations and academic institutions in various countries have publicly expressed

many opinions. Whether the standards set by the FATF guidelines draft will be officially announced in the future is still inconclusive; therefore, most of the current governments have not yet initiated formal amendment procedures in accordance with the draft FATF guidelines, including the provisions of Article 18 of Regulation: "Except for Article 7 which will be implemented separately by this Council, it will be implemented on July 1, 100th year of the Republic of China. " Therefore, under the current law, if the flow of virtual currency involves the transfer between different virtual currency platforms, especially if it involves foreign virtual currency platform operators (without establishing a branch or subsidiary in Taiwan), the flow of related virtual currency will also be difficult to be grasped by investigative agencies, which increases the difficulty of investigating and detaining illegal gains.

Chapter 3. Empirical Analysis and Typology of Types of Crimes by Electronic Payment Tools

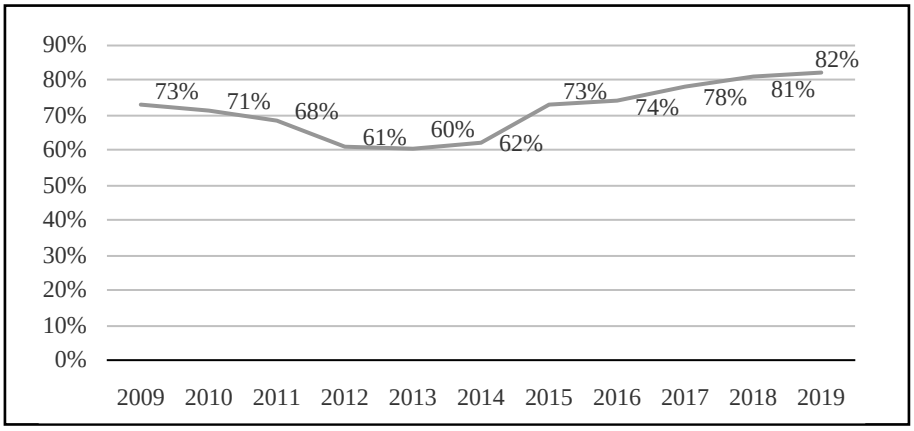
1. Analysis of the Trend of International Development

This study found that the types of crimes involved in electronic payment tools are mainly fraud and money laundering. The following is a brief introduction.

Fraud has always been one of the main types of crime faced in international business activities. According to a study by Association for Financial Professionals (AFP) in 2020, the number of fraud in B2B trading activities has increased significantly in the past five years. As shown in Figure 1 below, by 2018 and 2019, more than 80% of the interviewed institutions stated that it had encountered fraud.

Figure 1

Fraud rate of international business organizations (2009-2019)

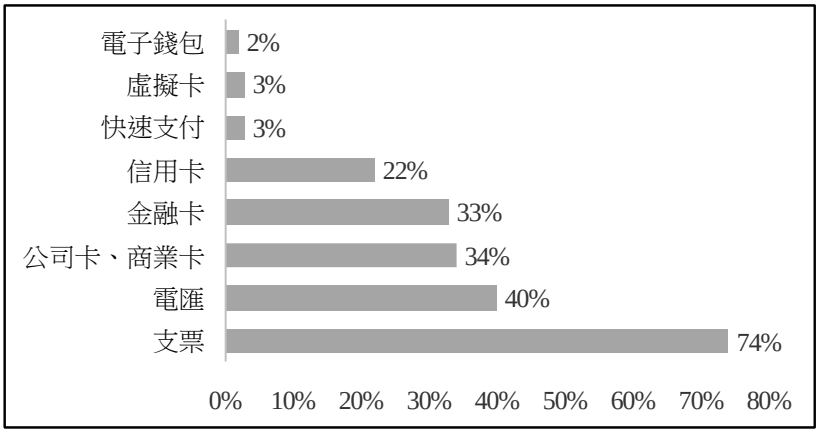


Note: 2020 AFP Payments Fraud and Control Survey Report: Key Highlights

With the changes in payment methods in recent years, the payment methods used in fraudulent activities have also changed to a certain extent. As shown in Figure 2 below, the largest payment methods used in fraudulent activities are still cheques and wire transfers, followed by credit cards, financial cards, corporate business cards and other automatic transfer services (Automated Clearing House, ACH). However, emerging payment methods such as fast payment systems and even electronic wallets have gradually become the payment methods used by fraudulent activities.

Figure 2

Fraud payment methods used by international business organizations (2019)



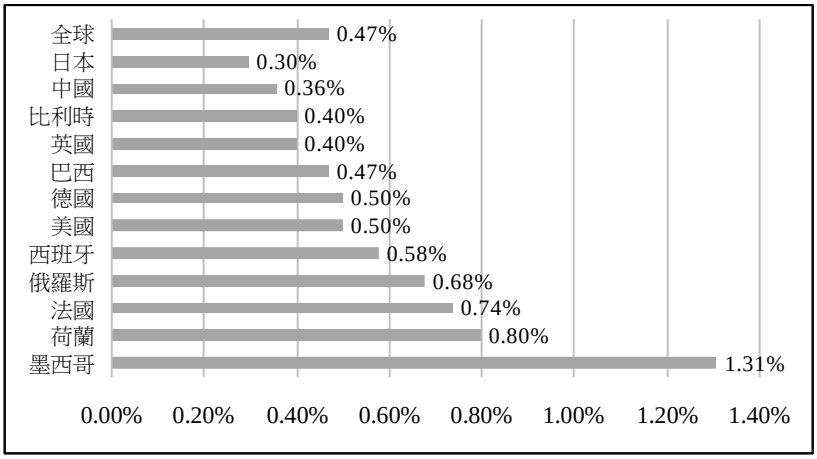
Note: 2020 AFP Payments Fraud and Control Survey Report

With the development of e-commerce in international business activities, derivative online payment of fraud has also received considerable attention. According to the statistics of Ingenico Payment Services, if the rate of online payment of fraud is calculated based on the ratio of the value of large companies' transaction fraud to the total transaction value, the global online payment fraud rate is about 0.47%. For a single country, as shown in Figure 3, the top three with the highest ranking are Mexico (1.31%), the

Netherlands (0.80%) and France (0.74%).

Figure 3

Online payment fraud rate in major countries

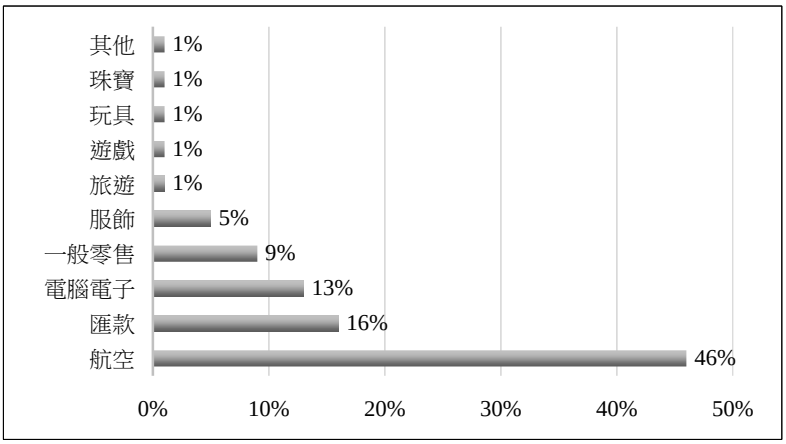


Note: Online Payment Fraud Whitepaper 2016-2020

In terms of industry, online payment fraud is relatively concentrated in a number of specific industries. Based on the number of fraudulent transactions accounting for the total number of transactions, as shown in Figure 4 below, the aviation industry (46%), the foreign exchange industry (16%), and the computer electronics industry (13%) have relatively high proportions of fraudulent transactions.

Figure 4

Proportion of online payment fraud transactions in major industries



Note: Online Payment Fraud Whitepaper 2016-2020

2. Statistics of crimes involving domestic payment instruments

This research is based on the Judgment Query System of the Judicial Yuan, using keywords: "electronic payment", "third-party payment", "mobile acquiring", "mPOS", "mobile electronic ticket", "mobile credit card", " "Mobile Banking Card", " GAMA PAY ", "International Link", " Pay2go ", "ezpay", " JKOPAY ", " O'Pay ", "Red Sun", "Green World", "Lanxin", "Alipay", "Youyoupay", "Gash",

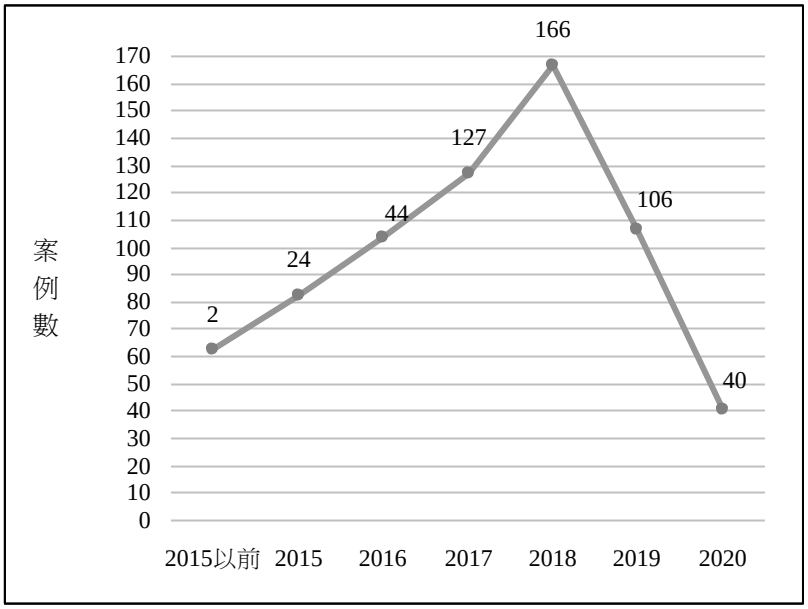
"Taiwan pay", "Line Pay", "androidpay", "samsungpay", "applepay" and "pay", collected from 2014 to July 29, 2021 The search initially found 2,070 results. After screening judgments not related to the use of payment instruments for crimes, a total of 1,078 judgments related to payment instruments were finally obtained. After further sorting and classification of this research, preliminary observations show that payment instruments are mainly used in the following five types of crimes in Taiwan:

A. Using payment instruments to commit fraud

This type of crime mostly involves criminal groups using information voluntarily provided by certain individuals to apply for the establishment of electronic payment companies or third-party payment companies, or using the criminal perpetrator’s own account, to inflict fraud on the victim by inducing the victim to wire money to the accounts through convenience stores. Figure 5 below shows the year-on-year trend of this type of crime, which has shown a trend of yearly growth until 2018.

Figure 5

Time distribution of crimes in payment instutment fraud cases



Note: Drawn by the research team.

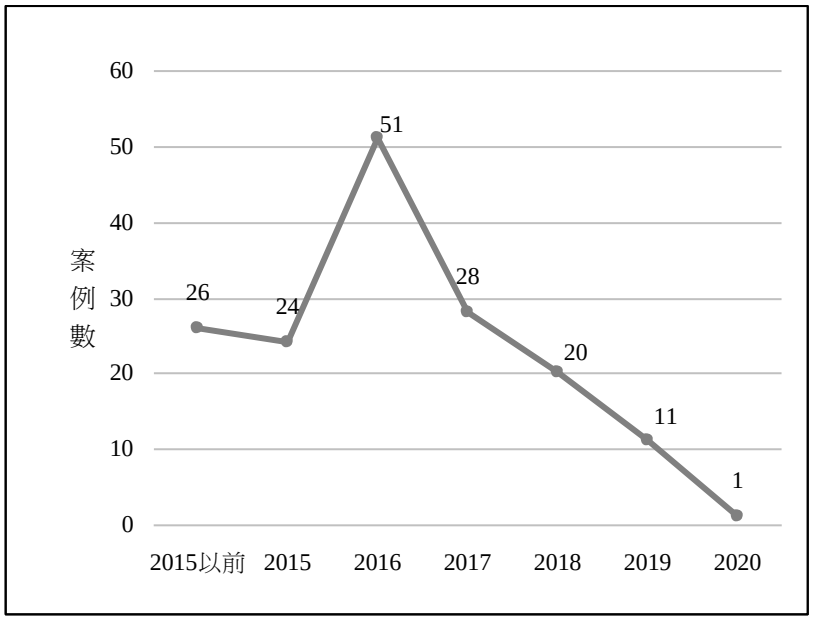
B. Online gambling deposits

This type of crime generally involves criminals operating online gambling platforms and using electronic payment or third-party payment providers to connect to designated bank accounts, allowing gamblers to use supermarket/convenience store printing codes or

remittances to make payments to the defendant. Figure 6 below shows the trend of this type of crime. We observe that most incidents of this crime are mainly concentrated in 2016.

Figure 6

Time distribution of crimes in online gambling deposit cases



Note: Drawn by the research team.

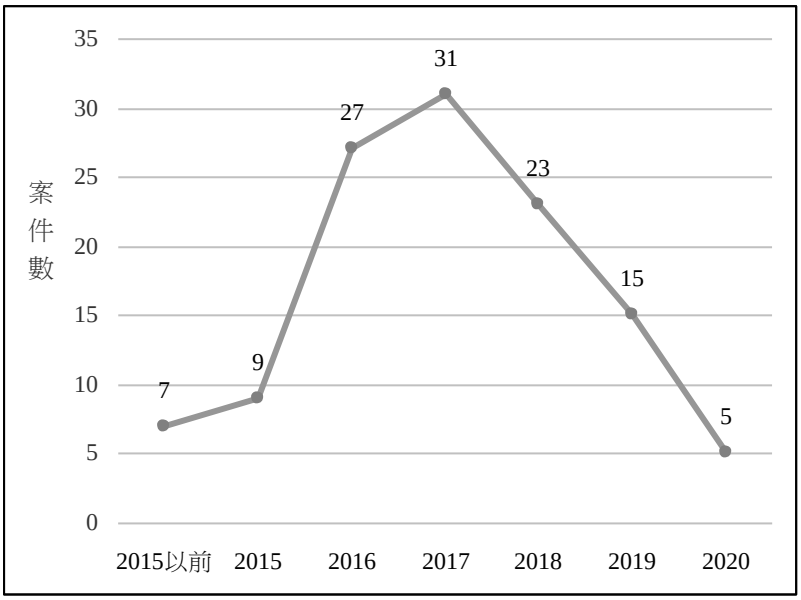
C. Theft of electronic payment account for consumption

This type of crime mainly uses credit cards or payment accounts as criminal objects or tools. This mostly involves the defendant stealing the victim's credit card, debit card, or digital account information, and using it to purchase things online through the payment service provided by online merchants. Therefore, under this type of crime, the payment service mainly acts as the financial intermediary of the crime, and the subjects involved include card issuing banks, payment service providers, consumer merchants, criminal perpetrators and victims.

Figure 7 below shows the trend of this type of crime. We observe that most incidents of this crime are mainly concentrated from 2016 to 2018.

Figure 7

Time distribution of crimes of stealing other people's information for consumption use



Note: Drawn by the research team.

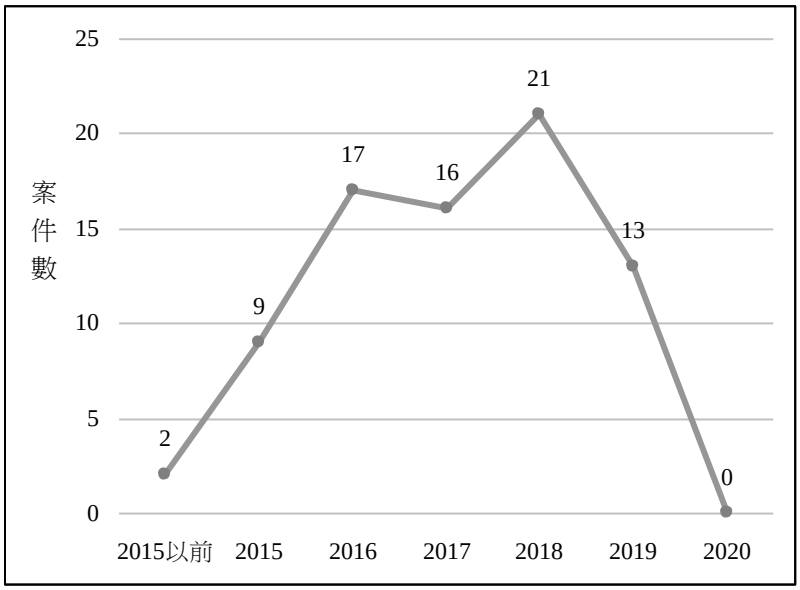
D. Theft of personal information to create fraudulent payment account

In this type of crime, the perpetrator first obtains the victim's personal information, including identity information, bank account information, credit card or

telecommunications number, etc., and then binds the information to a specific payment account, and conducts consumption or fraud based on this information. Figure 8 below shows the trend of this type of crime. We observe that most incidents of this crime are mainly concentrated from 2016 to 2018.

Figure 8

Time distribution of crimes of embezzling other people's information to set up payment accounts



Note: Drawn by the research team.

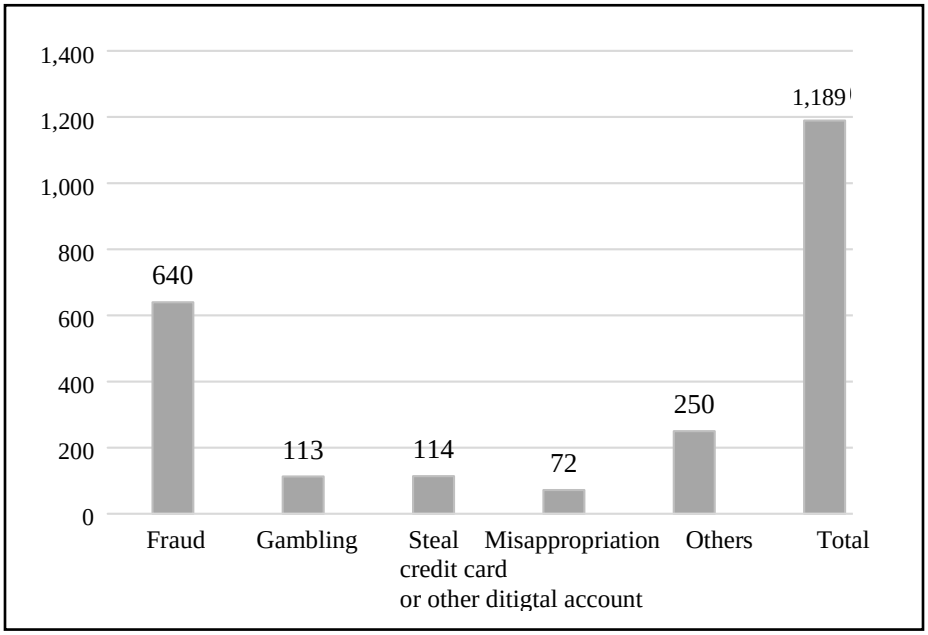
E. Others

In addition to the four common types of crimes mentioned above, this study also examines some smaller but representative crime types for reference, including illegal handling of domestic foreign exchange, illegal operation of multi-level MLM, illegal operation of futures consulting industry, etc. These crimes mostly involve a large number of victims and a large number of payment delivery activities, which have the need for remote payment. The characteristics of payment tools may help the scale of such crimes to expand and also reduce costs. In summary, in the criminal judgments of local courts found in this research, the distribution of the number of various types of crimes is shown in Figure 9 below. Among related crime types, fraud cases accounted for the highest proportion, with 640 cases recorded in the judgments collected in this study, about 53.9%. The remaining crimes are distributed in descending order: 112 online gambling deposit cases (approximately 9.4%), 114 (approximately 9.5%) of stealing credit card or digital account information of others, and 72 cases of embezzling other people's information to set up payment

accounts (approximately 6%), and a total of 250 other cases (approximately 21.2%).

Figure 9

Distribution of types of criminal cases involved in payment instruments



Note: Drawn by the research team.

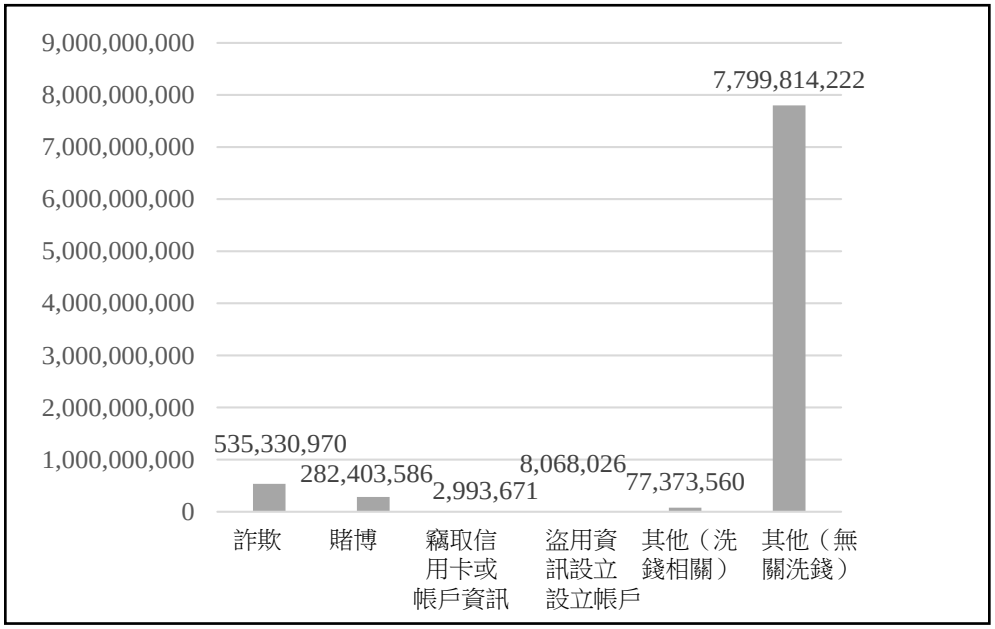
Among different payment tools, third-party payment and electronic payment are most commonly used in crimes. Common payment companies involved include Green World (235 cases in total), OuPay (214 cases in total), Lanxin (172 cases in total), Alipay (158 items in total), Hongyang (54 items in total). In addition, among the searched cases, a

total of 947 were local-based cases, accounting for approximately 87.8% of the total number of judgments, and the proportion of foreign-related cases was approximately 12.2%. Among the foreign-related cases, the number of cases involving mainland China is the largest, with a total of 124 cases, of which most are cases involving fraudulent syndicates and illegal operations of domestic foreign exchange, and most of the payment tools used are Alipay.

Finally, in terms of the amount of crime, Figure 10 shows the statistics of the amount of crime involved in various payment instruments. This figure shows that although the number of cases not involving money laundering crimes is relatively small, the monetary amount involved is considerable, involving more than NT$7.7 billion. In comparison, the number of fraud cases accounted for 53.9% of total, involving roughly NT$530 million. It is obvious that there are a large number of fraud cases, but the average monetary amount of each crime is low.

Figure10

The distribution of the monetary amount of crimes involving payment instruments



Note: Drawn by the research team.

3. Summary

Through the above-mentioned empirical research on judicial judgments, this study found that most fraudsters engage in fraud using dummy accounts. In addition, the proportion of cases where criminals embezzled the identity of others or other information to create payment service

accounts is also considerable, which shows that there is a risk that the current establishment of payment accountsmay be flooded with false information. The foregoing will lead to difficulties in tracing the cash flow of related property crimes, and because the application cost of the account is relatively low, it may also have a considerable degree of attraction for criminals as well. In the subsequent chapters of this research, relevant policy research and suggestions will be put forward in order to reduce the possibility of related crimes.

In addition to fraud cases, this research also found that the monetary amount of crimes involving payment tools used in certain illegal financial activities and online gambling is higher than other crimes. The preliminary conclusion is that such a result is related to the "fastness" and "cross-border nature" of payment tools. The above characteristics help criminals to quickly engage in the cross-border collection of money, which in turn helps the gaming industry to expand the scope of their online gambling business to not be limited to the participation of people in specific areas.

The last supplement is that this study recognizes that the criminal methods related to payment tools are changing

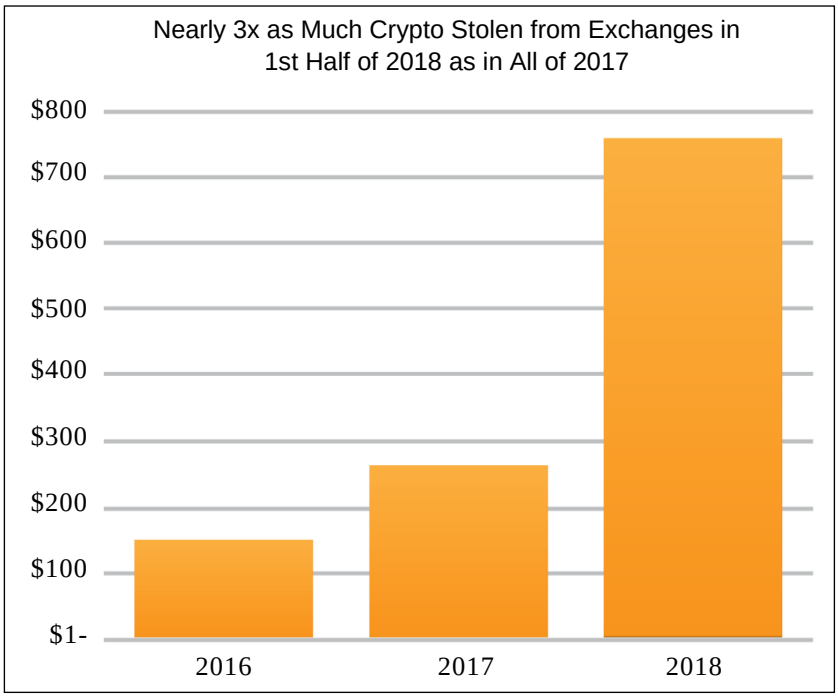
day by day, and there is often a time difference between the time when the judgment is made and the time when the crime is committed. Therefore, the crime trend summarized by the empirical study of judicial judgment alone may not fully reflect the current status of such crimes and related investigation. This is an inevitable limitation of this research method.

Chapter 4. Analysis of Types of Crimes Involving Virtual Currency

1. Global trend analysis

The stunning growth in the value of virtual currencies like Bitcoin in recent years has attracted investors, speculators and thieves. In 2017 and 2018 alone, a small number of criminals have gained US$1.21 billion in virtual currency equivalent from virtual currency exchanges. The virtual currency (value) stolen in the first half of 2018 alone was three times that of the entire year of 2017.

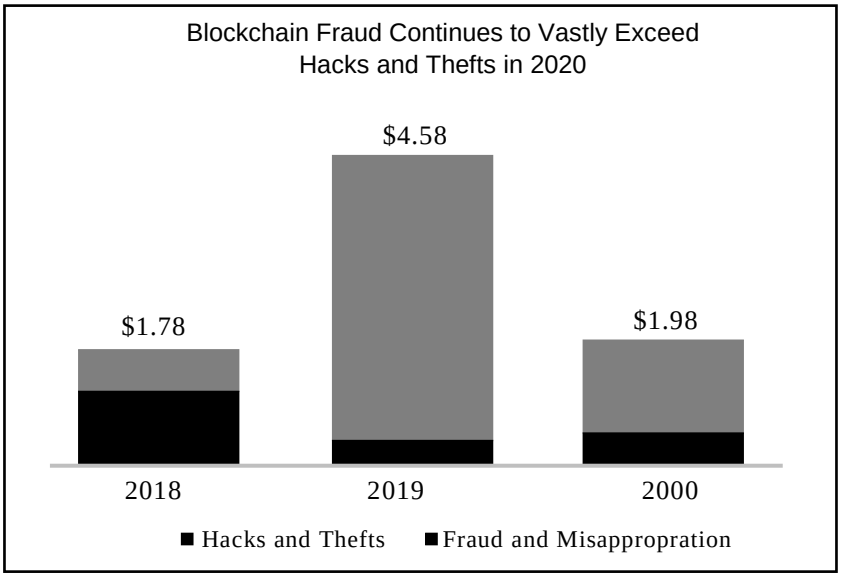
Figure 10: The value of virtual currency stolen from the exchange from 2016 to 2018



source：Q2 2018 Cryptocurrency Anti-Money Laundering Report。

B. According to the virtual currency crime and anti-money laundering report released by CipherTrace in 2020, the total amount of criminal proceeds related to virtual currency, hacking, and fraud in 2020 reached 1.9 billion U.S. dollars, the second highest in annual history. But there was a significant drop compared with the 4.5 billion U.S. dollars in 2019.

Figure 11: Trends in virtual currency fraud and hacking from 2018 to 2020



Note：Cryptocurrency Crime and Anti-Money Laundering Report, February 2021。

C. In the past two years, large-scale cross-border online scams have become one of the main sources of virtual currency crime. The PlusToken Ponzi scheme that broke out in 2019 generated up to 2.9 billion U.S. dollars in illegal gains, accounting for 64% of the amount of crime involved in virtual currency in that year. In 2020, WoToken broke out. It was an MLM plan operated by the MLM

structure, which was similar to PlusToken. By the time WoToken disintegrated, it defrauded investors of more than 1.1 billion U.S. dollars, accounting for 58% of the total amount of fraud losses in 2020. Although the number of major frauds involving virtual currencies has decreased significantly in 2020 as compared with the past, it still accounted for 73% of the total crimes in 2020.

D. The data shows that the number of cyber hacking attacks (including theft) and fraud incidents that occurred in 2020 is the same as in 2019 (it has stopped growing), and the illegal gains involved in crimes in 2020 have significantly declined as compared to 2019; the average profit per crime in 2019 was 160% higher than in 2020, indicating that strengthening the information security system and taking preventive measures can effectively respond to internal and external threats. In 2020, the KuCoin virtual currency exchange was hacked and lost US$281 million. However, the KuCoin exchange stated that it has recovered 84% of the stolen funds. Such cases have almost been unheard of in the past few years.

E. In 2020, more than half of the cases of hackers stealing virtual currency adopted the DeFi protocol (this model was very rare in the past, almost negligible), but in

the second half of 2020 alone, 99% of major frauds were derived from the DeFi agreement. This emerging criminal behavior shows that the vigorous development of Defi's virtual currency economic activities has led to rampant criminal behavior, similar to the ICO mania in 2017.

In summary, virtual currency has become a hotbed of money laundering and a tool used by criminals due to its characteristics of "anonymity", "carrier of economic value", and "incomplete supervision of virtual currencies in various countries". Virtual currency also poses challenges to traditional financial supervision. For instance, when using ICO (Initial Coin Offering) and Defi agreements to raise (or absorb) virtual currency around the world, because of the cross-border nature of virtual currency, current securities laws and regulations are unable to regulate such cases.

2. Statistics of domestic virtual currency crimes

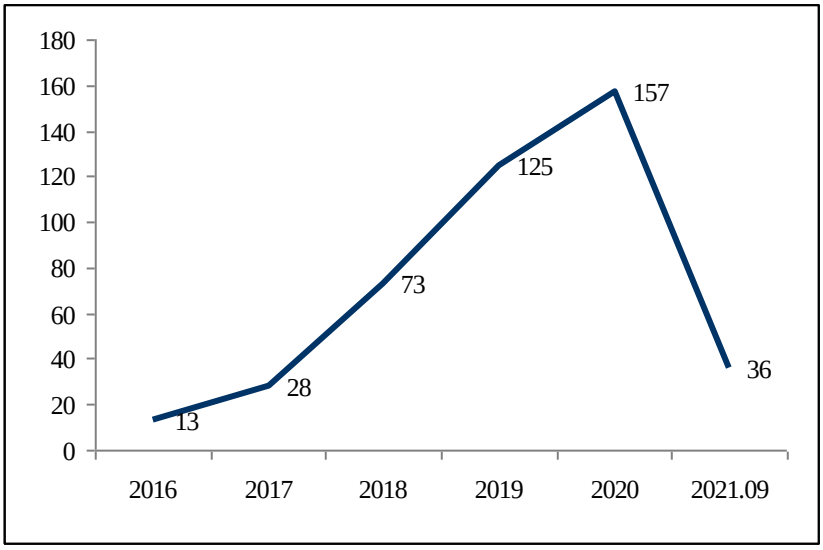
According to the search results of judgments on the Judicial Yuan’s Judicial Database, from 2016 to September 27, 2021, a total of 919 court criminal judgments were found using keywords such as virtual money, virtual currency, and encrypted currency. Excluding the judgments that mention the above keywords but are not substantively

related, a total of 819 cases were ultimately analyzed. In these 819 court judgments, based on the defendant's use of virtual currency in crimes, we found that based on the criminal charges and the manner in which virtual currency is used, they can be classified into the following six types of crimes:

A. Virtual currency as transaction subject

The defendant used virtual currency as the subject of investment or trading. The basic method is that the fraudster falsely claims that it is selling virtual currency, or hold seminars to defraud victims and conduct illegal fundraising, tricking victims to remit money. This type of crime began to increase rapidly in 2018 and reached a peak in 2020. According to this research, the rapidly increasing number of cases is related to the false trading, embezzlement, and investment disputes of virtual currency. This type of case is currently the largest type, with a total of 432 cases, accounting for 53% of the total number of six types of cases.

Figure 12: Trend chart of the “virtual currency as transaction subject” type cases over the years

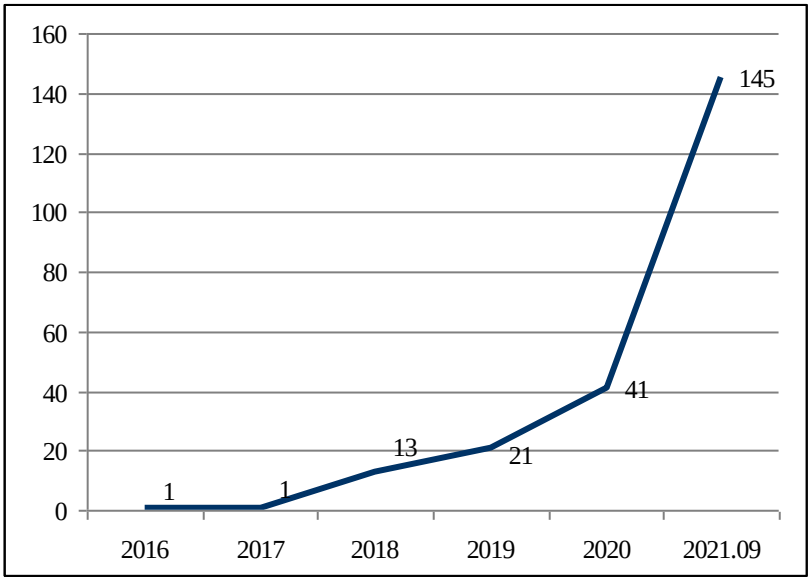


Note: Drawn by the research team.

B. Providing personal information

These cases involve the provision of personal information such as financial accounts and mobile phone numbers, or serving as a “driver” of a fraudster, in furtherance of fraud or money laundering. This type of criminal tactics is not new, but the number of cases which use virtual currency as bait began to increase year by year in 2018, and suddenly increased sharply in 2021. This type of case is currently the second most numerous case type, with a total of 222 cases, accounting for 27% of the total number of six types of cases.

Figure 13: Trend chart of the “providing personal information” type cases over the years



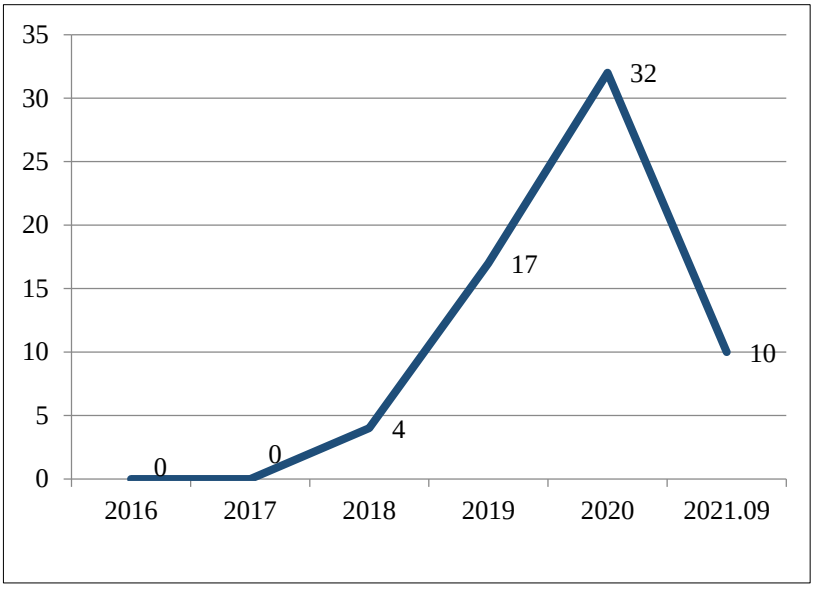
Note: Drawn by the research team.

C. Providing virtual currency account

Under current regulation, all the major virtual currency exchanges in Taiwan are required to implement user's real-name authentication procedure when users apply for accounts. Users should provide personal name, mobile phone account number, email address and other information and verify them before they can start trading. In these types

of cases, the defendant rents out or sells his account registered on the virtual currency exchanges to fraudsters, and thus constitutes the crime of helping fraud or money laundering. This is a new type of crime as it had not occurred before 2018, and it began to appear in 2018, and it has grown rapidly in recent years. The total number of such cases is 63, accounting for 8% of all six types of cases.

Figure 14: Trend chart of the "providing virtual currency account" type cases over the years



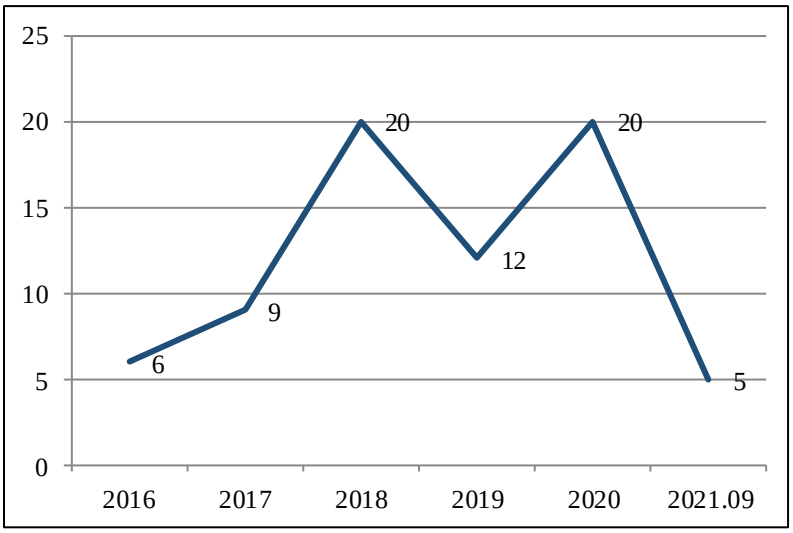
Note: Drawn by the research team.

D. Virtual currency as consideration

In this type of case, the defendant takes advantage of the secrecy and convenience of virtual currency to use virtual currency as a transaction price for buying or selling prohibited items, and is ultimately convicted of violating the Narcotics Hazard Prevention Act or The Smuggling Penalty Act.

Court judgements regarding cases of using bitcoin to pay for drugs first appeared in Taiwan in 2017, although there were also cases of using game currency to buy drugs before. In addition, some defendants paid virtual currency through anonymous dark web, decentralized exchanges wallets, or convenience store payment machines. The total number of such cases is 72, accounting for 9% of all six types of cases.

Figure 15: Trend chart of the “virtual currency as consideration” type cases over the years



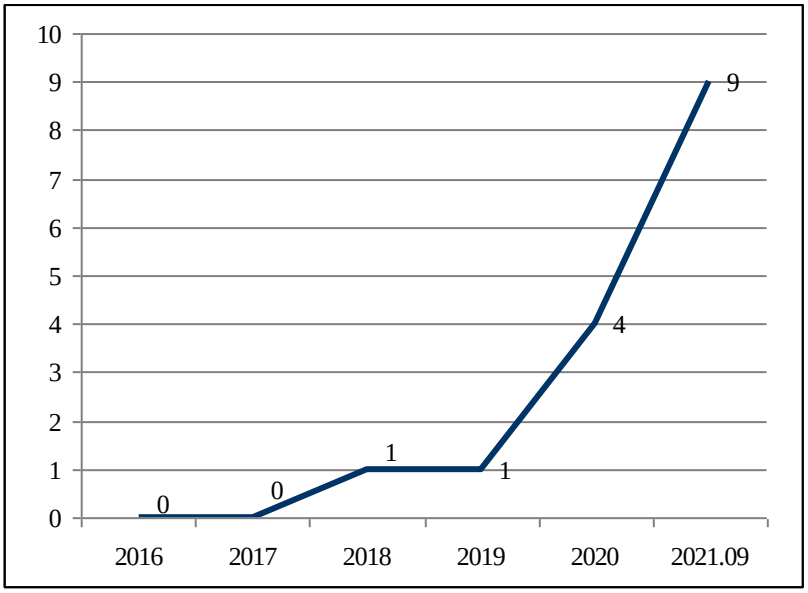
Note: Drawn by the research team.

E. Money laundering

The defendants used virtual currency as money laundering tool in this type of crime. They first committed fraud, theft or other crimes, and then converted the money generated by fraud and theft into virtual currency or transferred it to a virtual currency wallet with a non-real name system to cut the payment flow to avoid detection. This type is an emerging crime case that began to appear in 2018, with a total of 15 cases, accounting for 2% of all six types of cases.

Figure 16: Trend chart of the “money laundering” type

cases over the years



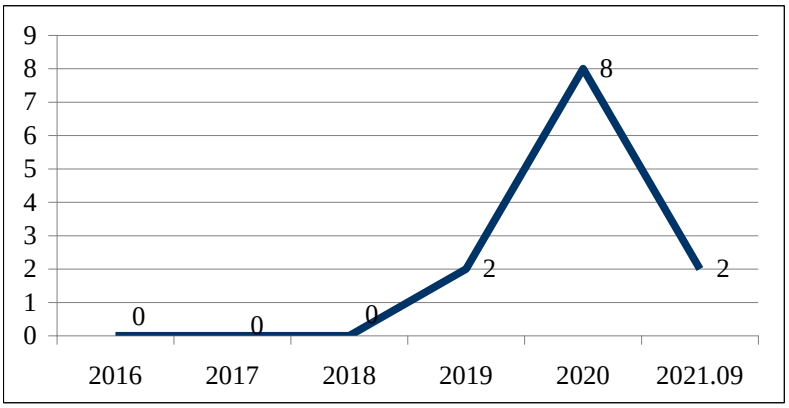
Note: Drawn by the research team.

F. Stealing electricity for mining

The principle of virtual currency mining is to use computer computing power to perform cryptographic calculations and decoding to obtain virtual currency. The calculation process requires a lot of electricity. In this type of crime, the defendant sets up a computer room and equipment to conduct large-scale virtual currency mining, and to provide electricity for mining, the defendant would

steal electrical energy by private electric wires, which is theft. This type of crime is a new type of crime that began to appear in 2019, with a total of 12 cases, accounting for 1% of all six types of cases.

Figure 17: Trend chart of the “stealing electricity for mining” type cases over the years



Note: Drawn by the research team.

3. Summary

The three types of crimes involving virtual currency in Taiwan are below: Using virtual currency as the subject of investment or trading; providing personal information such as financial account or cellphone number, or serving as a

“driver” of a fraudster, and being charged for helping fraud and money laundering; renting or selling one’s account registered in a virtual currency exchanges to a fraudster.

Due to its characteristics, blockchain technology is easily used by money laundering criminals, and blockchain technology has become the money laundering tool for criminals. The problem of money laundering is unavoidable in the virtual currency field. However, there is a strange trend in Taiwan’s cases: in the past three years, a large number of defendants have provided personal information for fraudsters to conduct virtual currency fraud, resulting in them being charged for helping fraud.

In addition, judgements involving the Money Laundering Control Act in Taiwan have seem to agree to a consensus on certain interpretations of the law. The court’s general interpretation is that the person who provides a personal Bitcoin wallet account or other type of virtual currency account to the fraudster is also the perpetrator of money laundering, if the illegal gains are deposited into the wallet. That is to say, the wallet account of virtual currency is considered similar to the bank account provided by the driver in the online fraud case. However, the wallet account of virtual currency is a product under decentralized

governance structure, which is different from an account provided by a financial institution. Whether such an interpretation by the courts runs contrary to the principle of legality and expand the penal power improperly, deserves further observation.

Chapter 5 Research conclusions and policy recommendations

1.This study analyzes foreign statistical data and empirical research on judicial judgments in Taiwan. It was discovered that as far as electronic payment tools are concerned, fraudulent groups in fraud cases using electronic payment tools often use dummy accounts to apply for mobile payment accounts. In addition, the proportion of cases where criminals embezzled the identity of others or other information to create electronic payment service accounts is also considerable, which shows that the current establishment of electronic payment accounts is at risk of being flooded with false information. Among the cases, a certain proportion of cases involved third-party payment service providers and convenience stores which, combined with the aforementioned creation of a large number of dummy accounts, has resulted in challenges for investigations and the tracing of related cash flows. In addition, as far as virtual currency is concerned, there are still endless cases of abuse of virtual currency in crime both

internationally and domestically, and because of the gradual growth of related economic activities, the abuse of virtual currency in crime is also increasing in severity year by year. Virtual currency operators can implement measures such as money laundering prevention and anti-capital terrorism, which can indeed prevent crimes effectively, or minimize the scope of influence after crimes occur.

2. The research team would like to make specific research suggestions as follows, in order to reduce the possibility of related crimes:

A. To implement money laundering prevention measures for electronic payment tool:

   a. On August 18, 2021, the Executive Yuan issued Yuantaifazi No. 1100181600 to authorize the designation of third-party payment services as non-financial enterprise or personnel per Article 5, Paragraph 3, Subparagraph 5 and Article 5, Paragraph 4 of the Money Laundering Prevention Law. Current law has relatively clear requirements that electronic payment tool-related businesses (including electronic payment institutions and third-party payment businesses) must have the obligation

to prevent money laundering. The focus of the next step is to implement relevant measures for the prevention of money laundering by electronic payment companies, including customer identification and continuous review, transaction data preservation and suspicious transaction reporting, etc. In addition to relying on electronic payment tool related companies to establish internal legal compliance procedures, they must also rely on the competent authority to implement external supervision to urge the industry to implement money laundering prevention measures. Therefore, the competent authority should regularly and irregularly check the anti money laundering measures of electronic payment tool companies.

b. Among the electronic payment tool related businesses, there are currently only 5 electronic payment institutions that are specialized in business, so the pressure on the competent authority is still controllable; however, there are currently 13,113 third-party payment providers registered, and the competent authority is obviously unable to supervise all of them.As such, it is necessary to adopt risk-

based supervision according to the money laundering risk and scale of the businesses. In addition to relying on the external supervision of the competent authority, after the right and responsiblities of the competent authority's supervision of the third-party payment industry have been clarified as described above, this research suggests that the inspector must obtain relevant information from the electronic payment tool related industry for the investigation of crimes. If it is discovered that any business has not fulfilled the obligation to prevent money laundering, they can take the initiative to notify the competent authority for inspection and punishment so as to integrate the resources of the executive branch of the government so as to moderately relieve the external supervision pressure of the competent authority.

B. It is recommended to set the effective date of Article 7 (travel rules) of the Measures for the Prevention of Money Laundering and Anti-Terrorism Measures for Virtual Currency Platforms and Transaction Business Enterprises as soon as possible.

a. Based on our observation of the current investigation practice of virtual currency crimes, it can be seen

that the illegal gains involved in virtual currency crimes are often laundered through the virtual currency industry, or through the use of dummy account to conceal the illegal gains , and the flow of related virtual currency is difficult to be investigated by the investigative agency.

b. In October 2018, the FATF revised and approved the 15th recommendation, mentioning that countries should ensure that virtual currency service providers (VASPs) are regulated to prevent money laundering and terrorism funding. In June 2019, the FATF issued the 15th recommendation and specific guidelines for supervising virtual currency service providers. The FATF's review report issued in June 2020 promised to further revise the guidelines and evaluate the proposed amendments to Article 15. FATF also issued a draft FATF guidelines in March 2021, including the revised definition of virtual currency, the scope of applicable industry, and specific recommendations to prevent money laundering and whether to formulate a "Travel Rule", etc. Due to the huge range of amendments to the existing money laundering prevention standards and

measures, and the substantial increase in the related obligations of virtual currency operators, industry associations and academic institutions in various countries have expressed many public opinions on the draft FATF guidelines. Whether the standards of the draft FATF guidelines will be officially announced in the future are still inconclusive. Therefore, most of the current governments have not yet initiated formal amendment procedures in accordance with the draft FATF guidelines.

c. Article 7 of the Regulations stipulates the "Travel Rule", which requires the transferor and receiver of virtual currency to implement the real-name system and the preservation of virtual currency cash flow information, which should be able to effectively solve the problem of difficulty in detecting virtual currency flow by investigative agencies.

d. However, in accordance with Article 18 of the Regulations: "Except for Article 7 which will be implemented separately by the Association, the Regulations shall be implemented on July 1, 2021. " Therefore, under the current law, if the flow of virtual currency involves different virtual currencies

transferring between platforms, especially those involving foreign virtual currency platforms, the flow of relevant virtual currency is also difficult to be grasped by investigative agencies, which increases the difficulty of detecting and detaining illegal gains. Therefore, the study proposes to fix the implementation date of Article 7 at an appropriate time.

3.In order to reduce the occurrence of crimes involving emerging financial technologies including electronic payment tools and virtual currencies, the study proposes a number of policy recommendations as follows:

A. A database related to financial technology crimes should be established：

In order to balance the competing interests of supervision of and benefiting the financial industry, FATF clearly pointed out that the key is that the competent authority should adopt a risk-based approach to supervision. It is not advisable to terminate or restrict the business of related businesses without proper risk assessment and risk mitigation measures, otherwise it will cause customers to transfer to services or channels with higher criminal risks. Therefore, the research team tried to

conduct empirical research through the public judicial judgment database to clarify the situation of relevant financial technology companies engaging in criminal acts in Taiwan. However, the judicial judgment database only covers prosecuted cases and does not cover all crimes that have occurred, so there are still limitations with this method. In addition, according to the research team's understanding, the current government database does not specifically provide statistics on crimes involving electronic payment tools, virtual currency and other financial technology tools. Therefore, the criminal risk assessment of financial technology tools in Taiwan is indeed facing the challenge of insufficient empirical data. This study suggests that the relevant authorities can start to establish a database of financial technology-related crimes in order to assess the crime profile involved in financial technology tools in the long-term.

B.The digitization of criminal investigation data and other regulatory technologies should be strengthened：

With limited supervision manpower and resources, the concept of supervisory technology (SupTech) has been gradually valued in recent years. That is to say, the supervision agency uses technology to effectively

implement its supervision responsibilities, and through technological methods, it assists itself to supervise the huge and complex system as comprehensively and promptly as possible under its limited supervision resources. It is necessary to digitalize the database of the criminal investigation to implement supervision technology to make relevant technological methods such as big data analysis or artificial intelligence work. It is possible to establish digital database to analyze relevant data, and to truly grasp the crime risk profile of financial technology tools in Taiwan.

C. It is recommended to add criminal law provisions for forgery and alteration of digital payment instruments for the following reasons：

a. There are more and more diversified types of emerging payment tools that have no physical presence. Based on the principle of*nulla poena sine lege*, the provisions of Article 201-1 of the Criminal Law cannot be applied. As a result, the current criminal law only protects the authenticity of card-based payment instruments, but does not protect the authenticity of other payment instruments that are intangible, obviously reflecting the shortcomings of

the current criminal law.

b. The provisions of Article 201-1 of the Criminal Law were revised in 2001. At that time, card-type payment tools such as financial cards and credit cards were among the emerging payment tools of the era and crimes of counterfeiting and altering financial cards and credit cards emerged endlessly. Most of the crimes were carried out by corporate, diversified and transnational criminal organizations. It severely endangered the integrity of the payment system, thereby endangering the overall social and economic order. Therefore, the legislators decided to punish the act of forgery and alteration of card payment instruments with a higher penalty than the crime of fraud, and established a fixed-term imprisonment of not less than one year and not more than seven years. But the contextual background at that time was dominated by card payment tools, therefore, the crime was limited to "credit card, financial card, stored-value card or other similar electromagnetic record "object" as a means of spending, withdrawing, transferring or paying." In other words, it is limited to tangible

payment instruments.

c. Emerging payment tools need to first gain public trust, so it can maintain the basic transactional liquidity, and then meet the public payment demand. Forging and altering the account records of emerging payment instruments may affect the public's trust in emerging payment instruments. Furthermore, it is unfavorable for the development of new payment tools in Taiwan. Therefore, this research suggests that emerging intangible payment tools should be included in the relevant definition of the criminal offense .

d. The specific amendment suggestions for this study are as follows:

Amendments	Current provisions	Explanation
Article 201-2 A person who counterfeits or alters a electronic payment account record, third-party payment account record, virtual currency or other similar types of electromagnetic records used as payment tools used	（New in this article）	1.Consider the rise of emerging digital payment tools such as electronic payment, third-party payment, virtual currency, etc. in recent years. However, the first provision of Article 201 of the current Criminal Law is only applicable to tangible card-type payment instruments such

Amendments	Current provisions	Explanation
for closing a bill, withdrawing money, transferring money, or paying money, with the intention that it be put into use, shall be sentenced to imprisonment for not less than one year but not more than seven years; in addition therefore, a fine of not more than ninety thousand dollars may be imposed. A person who uses the counterfeit or altered a electronic payment account record, third-party payment account record, virtual currency or other similar types of electromagnetic records for closing a bill, withdrawing money, transferring money, or paying money or who takes such an instrument from or gives one to another with the intention to circulate shall be sentenced to imprisonment of not		as forged credit cards, financial cards, stored-value cards, etc. Therefore, it is necessary to update the scope offorgery and alteration of intangible digital payment instruments to protect the integrity of the digital payment system. According to the first provision of Article 201 1 of the Criminal Law, the first provision of this article is updated so that the criminal act of forging and altering digital payment electromagnetic records are included in the scope of the offense. 2.With reference to the second paragraph of Article 201 of the Criminal Law, the second paragraph of this article is revised to regulate the use, transfer, or transfer of forgery and alteration of digital payment electromagnetic records.

Amendments	Current provisions	Explanation
more than five years; in addition thereto, a fine of ninety thousand dollars may be imposed.		
Article 205 A counterfeit or altered security, postal or revenue stamp, credit card, bank card, value-deposit card, or any other electromagnetic instrument used for closing a bill, withdrawing money, transferring money, or paying money, or electronic payment account records, or third-party payment account records, or virtual currency or other similar electromagnetic records used as payment tools or specified in the preceding article shall be confiscated whether or not it belongs to the offender.	Article 205 A counterfeit or altered security, postal or revenue stamp, credit card, bank card, value-deposit card, or any other electromagnetic instrument used for closing a bill, withdrawing money, transferring money, or paying money, or an instrument or material specified in the preceding article shall be confiscated whether or it belongs to the offender.	Corresponding amendment.