ISSN Print: 2707-1499 Online: 2707-1502
Advance in Law − 2025, 7(2)
https://doi.org/10.35534/al.0702017

Criminal Law Characterization of Property Infringement Involving Third-Party Payment Platforms

Kai Zhang Zehui Zou

Shanghai University of Political Science and Law, Shanghai

Abstract: This paper aims to discuss the criminal law evaluation of a series of financial abuses in the background of the rise of third-party payment platforms. In the first part of this paper, the concept of the third-party payment platform and the financial abuse related to the third-party payment platform and its characteristics are introduced. Then, the second part discusses the disputes concerning the criminal law evaluation of financial abuse involving the third-party payment platform, including the causes of the qualitative disputes and the premise of the settlement of the qualitative disputes. The causes of the qualitative dispute mainly include the identification of the legal status of the third-party payment platform, the identification of the legal nature of the funds in the account, and the dispute over theft and fraud. The premise of resolving qualitative disputes includes the identification of the legal status of the third-party payment platform, the legal nature of the funds in the account, and the boundary between theft and fraud. Finally, this paper analyzes the qualitative problems of financial abuse related to third-party payment platforms, proposes that the qualitative problems should be based on behavioral means and property attributes, and pays attention to the problems of one crime and several crimes.

Key words: Theft; Fraud; Third-party payment; Alipay

1 Overview of Property Infringement Involving Third-Party Payment Platforms

1.1 Clarification of the Concept of Third-Party Payment Platforms

With the rapid development of the economy and society, new payment methods have emerged to address the shortcomings of traditional monetary transactions, allowing consumers to make payments through mobile terminals or other electronic media for an enhanced transactional experience. These new methods include mobile payments, e-cash, digital currencies, and third-party payments. Among these, third-party payment stands out as the most representative. It refers to a payment service provided primarily by non-financial institutions, supported by the internet and agreements

Corresponding author: Kai Zhang, Graduate student in Criminal Law, School of Criminal Justice (School of Discipline Inspection and Supervision), Shanghai University of Political Science and Law.
Article Citation: Zhang, K. & Zou, Z. H. Criminal Law Characterization of Property Infringement Involving Third-Party Payment Platforms. *Advance in Law, 7*(2), 192-199.

with major banks, leveraging their financial strength and social credibility to facilitate public transactions. This paper defines the non-financial institutions providing such services as third-party payment platforms—entities that act as neutral intermediaries between e-commerce businesses and banks, serving as "technical plugins" to enable fund transfers and services for online transactions. The most well-known examples are Alibaba's Alipay and Tencent's WeChat Pay, which offer one-stop shopping services, enabling users to make payments, receive funds, and transfer money. Compared to traditional methods, third-party payments are distinguished by their convenience, diversity, and internet-based nature.

1.2 Categories and Characteristics of Property Infringement Involving Third-Party Payment Platforms

1.2.1 Classification of Infringement Behaviors

Property infringement involving third-party payment platforms refers to acts where criminals exploit regulatory loopholes in these platforms to illegally appropriate others' assets through false or fabricated transactions, resulting in financial losses. These behaviors can be analyzed through two categories: non-transactional and transactional infringements.

(1)Non-Transactional Infringement: These acts target funds directly within victims' accounts, bypassing e-commerce platforms like Taobao or JD.com. Examples include stealing balances from Alipay accounts or funds from credit services like Ant Credit Pay and Ant Cash Now. Such acts share similarities with credit card fraud, as discussed later.

(2)Transactional Infringement: Transactions via third-party platforms are divided into offline (face-to-face) and online models. Despite differing scenarios, both follow a core process: buyers pay funds to the platform, which holds them until goods are delivered and confirmed. However, the risks of infringement differ:

• Offline Transactions: Sellers retain some oversight, limiting opportunities for buyer fraud. A notable example is "QR code swapping," where criminals replace a seller's QR code with their own to redirect payments. However, platforms have mitigated this risk by shifting to seller-initiated QR code scanning. Legal debates persist over whether such acts constitute theft or fraud.

• Online Transactions: The digital nature of online payments increases risks. Two common scenarios include:

• Exploiting Transaction Rules: For example, sellers listing low-priced goods with extended delivery times (e.g., 45 days), then closing shops after automatic payment release ("overtime transfer"), or falsely claiming shipment to trick buyers into confirming receipt ("deceptive payment").

• Cash-Out Fraud with Small Loans: Platforms like Alipay's Ant Credit Pay (a credit service) prohibit direct cash withdrawals, leading to collusion between users and merchants to simulate transactions. Criminals may further defraud users by cutting contact after receiving funds.

1.2.2 Characteristics of Such Infringements

(1)Convenience and Concealment: The internet's anonymity and accessibility enable perpetrators to commit crimes with minimal technical barriers (e.g., virtual IP addresses), complicating detection.

(2) Diverse Methods: Beyond direct theft, perpetrators exploit platform vulnerabilities to devise novel tactics like "overtime transfers" or "cash-out fraud."

(3) High Monetary Gains: The efficiency of digital platforms allows criminals to obtain sums far exceeding those from traditional theft.

1.3 Legal Disputes Over the Characterization of Infringements

1.3.1 Challenges in Legal Characterization

(1)Transactional Infringements

• QR Code Swapping: Courts debate whether such acts constitute fraud (by deceiving customers) or theft (by covertly diverting funds from merchants).

• Small Loan Cash-Outs: Legal opinions conflict over whether Ant Credit Pay cash-outs fall under credit card fraud (due to functional parallels) or loan fraud (as deliberate deception for illicit gains).

(2)Non-Transactional Infringements

• Account Hijacking: Disputes arise over whether unauthorized transfers via stolen credentials constitute fraud (by deceiving the platform) or theft (as a "secret" appropriation).

• Unauthorized Credit Card Binding: Debates center on whether binding a victim's credit card to a third-party account violates the credit card management order (as fraud) or merely constitutes theft.

1.3.2 Causes of Disputes

(1)Ambiguity in Platform Legal Status: Third-party platforms blur lines between financial and non-financial institutions, complicating determinations of fund ownership and platform liability.

(2)Unclear Legal Nature of Platform Funds: Whether funds in platform accounts qualify as "property" or "property interests" affects applicable charges (e.g., theft vs. fraud).

(3)Overlap Between Theft and Fraud: Evolving infringement tactics challenge traditional distinctions, necessitating deeper analysis of intent and deception mechanisms.

2 Prerequisites for Resolving Disputes Over the Characterization of Property Infringement Involving Third-Party Payment Platforms

2.1 Legal Status of Third-Party Payment Platforms

As previously discussed, third-party payment refers to a service provided primarily by non-financial institutions through internet-based agreements with banks, leveraging financial strength and social credibility to facilitate public transactions. By integrating modern internet technology, third-party payment platforms have expanded beyond traditional financial services to include innovations such as microloans and wealth management products. This functional overlap with credit cards has sparked debates over whether third-party payment platforms should be legally equated to credit cards. This section addresses this controversy to clarify the legal status of third-party payment platforms.

2.2 Legal Nature of Funds in Third-Party Payment Platform Accounts

In Q2 2020, Alipay accounted for approximately 55.39% of China's third-party payment market. This section focuses on Alipay, analyzing theoretical disputes and defining the legal nature of funds in its accounts, including

balances, Yu'e Bao (a wealth management product), Ant Credit Pay (credit line), and Ant Cash Now (loan service).

2.2.1 Legal Nature of Alipay Balances

(1)Creditors' Rights Theory: Proponents argue that users hold a contractual claim against Alipay based on custodial and payment agency agreements. Balances represent a digital ledger of debts owed by Alipay to users.

(2)Prepaid Value Theory: Balances are likened to prepaid cards (e.g., phone credits), where users deposit funds for future use. This aligns with Article 7 of the Non-Bank Payment Institution Online Payment Business Management Measures, which defines balances as "prepaid value" held in trust by payment institutions.

(3)Virtual Property Theory: Balances are classified as virtual property, protected under China's Civil Code. Similar to in-game assets, they are convertible into tangible property under specific conditions.

(4)Electronic Currency Theory: Balances function as digital equivalents of traditional currency, enabling direct transactions. This view emphasizes their seamless convertibility and widespread acceptance in commerce.

Conclusion: The Electronic Currency Theory best captures the legal nature of Alipay balances. While creditors' rights and prepaid value theories recognize their contractual basis, they overlook the balances' practical equivalence to currency. The electronic currency theory accommodates their dual role as debt claims and transactional mediums, reflecting modern payment trends.

2.2.2 Legal Nature of Yu'e Bao Funds

Launched in 2013, Yu'e Bao allows users to invest in money market funds (e.g., Tianhong Fund) through Alipay. While formally a debt instrument (as users purchase fund shares), Yu'e Bao's liquidity, allowing instant withdrawals and payments, mirrors Alipay balances. Thus, Yu'e Bao funds are electronic currency in substance, despite their formal classification as investment products.

2.2.3 Legal Nature of Ant Credit Pay and Ant Cash Now (Credit Services)

• Ant Credit Pay: A credit line for consumption on platforms like Taobao, requiring users to sign service agreements with Ant Small Loan Co. and Shangrong Commercial Factoring Co. Funds are non-withdrawable and tied to credit scores.

• Ant Cash Now: A withdrawable loan service requiring stringent credit checks (e.g., credit scores ≥ 600).

Both are consumer credit products, distinct from electronic currency, as they involve credit extensions rather than stored value.

2.3 Theft vs. Fraud in the Context of Third-Party Payment Platforms

Divergent legal characterizations stem from debates over two issues: (1) whether platforms have disposition rights over funds, and (2) whether machines (e.g., payment systems) can be "deceived."

2.3.1 Platform Disposition Rights Over Funds

If platforms hold disposition rights, infringements may constitute triangular fraud (deceiving the platform into transferring funds). However, Ant Credit Pay/Ant Cash Now funds are user-owned upon disbursement, extinguishing platform control. For balance funds:

• Factual Control: Platforms manage funds per user instructions but lack independent ownership.

• Normative Control: Societal consensus views users as retaining ultimate control, even if platforms execute transactions.

Theft Argument: Platforms lack disposition rights, as users retain factual and normative control. Unauthorized transfers thus constitute theft.

Counterargument: Platforms exercise delegated disposition rights under user agreements, enabling lawful fund transfers within the authorized scope.

2.3.2 Whether Machines Can Be Deceived

The question of whether machines can be deceived significantly impacts the criminal characterization of property infringement involving third-party payment platforms. If machines are deemed capable of being deceived, acts causing machines to "misunderstand" may constitute fraud; otherwise, they may be classified as theft.

This issue originated from the 2006 Xu Ting ATM case, where Xu exploited a malfunctioning ATM to withdraw 175,000 RMB with only 175 RMB. The Guangzhou Intermediate Court convicted him of "theft from a financial institution." The case sparked intense debate in Chinese criminal law theory:

① Machines Cannot Be Deceived (German Theory): Machines lack consciousness and are mere data-driven tools. Deception requires a human victim capable of cognitive error.

② Indirect Deception of Humans: While machines themselves cannot be deceived, their operators (e.g., platform managers) are the true victims. Machines act as intermediaries executing human-designed protocols.

③ Machines Can Be Deceived (Chinese Context): Unlike German law, Chinese statutes do not explicitly limit fraud to human victims. Thus, the premise that machines cannot be deceived is logically flawed in China.

In the Context of Third-Party Payment Platforms:

(1)Theft Doctrine

• Platforms, as machines, cannot be deceived. Fraud requires inducing a victim's cognitive error, which machines inherently lack.

• Inputting correct credentials (e.g., passwords) triggers automated responses without "misunderstanding." Thus, unauthorized access constitutes theft.

(2)Fraud Doctrine (Preset Consent Theory)

• Machines embody the preset consent of their operators. Correct credentials validate transactions under predefined rules, implying operator consent.

• Theft requires violating consent. If credentials are valid, no theft occurs.

• In practice, platforms deny "cognitive error," arguing they lack the capacity for subjective judgment.

This Paper's Position:

Machines can be deceived under the present consent framework:

• The essence of theft is violating the victim's consent. Consent includes not only explicit agreement but also preset conditions (e.g., ATM protocols).

• Example: In normal ATM use, withdrawals comply with the bank's preset conditions (e.g., valid card, PIN). Xu Ting exploited a system glitch, bypassing these conditions. The malfunction nullified the bank's "preset consent," rendering his acts non-consensual and thus theft, not fraud.

3 Analysis of the Characterization of Property Infringement Involving Third-Party Payment Platforms

This section conducts a legal analysis of two categories of property infringement involving third-party payment platforms: (1) QR code swapping in offline transactions and (2) unauthorized transfers of funds (e.g., Ant Credit Pay, Ant Cash Now, account balances, Yu'e Bao, or credit card funds) in non-transactional contexts, based on the behavioral methods employed and the nature of the property involved.

(1)QR Code Swapping Should Be Characterized as Theft

As previously described, the "QR code swapping" case involves a perpetrator replacing a merchant's QR code with their own, redirecting customer payments to the perpetrator's account. While this act exhibits characteristics of both covert appropriation (theft) and deception (fraud), academic debates center on whether it constitutes theft or tripartite fraud.

(2)Tripartite Fraud Argument

Proponents argue that in fraud, the deceived party (customer) and the property disposer (customer) need not coincide with the victim (merchant). In QR code cases, customers transfer funds under the mistaken belief that they are paying the merchant, adhering to the transactional norm of "payment for goods." However, customers suffer no actual loss, as they receive the goods. The merchant, having delivered the goods but deprived of payment, becomes the true victim. This aligns with a modern tripartite fraud model, where the deceived party (customer) disposes of their own property (funds) rather than the victim's (merchant's), yet the perpetrator's deception directly causes the victim's loss.

(3)Traditional Theft Argument

Scholars supporting theft analogize QR code swapping to "drilling a hole under a merchant's counter" to divert funds. However, this analogy is flawed. In the "hole drilling" scenario, funds pass through the merchant's possession (counter) before being stolen, satisfying the theft's requirement of unauthorized transfer from the victim's control. In QR code cases, funds never enter the merchant's possession; they flow directly from the customer to the perpetrator. Thus, the merchant never gains control over the funds, rendering the analogy inapt.

This Paper's Position:

QR code swapping should be characterized as theft, albeit with nuances distinct from traditional theft arguments. While tripartite fraud theory highlights the customer's role as the deceived party, the key distinction between theft and fraud lies in whether the victim (merchant) voluntarily disposed of the property with awareness of the loss. Here:

• The merchant disposed of goods (voluntarily and knowingly) but did not dispose of the payment (property interest).

• The perpetrator's act directly deprived the merchant of the property interest (payment for goods) without the merchant's consent or awareness.

Since the merchant lacked both disposition act and disposition intent regarding the lost payment, the act meets theft's core elements: unauthorized transfer of possession against the victim's will.

Characterization of Unauthorized Transfers via Third-Party Payment Accounts

Unauthorized transfers using third-party payment accounts involve disputes over whether they constitute theft or fraud. As established earlier, funds in Alipay balances and Yu'e Bao are legally classified as electronic currency, while Ant Credit Pay and Ant Cash Now are categorized as consumer credit. The characterization of unauthorized transfers

involving Ant Credit Pay and Ant Cash Now is relatively uncontroversial and will be addressed first.

(1) Infringements Involving Ant Credit Pay and Ant Cash Now

Ant Credit Pay and Ant Cash Now are credit products offered by Alipay, differing primarily in application procedures, eligibility criteria, and credit limits.

① Ant Credit Pay

• Unlike traditional credit cards, Ant Credit Pay requires no rigorous approval process, functioning similarly to balance-based payments. This blurs the line between theft and fraud. Given Ant Credit Pay's "use first, repay later" model, unauthorized use should be classified as loan fraud, regardless of whether the victim had activated Ant Credit Pay prior to the infringement. If the act also meets the criteria for illegal business operations, it should be treated as a concurrence of crimes. Some argue for contract fraud, but Ant Credit Pay's credit nature necessitates classification under loan fraud for comprehensive legal evaluation.

② Ant Cash Now

• While Ant Cash Now's application process is streamlined compared to traditional loans, it still requires user-initiated requests. Impersonating the account holder to apply for Ant Cash Now funds constitutes loan fraud; stealing already-approved funds (owned by the user) constitutes theft.

(2) Infringements Involving Balances and Yu'e Bao

Scholars advocating fraud argue that unauthorized transfers deceive the platform (as custodian of funds) into releasing funds, satisfying fraud's elements. Conversely, proponents of theft emphasize the covert breach of the user's control over funds.

This Paper's Position:

The characterization depends on the authentication method compromised:

• Fraud: If transfers require biometric verification (e.g., facial recognition or fingerprints), bypassing such safeguards deceives the platform, constituting fraud under the "machine deception" framework.

• Theft: If transfers rely solely on passwords (treated as "user equivalence" by platforms), unauthorized password use constitutes theft, as platforms mechanically execute pre-authorized instructions.

(3) Infringements Involving Credit Cards

Unauthorized credit card use via third-party platforms hinges on whether the act disrupts the credit card management order. Under the "machine deception" doctrine:

• Credit Card Fraud: Illegally obtaining card information to bind cards to platforms deceives the platform into processing transactions, violating the credit card management order. This aligns with statutory definitions of credit card fraud.

• Theft: Stealing funds from already-bound cards (without exploiting card protocols) constitutes theft, as no order of credit card administration is breached.

4 Conclusion

As third-party payment platforms grow in popularity, so do novel infringement tactics. Current legal ambiguities stem from divergent interpretations of emerging technologies. Absent legislative updates, judicial interpretation must prioritize doctrinal coherence to ensure transactional security. Expanding criminal liability should remain a last resort,

reserved for cases where existing laws demonstrably fail to address harm.

Reference

[1] Gong, P.H. & Chen, H.Y. (2010). Criminal issues and legal countermeasures in third-party payment platforms. *Journal of Shanghai Institute of Political Science and Law*, (1).

[2] Liu, M.Y. & Zhang, A.Y. (2018). Criminal law determination of the case of exchanging merchant payment QR codes. *The Chinese Prosecutor*, (2).

[3] Ningbo Haishu District Court Criminal Judgment No. 392 (2015). from http://www.fxcxw.org.cn/dyna/contentM.php?id=22212

[4] Analysys: China Third-Party Mobile Payment Market Quarterly Monitoring Report Q2 2020. Accessed February 1, 2024, from https://www.analysys.cn/article/detail/20019936

[5] China Criminal Law Society. (2022). *Judicial Practice of Online Payment Fraud*, 3rd Practical Criminal Law Forum.

[6] Che, H. (2012). The victim in theft agrees. *Chinese Journal of Law*, (2).

[7] Yang, X. P. (2014). The nature of the act of reporting loss and withdrawing deposits from someone else's account. *Law Science*, (11).

[8] He, X. (2017). Analysis of the charges related to property crimes involving payment institutions. *The Chinese Prosecutor*, (14).

[9] Liu, X. Q. (2017). The basic issues of criminal law regulation and characterization of online property infringement crimes. *Peking University Law Journal*, (4).

[10] Wu, B. (2017). Qualitative analysis of the secret transfer of funds from third-party payment platforms-take Alipay as an example. *ECUPL Journal*, (3).