JILPR Vol. 8, No. 1 October 2026
Journal of Indonesia Law & Policy Review 2715-498X

LEGAL PROTECTION FOR THIRD PARTIES OVER THE USE OF TELEPHONE NUMBERS AS EMERGENCY CONTACTS IN ELECTRONIC CREDIT AGREEMENTS

Ida Ayu Asti Manuaba[1], Appe Hutauruk[2*], Hotman Sinambela[3], Sunarno[4]
[1,2,3,4]Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Mpu Tantular, Jakarta, Indonesia
idayumanuaba@gmail.com[1], appehturuk@gmail.com[2*], hotmanbertaok@gmail.com[3], sunarno.partners@gmail.com[4]

Abstract

The development of electronic lending services has increased the use of personal data in the financing process, including the use of third-party telephone numbers as emergency contacts. In practice, the inclusion of these telephone numbers is often done without the consent of the data owner and has the potential to cause losses when electronic credit providers use these numbers for collection purposes. This situation raises issues regarding legal protection for third parties outside the contractual relationship and the basis for the provider's legal liability for processing personal data without consent. This study aims to analyze the legal status of third parties whose telephone numbers are used as emergency contacts without consent and examine the basis for the legal liability of electronic credit providers for the losses incurred. The study uses a normative legal research method with a statutory approach, a conceptual approach, and a case approach. Legal materials are analyzed qualitatively using a descriptive-analytical method. The results indicate that third parties do not have a contractual legal relationship with the provider or the debtor and therefore cannot be burdened with legal consequences arising from electronic credit agreements. Legal protection for third parties stems from the personal data protection regime, the obligations of electronic system providers, and the protection of the right to privacy. This study also found that electronic credit providers can be held liable under the doctrine of unlawful acts if they continue to process personal data without a valid legal basis and such actions cause losses that have a causal relationship with the data processing activity. The contribution of this study lies in the preparation of a normative analytical framework that integrates the principle of consent in protecting personal data, the obligations of electronic system providers, and elements of unlawful acts as a basis for determining the provider's liability for the use of third-party telephone numbers as emergency contacts without consent.

Keywords: Emergency Contact, Electronic Credit, Personal Data Protection, Unlawful Acts, Legal Responsibility

INTRODUCTION

The development of information technology has driven the transformation of the financial services sector through the provision of digital-based financial services, including electronic lending. The rise of illegal peer-to-peer lending providers also demonstrates that weak compliance with personal data protection is a major issue in Indonesia's digital financial services ecosystem (Arvante, 2022). The digitalization of financing services makes it easier for the public to access funding quickly, efficiently, and without face-to-face interaction. Despite these conveniences, electronic lending relies on the processing of personal data at every stage of the service, from identity verification and creditworthiness analysis to financing risk mitigation. This situation places personal data protection as a fundamental aspect in the provision of digital financial services, considering that personal data is part of the right to privacy that must be respected and protected by every electronic system provider in accordance with the principles of legality, transparency, accountability, and data processing security, as stipulated in Law Number 27 of 2022 concerning Personal Data Protection and Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions.

One emerging practice in electronic credit is the requirement to include an emergency contact as an administrative requirement for credit applications. In practice, debtors often list the telephone numbers of family members, friends, or colleagues without first obtaining the consent of the number holder. Legal issues arise when the debtor defaults, causing the electronic credit provider or debt collection agency to repeatedly contact the emergency contact in an effort to collect the debt. As a result, third parties, who were never parties to the contractual relationship, experience communication disruptions, psychological distress, reputational damage, and even immaterial losses due to the unauthorized use of their personal data. This practice demonstrates that the use of emergency contacts is no longer solely a means of mitigating financing risks but has evolved into a legal issue related to personal data protection, respect for privacy rights, and the limits of digital financial service providers' liability to third parties (Harits, 2021). This phenomenon demonstrates that the growth of peer-to-peer lending services not only increases access to digital financing but also increases the risk of personal data misuse if data processing governance is not implemented accountably (Uyun, Herwiyanti & Budiarti, 2024).

From a civil law perspective, the practice of using a third party's phone number as an emergency contact without consent raises issues regarding the legal standing of third parties who are outside the contractual relationship but also bear the legal consequences of an agreement they never agreed to. Based on the principle of privity of contract (Karuniahaj, 2021), an agreement is, in principle, only binding on the parties who entered into it, so that the rights and obligations arising from the agreement cannot be imposed on a third party. Therefore, a third party whose phone number is used without consent cannot be held responsible for the debtor's obligations. If the use of personal data results in harm, whether in the form of interference with privacy rights, psychological distress, or other immaterial losses, then such action is no longer merely viewed as a matter of contractual implementation but has the potential to fulfill the elements of an unlawful act as stipulated in Article 1365 of the Indonesian Criminal Code (Waluyo, 2022).

In addition to having implications within the civil law regime, the use of third-party telephone numbers as emergency contacts without consent is also closely related to the personal data protection regime. Law Number 27 of 2022 concerning Personal Data Protection emphasizes that any processing of personal data must, in principle, be based on the valid consent of the data subject or other processing basis determined by law. In this context, telephone numbers constitute personal data that cannot be processed arbitrarily without a clear legal basis. Therefore, electronic credit providers, as part of electronic system providers

(Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions), are not only obliged to guarantee the security of processed personal data but also to ensure that every stage of data collection, use, storage, and utilization is carried out in accordance with the principles of legality, transparency, purpose limitation, accountability, and protection of data subjects' rights. Thus, the use of a third-party telephone number as an emergency contact without consent cannot be viewed solely as a financing risk mitigation mechanism, but rather as a form of personal data processing that has the potential to give rise to legal liability if conducted without a legitimate basis or results in harm to the data subject (Darmayanti & Wiraguna, 2025).

Various previous studies have examined legal protection for the use of emergency contacts in online lending services, the protection of personal data in electronic system administration, and the responsibilities of digital financial service providers. Anggraini & Wiraguna (2025) explain that the use of emergency contacts without consent has the potential to violate third parties' privacy rights and lead to legal consequences in online loan collection practices. Other research indicates that the processing of personal data by digital financial service providers must be carried out based on the principles of consent, transparency, and accountability as stipulated in the personal data protection regime, so that providers cannot use personal data for purposes other than legitimate purposes (Kesuma, Budiartha & Wesna, 2021). Meanwhile, several studies on personal data protection in information technology-based lending services have focused more on the legal relationship between providers and service users as contractual subjects, as well as consumer protection against misuse of personal data in electronic transactions (Rumlus & Hartadi, 2020). These studies make important contributions to the development of personal data protection law and digital financial services, but their discussions still focus on the legal relationship between providers and debtors and therefore do not provide a comprehensive analysis of legal protection for third parties outside the contractual relationship.

Based on a review of previous research, there is still a research gap in the study of the use of third-party telephone numbers as emergency contacts in electronic credit agreements. Previous studies generally examine this issue from the perspective of consumer protection, personal data protection, or the legal relationship between the provider and the debtor as parties to the agreement. However, there is not much research that comprehensively integrates the doctrine of unlawful acts under Article 1365 of the Civil Code, the principle of processing personal data based on valid consent as stipulated in Law Number 27 of 2022 concerning Personal Data Protection, and the responsibilities of electronic system providers as a basis for determining civil liability for losses suffered by third parties outside the contractual relationship (Article 1365 of the Civil Code; Law Number 27 of 2022; Government Regulation Number 71 of 2019). The lack of an integrated approach has resulted in legal protection for third parties lacking a comprehensive analytical basis, even though third parties are the subjects who can actually suffer losses due to the processing of personal data without consent in electronic credit.

Based on this research gap, this study aims to analyze the legal protection for third parties whose telephone numbers are used as emergency contacts in electronic credit agreements without consent, and to examine the basis for the legal liability of electronic credit providers for losses arising from the processing of such personal data. This study offers an approach that integrates the doctrine of torts, the principle of personal data protection, and the responsibility of electronic system providers as an analytical framework for assessing the legal standing of third parties outside of contractual relationships. Through this approach, this research is expected to not only contribute to the development of civil law studies in electronic transactions but also serve as an academic reference for the development of personal data protection policies and governance practices for the provision of digital financial services that

align with the principles of legal certainty, justice, and the protection of the human rights of each data subject.

RESEARCH METHODS

This research employs a normative legal research method with a statutory approach, a conceptual approach, and a case approach (Jonaedi & Johnny, 2018). The statutory approach is used to examine legal provisions governing personal data protection, electronic transactions, and civil liability. The conceptual approach is used to analyze legal doctrines and principles related to third-party legal protection, unlawful acts, and the liability of electronic system providers. The case approach is used to identify the application of legal norms to the practice of using third-party telephone numbers as emergency contacts in electronic credit agreements without consent.

The legal materials used in this research consist of primary legal materials, secondary legal materials, and tertiary legal materials. Primary legal materials include the Civil Code, Law Number 27 of 2022 concerning Personal Data Protection, Law Number 11 of 2008 concerning Electronic Information and Transactions, as most recently amended by Law Number 1 of 2024, Government Regulation Number 71 of 2019 concerning the Implementation of Electronic Systems and Transactions, and Financial Services Authority regulations governing the provision of information technology-based funding services. Secondary legal materials were obtained from law books, scientific journal articles, research results, and doctrines relevant to personal data protection, contract law, torts, and electronic transactions. Meanwhile, tertiary legal materials included legal dictionaries, legal encyclopedias, and other supporting sources related to the research object.

The legal material collection technique was conducted through library research, which examined various laws and regulations, scientific literature, and research results relevant to the issues under study. All legal materials were then analyzed qualitatively using normative legal analysis methods through a process of norm inventory, legal interpretation, and systematic legal reasoning. The analysis was conducted by linking positive legal provisions, legal doctrine, and developments in personal data protection in the provision of electronic credit to obtain arguments regarding the form of legal protection for third parties and the basis for the provider's legal liability for the use of telephone numbers as emergency contacts without consent.

RESULT AND DISCUSSION

An electronic credit agreement is a legal relationship created by an agreement between an electronic credit provider and a debtor. Like any agreement, this legal relationship is subject to civil law provisions, which position the parties as subjects who acquire rights and assume obligations based on their agreement. Consequently, the rights and obligations arising from an agreement are essentially binding only on the parties involved. This principle is known as privity of contract, which asserts that a contract cannot have legal consequences for parties not bound by the agreement (Pane, 2022).

In the practice of electronic credit, including a telephone number as an emergency contact has become a common administrative requirement implemented by providers. Functionally, the existence of an emergency contact is intended as a means of communication if the debtor cannot be contacted. However, this practice often extends beyond its original purpose, when a third party's telephone number is used for collection after the debtor defaults. Research by Melin Simorangkir and Josep Irvan Gilang indicates that an emergency contact is a party outside the legal relationship of a loan and therefore is not burdened with the rights or obligations stipulated in an electronic credit agreement. Therefore, the use of their personal data still requires legal protection.

This view aligns with research by Chotimah (2019), which asserts that an emergency contact is a party outside the legal relationship of an information technology-based loan and therefore is not burdened with the rights or obligations arising from that agreement. Therefore, listing a telephone number as an emergency contact cannot be interpreted as agreement to become a guarantor or the party responsible for the debtor's debt repayment.

This opinion is also supported by Shandy & Sari (2023), who state that an emergency contact cannot be equated with a guarantor, because a guarantor agreement, according to Article 1820 of the Civil Code, requires a clear statement of intent from the party binding themselves as guarantor. Therefore, the provider's actions in treating the emergency contact as the party responsible for the debtor's debt have no legal basis.

From a contract law perspective, the inclusion of a person's telephone number by a debtor does not automatically create a legal relationship between the number owner and the electronic credit provider. The consent given by the debtor is only binding on the individual and cannot be viewed as consent representing the wishes of a third party. Therefore, the provider cannot assume that the inclusion of a telephone number on a credit application form legitimizes the use of a third party's personal data without the data owner's direct consent. This approach aligns with the principle of consensualism and the principle that an agreement only binds parties who consciously express their desire to be bound by a legal relationship.

This issue becomes even more complex when the use of a third party's telephone number is no longer limited to administrative information but develops into an active means of communication in the collection process. At this stage, the third party not only loses control over the use of their personal data but also potentially experiences violations of their rights to privacy, security, and good reputation. Research on emergency contact protection in peer-to-peer lending services shows that collection practices involving third parties are often carried out through repeated communication and even accompanied by pressure, thus causing losses for individuals who do not have a contractual relationship with the provider.

In this context, the legal standing of third parties cannot be equated with that of debtors or guarantors. Third parties are not subjects who benefit from or bear obligations under electronic credit agreements. Therefore, any actions by providers that utilize third parties' personal data must be assessed based on legal regimes outside of contract law, particularly provisions regarding personal data protection and unlawful acts. This shift in perspective is important because disputes that arise are no longer solely related to the implementation of the agreement, but rather to the legality of using an individual's personal data outside of a contractual relationship. Recent research on personal data protection in online loan agreements also confirms that the use of a third party's telephone number without consent violates the principle of consent, which underlies personal data processing under Law Number 27 of 2022.

Based on this analysis, it is understood that listing a telephone number as an emergency contact does not automatically create a legal relationship between the electronic credit provider and the third party. The absence of a contractual relationship prevents the third party from being legally liable for the debtor's default. Therefore, when the use of a telephone number without consent results in harm, the basis of legal protection for third parties no longer rests on contract law, but rather on the personal data protection regime and liability for unlawful acts. This finding provides the basis for analyzing the forms of legal protection available to third parties in the provision of electronic credit.

The harm experienced by third parties due to the use of a telephone number as an emergency contact without consent does not always take the form of economic loss. The use of personal data that results in communication disruptions, psychological distress, reputational damage, and loss of control over personal data are forms of immaterial harm recognized in the development of the personal data protection regime. Therefore, third-party harm in this context

should be understood more broadly as a violation of the right to privacy and the right to personal data protection, not solely a financial loss.

Based on the above analysis, this study finds that the legal standing of third parties whose telephone numbers are listed as emergency contacts does not arise from a contractual relationship. However, the absence of a contractual relationship does not mean that the provider is free to process the third-party telephone number listed as an emergency contact. From a personal data protection perspective, the legal relationship between the provider and the third party does not arise from an electronic credit agreement, but rather from the processing of personal data, which must have a legal basis as stipulated in Law Number 27 of 2022 concerning Personal Data Protection. Therefore, the inclusion of a telephone number by a debtor cannot automatically be equated with the data owner's consent for the provider to process it, preventing the third party from being burdened with legal consequences for the debtor's default. Consequently, legal protection for third parties must be established through a personal data protection regime and the doctrine of torts, not solely through contract law.

Based on this description, the legal status of a third party whose telephone number is used as an emergency contact cannot be positioned as part of the contractual relationship between the debtor and the electronic credit provider. Instead, the third party must be viewed as a personal data subject with independent rights under laws and regulations concerning personal data protection. The function of emergency contact is essentially intended only as a means of communication in certain circumstances and cannot be interpreted as a form of transfer of responsibility for debt repayment or consent to unlimited data processing (Adawiyah, 2020). Consequently, any processing of personal data by third parties must meet a legitimate basis for processing and remain open to legal liability if the processing is carried out without consent or results in harm. This legal standing forms the basis for analyzing the forms of legal protection and liability of electronic credit providers in the following discussion.

The use of third-party telephone numbers as emergency contacts in electronic credit services not only raises issues regarding contractual relationships but is also closely related to the legal protection of personal data. In Indonesian legal developments, personal data is viewed as part of the inherent right to privacy of every individual, and therefore, all processing must be conducted based on the principles of legality, transparency, and respect for the rights of data subjects. The development of financial technology lending services that rely on electronic data processing further emphasizes that personal data protection is an integral part of responsible electronic system management. Legal protection for personal data gained a more comprehensive foundation following the enactment of Law Number 27 of 2022 concerning Personal Data Protection. This law establishes consent as one of the primary foundations for processing personal data. Consent must be validly granted by the data subject after receiving sufficient information regarding the purpose and scope of the data processing. Therefore, a debtor's inclusion of a third-party telephone number on a credit application form cannot be equated with the consent of the telephone number owner. The right to consent is an individual right inherent to the data subject and cannot be transferred to another party without a valid legal basis.

The consequence of this principle is that electronic credit providers remain obligated to ensure that any personal data they process has a clear legal basis. The mere fact that a telephone number is obtained from a debtor does not automatically absolve the provider from its legal responsibility as a controller or data processor. Research on the restriction of the use of emergency contact data in fintech lending services indicates that providers remain obligated to limit data use to the original purpose of collection and not to use it beyond the purposes authorized by the data subject. In addition to the Personal Data Protection Law, protection for third parties is also strengthened by the electronic system implementation regime. Electronic system providers are required to maintain reliable, secure, and responsible systems, including

ensuring the security and confidentiality of personal data processed in the provision of digital services. This obligation demonstrates that personal data protection is not merely an administrative obligation but also a form of legal responsibility of the provider to all parties affected by data processing activities.

In practice, the use of a third party's telephone number without consent is often followed by collection actions via phone calls, text messages, or other communication applications. Although third parties have no legal obligation to fulfill debtors' obligations, they are often the ones under pressure due to the collection process. Research on emergency contact protection in online loan transactions shows that third parties are outside the legal relationship of lending and borrowing, so that collection actions involving them without a valid legal basis have the potential to violate the right to privacy and open up opportunities for civil lawsuits under Article 1365 of the Civil Code. Legal protection for third parties is ultimately interpreted not only as the right to refuse the use of personal data without consent, but also as the right to obtain redress if the use of such data results in losses. These losses are not always material losses, but can include interference with privacy, psychological distress, reputational damage, or a sense of security due to repeated collection communications. Therefore, the personal data protection regime must be understood as an instrument that not only protects data as an object but also protects the legal interests of individuals as data subjects. This view is also in line with the development of studies on the urgency of personal data protection for users and emergency contacts in online loan transactions. Based on this description, legal protection for third parties in using telephone numbers as emergency contacts is both preventive and repressive. Preventive protection is realized through the obligation of the organizer to ensure that there is a valid legal basis before processing personal data, while repressive protection is realized through a legal accountability mechanism if the use of personal data without consent causes harm.

The practice of misuse of personal data in online loan collections demonstrates that violations occur not only against debtors but also against third parties whose data is used beyond the original processing purposes. The implementation of the Personal Data Protection Law provides a legal basis for data subjects to seek redress for unlawful use of personal data. Thus, the personal data protection regime not only recognizes data subjects' rights but also serves as a tool for assessing e-credit providers' compliance with the principles of lawfulness, fairness, and accountability in personal data processing. In e-credit operations, providers act as personal data controllers because they determine the purposes and methods of processing personal data for users and third parties. This position creates a legal obligation to ensure that all stages of data processing are conducted on a lawful basis, implement adequate security measures, and prevent data use beyond the intended purpose. This obligation aligns with the principles of fintech service governance, which places personal data protection as part of responsible electronic system management.

Preventive legal protection for third parties is realized through the obligation of electronic credit providers to ensure that all personal data processing has a valid legal basis, is carried out transparently, is limited to specific purposes (purpose limitation), and only uses data relevant to service needs (data minimization). In the context of using emergency contact, providers are not sufficient to simply receive the telephone number provided by the debtor, but must also ensure that the data processing complies with the provisions of Law Number 27 of 2022 concerning Personal Data Protection and the principles of electronic system governance. If these obligations are not met and result in losses for third parties, repressive legal protection can be realized through objection mechanisms, claims for compensation, or other legal remedies in accordance with statutory provisions. This preventative protection also represents the implementation of personal data protection governance in the provision of technology-based lending services, which prioritizes compliance with data processing principles as a form of legal risk mitigation. As personal data subjects, third parties have the right to obtain

information regarding the processing of their personal data, the right to protection against unauthorized use of their data, the right to object to certain processing, and the right to demand redress if the use of such data results in harm. These rights demonstrate that legal protection within the personal data protection regime is not merely declaratory but provides data subjects with an active legal standing to defend their rights. In addition to complying with personal data protection provisions, electronic credit providers are also required to comply with governance provisions established by the Financial Services Authority. These regulations demonstrate that legal protection for service users and third parties is established not only through the personal data protection regime but also through sectoral compliance obligations governing the provision of information technology-based funding services. Protection of data subjects' rights in technology-based lending services aims not only to maintain data confidentiality but also to provide legal certainty regarding all forms of personal data processing.

Based on this description, legal protection for third parties does not stop at recognizing their rights as personal data subjects but also creates a legal obligation for electronic credit providers to carry out data processing lawfully, proportionally, and accountably. Violation of these obligations serves as the basis for assessing the legal liability of the provider if the use of a third-party telephone number as an emergency contact is conducted without a legitimate basis or results in harm. Therefore, the discussion of legal protection in this subchapter serves as the basis for examining the form and basis of the provider's liability in the following subchapter.

The legal liability of electronic credit providers for using third-party telephone numbers as emergency contacts without consent is based not only on the existence of a contractual relationship, but also on a breach of legal obligations regarding the processing of personal data. In this context, the provider acts as a Personal Data Controller, responsible for ensuring that all data processing is conducted on a valid legal basis and complies with the principles of personal data protection. This approach also aligns with emerging studies that position fintech platforms as Personal Data Controllers, assuming responsibility for the entire processing of emergency contact data, regardless of whether the data was initially provided by the debtor.

From a civil law perspective, this liability can be analyzed through the doctrine of unlawful acts as stipulated in Article 1365 of the Civil Code. This provision requires the presence of five elements: the existence of an act, its unlawful nature, fault, loss, and a causal relationship between the act and the resulting loss. In the context of using emergency contact information, these five elements cannot be understood abstractly but must be applied to the characteristics of the legal relationship within electronic credit. The unauthorized use of a third party's telephone number as an emergency contact and then exploited in the collection process has the potential to fulfill all of these elements if it results in losses to the data owner, whether material or immaterial.

The first element, namely the existence of an act, is fulfilled when the service provider receives, stores, uses, and utilizes the third party's telephone number as part of the electronic credit service process. Although the telephone number is initially obtained from the debtor, subsequent processing is under the control of the service provider. Therefore, the use of personal data is not solely a result of the debtor's action in providing the telephone number, but also the result of the service provider's decision to process and use the data in operational activities, including the collection stage. Even though there is no contractual relationship between the service provider and the third party, the service provider's legal obligations still arise because the service provider processes the third party's personal data. Therefore, the basis for liability does not stem solely from breach of contract, but rather from a breach of legal obligations in the processing of personal data without a legitimate basis for processing. This approach demonstrates that the personal data protection regime provides independent protection for data subjects outside of a contractual relationship.

Furthermore, the unlawful element can be assessed from the inconsistency of the organizer's actions with legal provisions governing the protection of personal data and the implementation of electronic systems. The use of a third party's telephone number without consent contradicts the principles of legality and consent in the processing of personal data. Furthermore, if the data is used for repeated billing purposes, thereby violating the third party's right to privacy, such actions also contradict the organizer's obligation to operate electronic systems securely, responsibly, and respect the rights of every data subject. Thus, the unlawful nature arises not only from a violation of statutory provisions, but also because such actions violate the third party's subjective right to control and protect their personal data. In addition to being subject to the personal data protection regime, electronic credit providers are also required to comply with sectoral provisions governing the governance of information technology-based funding services. Compliance with Financial Services Authority regulations is part of the organizer's legal obligation to ensure the protection of users and third parties affected by the provision of services. Therefore, violations of these provisions can be an indicator of the organizer's negligence in meeting compliance standards set by statutory regulations.

The element of error is reflected in the failure to comply with the duty of care that should be applied by electronic credit providers in processing personal data. As business actors utilizing electronic systems and information technology, providers have the capacity to establish verification mechanisms for the use of third-party data before the data is further processed. When providers continue to use telephone numbers without ensuring a valid legal basis, this action indicates negligence or even deliberate disregard for the principles of personal data protection established by positive law. If proven to have processed personal data without a valid legal basis and resulting in losses to third parties, electronic credit providers can be held accountable through various legal mechanisms. This accountability can take the form of stopping data processing, deleting personal data, fulfilling data subject rights, providing compensation under civil law, or imposing administrative sanctions in accordance with applicable laws and regulations. In the literature, the position of fintech platforms as Personal Data Controllers also gives rise to administrative, civil, and criminal liability in the event of misuse of personal data during the service delivery process. The responsibility of electronic system providers extends beyond system security to include accountability for all personal data processing activities under their control.

Losses encompass not only material losses but also immaterial ones. Third parties may experience communication disruptions due to persistent debt collection calls or messages, psychological distress from being linked to someone else's debt obligations, and even damage to their social and professional reputations. These losses demonstrate that misuse of telephone numbers as emergency contacts has broader impacts than simply the unauthorized use of personal data. The causal relationship is the most crucial aspect in determining the provider's liability. In practice, it may be argued that losses arise from the debtor's actions in listing the third party's telephone number. However, this study argues that the causal relationship does not end with the debtor's actions alone. Losses only occur after the provider decides to receive, store, process, and use the telephone number as a means of debt collection communication. In other words, the debtor's actions only initiate the data acquisition, while losses to third parties are a direct consequence of the provider's data processing activities. Therefore, the relevant causal relationship in the context of Article 1365 of the Civil Code lies in the actions of the organizer as the party controlling the use of personal data.

Based on an analysis of these elements, this study argues that the legal liability of service providers is not solely based on a violation of the Personal Data Protection Law, but must also be understood as a form of civil liability for unlawful acts. This approach provides more comprehensive protection for third parties because it not only allows for the termination

of unlawful data processing but also allows for claims for compensation if all elements of an unlawful act are met. Based on this description, e-credit providers cannot escape responsibility simply by reason of obtaining a telephone number from a debtor. As Personal Data Controllers and Electronic System Operators, providers remain obligated to ensure that all data processing is conducted on a valid legal basis and respects the rights of data subjects. If these obligations are violated, resulting in losses for third parties, then the providers may be held liable under the doctrine of unlawful acts, the Personal Data Protection Law, and sectoral provisions governing the provision of information technology-based funding services.

As a research contribution, this article offers an analytical framework for the liability of e-credit providers based on three main indicators: (1) the absence of a legal basis or valid consent for the processing of third-party personal data; (2) the continued processing and use of data by the organizer for operational purposes, including billing; and (3) the occurrence of losses that have a causal relationship with the data processing activities. If these three indicators are met, the organizer can in principle be held civilly liable based on Article 1365 of the Civil Code while still paying attention to the provisions of Law Number 27 of 2022 concerning Personal Data Protection and regulations regarding the implementation of electronic systems.

Table 1. Framework for Analysis of Legal Responsibility of Electronic Credit Providers

Indicators	Analysis
Data processing basis	No valid consent from a third party as the data subject
Organizer actions	Receiving, storing, processing, and using telephone numbers for billing purposes
Legal violations	Contrary to the principles of personal data protection, privacy rights, and the obligations of electronic system providers
Losses	Communication disruption, psychological distress, reputational harm, and immaterial losses
Causal relationship	Losses are a direct result of data processing by the provider
Legal consequences	The provider may be held liable under Article 1365 of the Civil Code and provisions on personal data protection

Table 1 in this study found that the basis for legal liability for electronic credit providers stems not only from violations of personal data protection provisions, but also from fulfilling the elements of an unlawful act as stipulated in Article 1365 of the Civil Code. Therefore, the use of a third-party telephone number as an emergency contact without consent, accompanied by data processing and resulting in losses, provides sufficient grounds for civil liability for the provider.

CONCLUSIONS

The use of a third party's telephone number as an emergency contact in an electronic credit agreement without consent does not create a contractual legal relationship between the third party and the provider or the debtor. Based on the principle of privity of contract, the rights and obligations arising from an agreement are binding only on the parties who entered into it, therefore, a third party cannot be positioned as a guarantor or responsible for fulfilling the debtor's obligations. Nevertheless, the third party retains legal standing as a personal data subject, who is protected under Law Number 27 of 2022 concerning Personal Data Protection. Therefore, any processing of a third party's telephone number must be conducted on a lawful basis, respect the data subject's rights, and comply with the principles of legality, transparency, accountability, and purpose limitation. Legal protection for third parties is realized through preventive and repressive mechanisms. Preventive protection is reflected in the obligations of electronic credit providers as Personal Data Controllers and Electronic System Operators to ensure that the collection, use, storage, and utilization of personal data are carried out in accordance with statutory provisions. Meanwhile, repressive protection is provided through legal enforcement mechanisms in the event of a violation that results in losses for a third party, including through lawsuits for unlawful acts, claims for compensation, and other mechanisms

available under the personal data protection regime and civil law. The position of data controller carries the consequence of legal responsibility for all personal data processing processes under the provider's control.

This study concludes that the legal liability of e-credit providers arises not only from the contractual relationship with the debtor, but also from legal obligations related to the processing of third-party personal data. If the provider processes a third-party's telephone number without a valid legal basis or uses the data for purposes other than those permitted, resulting in losses, the provider may be held liable under Article 1365 of the Civil Code, Law Number 27 of 2022 concerning Personal Data Protection, and sectoral provisions governing the provision of information technology-based funding services. Therefore, this study confirms that these findings reinforce the urgency of implementing the Personal Data Protection Law in the provision of online lending services to provide legal certainty for third parties who have not yet obtained adequate legal standing. Protection for third parties in the use of emergency contacts must be placed within an integrated framework between civil law, personal data protection, and governance of digital financial services to ensure legal certainty, justice, and respect for the right to personal data.

REFERENCES

Arvante, J. Z. Y. (2022). Dampak Permasalahan Pinjaman Online dan Perlindungan Hukum Bagi Konsumen Pinjaman Online. *Ikatan Penulis Mahasiswa Hukum Indonesia Law Journal*, *2*(1), 73–87. https://doi.org/10.15294/ipmhi.v2i1.53736

Harits, T. M. (2021). Konflik norma dalam pengaturan kartu kredit pemerintah. *Jurist-Diction*, *4*(2), 759. https://doi.org/10.20473/jd.v4i2.25788

Uyun, L., Herwiyanti, E., & Budiarti, L. (2024). Dampak pinjol pada generasi Z dan generasi milenial. *Sosio E-kons*, *16*(1), 73. https://doi.org/10.30998/sosioekons.v16i1.22041

Karuniahaj, S. E. (2021). Asas Privity of Contract Dalam Layanan Pinjam Meminjam Uang Berbasis Teknologi Informasi (Studi Kasus pada Penyelenggara DanaRupiah). *Jurist-Diction*, *4*(4), 1629. https://doi.org/10.20473/jd.v4i4.28491

Waluyo, B. (2022). Kajian terhadap perbuatan melawan hukum berdasarkan pada Pasal 1365 Kitab Undang-Undang Hukum Perdata. *Cakrawala Hukum Majalah Ilmiah Fakultas Hukum Universitas Wijayakusuma*, *24*(1), 14–22. https://doi.org/10.51921/chk.v24i1.186

Darmayanti, E. S., & Wiraguna, S. A. (2025). Tanggung Jawab Hukum Pinjaman Online terhadap Penyebaran Data Nasabah secara Ilegal. *ALADALAH Jurnal Politik Sosial Hukum Dan Humaniora*, *3*(2), 233–251. https://doi.org/10.59246/aladalah.v3i2.1313

Anggraini, N. F., & Wiraguna, S. A. (2025). Tanggung Jawab Hukum Platform Pinjaman Online terhadap Penyalahgunaan dan Penyebaran Data Pribadi Konsumen secara Ilegal. *Jurnal Riset Sosial Humaniora Dan Pendidikan*, *3*(3), 144–167. https://doi.org/10.62383/risoma.v3i3.767

Kesuma, A. a. N. D. H., Budiartha, I. N. P., & Wesna, P. a. S. (2021). Perlindungan Hukum Terhadap Keamanan Data Pribadi Konsumen Teknologi Finansial dalam Transaksi Elektronik. *Jurnal Preferensi Hukum*, *2*(2), 411–416. https://doi.org/10.22225/jph.2.2.3350.411-416

Rumlus, M. H., & Hartadi, H. (2020). Kebijakan Penanggulangan Pencurian Data Pribadi dalam Media Elektronik. *Jurnal HAM*, *11*(2), 285. https://doi.org/10.30641/ham.2020.11.285-299

Jonaedi, E., & Johnny, I. (2018). Metode penelitian hukum: normatif dan empiris. In *Prenadamedia Group eBooks*. http://repository.um-palembang.ac.id/id/eprint/10148/

Pane, E. P. (2022). Penerapan asas proporsionalitas dalam perjanjian kredit berbasis online. *Locus Journal of Academic Literature Review*, 36–45. https://doi.org/10.56128/ljoalr.v1i1.50

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara [Cyber Security Governance and Indonesian Cyber Diplomacy by National Cyber and Encryption Agency]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *10*(2), 113–128. https://doi.org/10.22212/jp.v10i2.1447

Shandy, R., & Sari, R. D. P. (2023). Aspek hukum pencantuman data pribadi secara sepihak sebagai kontak darurat dalam perjanjian kredit online. *Binamulia Hukum*, *12*(1), 39–45. https://doi.org/10.37893/jbh.v12i1.452

Adawiyah, K. A. (2020). Perlindungan hukum atas ketidakamanan data nasabah financial technology pada sektor peer to peer lending. In *eTheses of Maulana Malik Ibrahim State Islamic University (Maulana Malik Ibrahim State Islamic University)*. http://etheses.uin-malang.ac.id/20636/7/15220045.pdf

Nurisman, E. (2022). Risalah Tantangan penegakan hukum Tindak pidana Kekerasan Seksual pasca lahirnya Undang-Undang Nomor 12 Tahun 2022. *Jurnal Pembangunan Hukum Indonesia*, *4*(2), 170–196. https://doi.org/10.14710/jphi.v4i2.170-196