Modern Technologies Law

University of Science and Culture

http://doi.org//10.22133/mtlj.2025.462387.1338

Security Challenges in Mobile Payments: The EU's Approach

Sajjad Shahbaz Qahfarrokhi

Assistant Prof., Department of Islamic Jurisprudence and Law, University of Shahrekord, Shahrekord, Iran.

Article Info

Original Article

Received:
11-05-2024
Accepted:
25-10-2024

Key Words:
Retail Payments
Mobile Payments
User Security
Payment Services

Abstract

Mobile payments have emerged as a pivotal force in the realm of retail transactions, offering a convenient, secure, and accessible alternative to traditional payment methods. Recognizing their immense potential to drive economic growth and innovation, the European Union (EU) has taken a proactive stance in regulating this burgeoning industry. A cornerstone of this regulatory endeavor is the EU's unwavering focus on ensuring the robust security of mobile payment systems, safeguarding both consumers and service providers. The EU's proactive approach to regulating mobile payments, with a strong emphasis on user security and fostering innovation, provides a valuable model for other jurisdictions, including Iran. By adopting a similar approach, Iran can effectively integrate mobile payments into its digital economy, ensuring a secure, competitive, and inclusive financial landscape for its citizens. The EU's proactive approach to regulating mobile payments, with a strong emphasis on user security and fostering innovation, provides a valuable model for other jurisdictions, including Iran. By adopting a similar approach, Iran can effectively integrate mobile payments into its digital economy, ensuring a secure, competitive, and inclusive financial landscape for its citizens.

***Corresponding author**
e-mail: sajjadshahbaz@sku.ac.ir

How to Cite:
Shahbaz Qahfarrokhi, S. (2025). Security Challenges in Mobile Payments: The EU's Approach. *Modern Technologies Law*, *6*(12), 195-212.

Published by University of Science and Culture https://www.usc.ac.ir
Online ISSN: 2783-3836

1. Introduction

The rise of innovative payment methods represents a transformative shift in the retail payments landscape, promising significant economic benefits and enhanced consumer convenience. However, despite their potential, the adoption of these innovative payment tools has been sluggish, primarily due to concerns surrounding security and usability. This article explores the legal implications of these challenges, particularly within the context of the European Union (EU) regulatory framework, and examines how the balance between security and accessibility can be achieved. Consumer acceptance of innovative payment methods hinges on two critical factors: security and usability. Security encompasses not only the protection of financial information but also the consumer's perception of safety when using these new tools. The concept of "sustainable security" is vital; if consumers believe that a payment method is insecure, they are unlikely to adopt it. This perception is often shaped by high-profile data breaches and fraud incidents that have plagued the financial sector. Usability, on the other hand, refers to how easily consumers can access and use these payment methods. If a payment system is overly complex or difficult to navigate, it will deter consumers from utilizing it, regardless of its security features. Therefore, regulators face the challenge of ensuring that innovative payment systems are both secure and user-friendly. The question of how to regulate innovative payment methods effectively is complex. Legislators must strike a balance between fostering innovation and ensuring consumer protection. The EU has made strides in this area through various directives, notably the Payment Services Directive (PSD), which was first adopted in 2007 and revised in 2015. These directives aim to create a single market for payments, enhance consumer protection, and promote competition.

However, the rapid evolution of technology and payment systems presents ongoing challenges. For instance, the emergence of mobile payments has introduced new security risks that were not adequately addressed in earlier legislation. The EU's regulatory framework must evolve to keep pace with these developments, ensuring that it remains relevant and effective in safeguarding consumers. Mobile payments, while convenient, present unique security challenges. The reliance on smartphones and mobile applications for transactions increases the risk of unauthorized access and data breaches. The concepts of "reliability," "integrity," and "accessibility" become paramount in this context. Reliability ensures that transaction information is secure from unauthorized access, while integrity guarantees that the information remains unchanged throughout the transaction process. Accessibility ensures that payment services are available and usable for all consumers, including those with disabilities. The legal framework must address these security risks comprehensively. For example, the General Data Protection Regulation (GDPR) imposes strict requirements on how personal data is collected and processed, which directly impacts the operations of payment service providers (PSPs). As the landscape of payment methods continues to evolve, the interplay between GDPR and the Payment Services Directive (PSD2) becomes increasingly significant. This article delves into the implications of these regulations, highlighting the need for a cohesive approach that not only protects consumer data but also fosters an environment conducive to innovation. In this context, the article will analyze the current state of the EU regulatory framework concerning innovative payment methods, focusing on the gaps and challenges that persist. It will explore the implications of strong customer authentication (SCA) requirements, which, while essential for enhancing security, may inadvertently hinder user experience and adoption rates. The need for clearer guidelines regarding the liability of PSPs in cases of data breaches will also be examined, as ambiguity in this area can lead to consumer distrust. In conclusion, the successful integration of innovative payment methods into the retail landscape hinges on a well-balanced regulatory approach that prioritizes both security and usability. By addressing the existing gaps and challenges within the EU regulatory framework, stakeholders can work towards fostering a secure, efficient, and consumer-friendly payment ecosystem that encourages the adoption of new technologies while safeguarding consumer interests.

2. Methodology

To regularly assess and update regulatory frameworks to address emerging challenges. The interplay between technological advancements and regulatory measures is critical in ensuring that consumer rights are upheld while fostering an environment conducive to innovation. One significant gap identified in the current regulatory framework is the need for clearer guidelines on the responsibilities of payment service providers regarding data protection and privacy. While PSD2 encourages third-party access to payment accounts, it does not sufficiently clarify the liability of PSPs in cases of data breaches or misuse of consumer information. This ambiguity can lead to consumer distrust and reluctance to engage with new payment technologies. Moreover, the implementation of strong customer authentication (SCA) has raised concerns about user experience. While SCA is essential for enhancing security, overly stringent requirements can lead to friction in the payment process, potentially discouraging consumers from using mobile payment solutions. Regulators must strike a balance between security and convenience to ensure that consumer adoption of mobile payments continues to grow. Additionally, the rise of decentralized finance (DeFi) and cryptocurrencies presents new regulatory challenges that the existing framework may not adequately address. As these technologies gain traction, regulators must consider how to incorporate them into the existing legal structure while ensuring consumer protection and financial stability. In summary, while the EU's PSD and PSD2 have made significant contributions to the regulation of mobile payments, ongoing evaluation and adaptation of these frameworks are necessary. Addressing gaps related to data protection, user experience, and emerging technologies will be crucial in maintaining consumer trust and fostering a secure and innovative payment ecosystem. As the landscape continues to evolve, collaboration between regulators, industry stakeholders, and consumers will be essential in shaping a regulatory environment that effectively balances innovation with consumer protection.

3. Results and Discussion

This analysis examines the European Union's (EU) regulatory response to the growth of mobile payments and the associated security risks. As mobile payment systems become increasingly prevalent, the need for a robust legal framework to protect consumers and ensure the integrity of financial transactions has never been more critical. This section discusses key findings related to the EU's regulatory landscape, security challenges, and comparative insights with other jurisdictions. The EU has implemented the Payment Services Directive (PSD) and its revised version, the Payment Services Directive 2 (PSD2), to regulate payment services, including mobile payments. The original PSD, adopted in 2007, aimed to create a single market for payment services across the EU, enhancing consumer protection and fostering competition among payment service providers (PSPs). However, as technology evolved, so did the need for a more comprehensive regulatory framework, leading to the introduction of PSD2 in 2018. PSD2 builds upon its predecessor by introducing several key enhancements aimed at addressing the challenges posed by new payment technologies. One of the most significant aspects of PSD2 is its emphasis on strong customer authentication (SCA), which mandates that PSPs implement multi-factor authentication to verify the identity of users during transactions. This requirement is crucial in mitigating risks associated with unauthorized access and fraud, which are prevalent in mobile payment systems. Moreover, PSD2 encourages innovation by allowing third-party providers to access customer account information, provided that consumers give explicit consent. This provision fosters competition and the development of new financial technologies, aligning with the EU's broader goals of enhancing market integration and consumer choice. The legal principle of transparency, as outlined in the Consumer Rights Directive, is also reinforced under PSD2, ensuring that consumers are adequately informed about the terms and conditions of payment services.

Despite the regulatory advancements brought about by PSD2, mobile payment security risks primarily stem from device vulnerabilities and weaknesses in payment platforms. The reliance on smartphones and mobile applications for transactions increases the potential for unauthorized access, data breaches, and fraud. For instance, malware targeting mobile devices can compromise sensitive information, leading to significant financial losses for

consumers and PSPs alike. The European Court of Justice (ECJ) has played a pivotal role in interpreting existing directives and addressing issues related to consumer protection and the responsibilities of PSPs. In the landmark case of C-290/18, the ECJ ruled that payment service providers must ensure the security of payment transactions and are liable for losses incurred due to unauthorized transactions unless they can prove that the consumer acted fraudulently or failed to fulfill their obligations to safeguard their payment instruments. This case underscores the importance of the legal principle of liability in the context of mobile payments. The ambiguity of liability can create challenges for both consumers and payment service providers (PSPs). As mobile payment systems evolve, the delineation of responsibilities between consumers and PSPs becomes increasingly critical, particularly in cases of fraud or unauthorized transactions.

When examining the EU's regulatory framework for mobile payments, it is beneficial to compare it with approaches taken in other jurisdictions, such as the United States and Asia. In the U.S., the regulatory landscape is less centralized, with various federal and state laws governing payment systems. The lack of a comprehensive federal framework can lead to inconsistencies in consumer protection and security measures across different states. However, initiatives like the Consumer Financial Protection Bureau (CFPB) have made strides in addressing consumer rights in digital payments .In contrast, Asian markets, particularly in countries like China and South Korea, have seen rapid adoption of mobile payments, often driven by technological innovation and consumer demand. Regulatory responses in these regions have varied, with some governments implementing strict guidelines to ensure security and consumer protection, while others have taken a more laissez-faire approach, allowing market forces to dictate the pace of innovation.

4. Conclusions and Future Research

In the rapidly evolving landscape of mobile payments, fostering widespread adoption of these tools is essential for stimulating economic growth. However, this endeavor must prioritize both security and user-friendliness to ensure consumer confidence and protect sensitive financial information. The unique challenges presented by mobile devices—such as their physical design, input limitations, and vulnerability to malware—demand a nuanced approach to regulation and security measures. Additionally, the risks associated with user inexperience and potential deficiencies in the practices of payment service providers (PSPs) must be addressed to create a safe and efficient payment ecosystem. Legislators face the critical task of balancing the establishment of minimum security standards with the imperative of maintaining ease of use in payment systems. This balance is particularly important given the dynamic nature of mobile payment technology, which is characterized by rapid innovation and the emergence of new threats. Security measures must not only be robust but also adaptable to technological advancements, ensuring that they remain effective against evolving risks. For instance, the European Union's Payment Services Directive 2 (PSD2) emphasizes the importance of strong customer authentication and the security of payment transactions, setting a precedent for how security can be integrated into user-friendly systems. Iranian legislators can draw valuable insights from the EU's regulatory framework, which outlines consumer protections and the obligations of PSPs and governments. By analyzing existing domestic regulations and capabilities, Iran can craft a legislative framework tailored to its unique context, ensuring that it addresses the specific challenges of mobile payments while enhancing user experience. This framework should incorporate principles of transparency, accountability, and consumer rights, aligning with international best practices. Future research should focus on the effectiveness of various security measures in real-world applications, exploring how different regulatory approaches impact consumer behavior and trust in mobile payment systems. Additionally, studies could investigate the role of education and awareness in mitigating risks associated with user inexperience, as well as the potential for technological innovations, such as biometric authentication, to enhance security without compromising usability.

حقوق فناوری‌های نوین

http://doi.org//10.22133/mtlj.2025.462387.1338

چالش‌های امنیتی فراروی پرداخت‌های موبایلی با مطالعه تطبیقی در مقررات اتحادیهٔ اروپا

سجاد شهباز قهفرخی

استادیار گروه فقه و حقوق اسلامی دانشگاه شهرکرد، شهرکرد، ایران.

اطلاعات مقاله

مقالهٔ پژوهشی

تاریخ دریافت:
۱۴۰۳/۰۲/۲۲

تاریخ پذیرش:
۱۴۰۳/۰۸/۰۴

واژگان کلیدی:
پرداخت‌های جزئی
پرداخت‌های موبایلی
امنیت کاربر
خدمات پرداخت

چکیده

پرداخت‌های ابتکاری یکی از بازارهای نوپدید در پرداخت‌های جزئی هستند که تأثیر بسزایی در توسعهٔ اقتصادی دارند. یکی از این ابزارها، پرداخت‌های موبایلی است که روند رو به رشد، سیال بودن توسعهٔ فنی، امکان استفاده در همهٔ گسترهٔ جغرافیایی باعث شد تا اتحادیهٔ اروپا به فکر سامان‌دهی حقوقی آن باشد. مهم‌ترین موضوع در مواجهه با پرداخت‌های موبایلی، حفظ امنیت کاربران و سامانه‌های پرداخت است که اتحادیهٔ اروپا با صدور دو دستورالعمل در این زمینه پیشتاز مقرره‌گذاری است. در این مقاله، با شناسایی چالش‌های امنیتی و راهکارهای کاهش و حذف مشکلات امنیتی، به تحلیل راهکارهای این دو دستورالعمل پرداخته خواهد شد. بیان الزامات راجع به تهیه‌کنندگان سرویس‌های خدمات پرداخت و همچنین تکالیف دولت‌های عضو در حمایت از کاربران و تبیین تحولات مقرره‌گذاری اتحادیهٔ اروپا ضمن ایجاد ادبیات حقوقی و ترسیم افق‌های پژوهشی، الگویی برای قانون‌گذار ایرانی در راستای توسعهٔ حقوقی این ابزارها قرار می‌گیرد. داده‌ها در این مقاله ازطریق کتابخانه‌ای جمع‌آوری و با روش تحلیلی بررسی شده‌اند.

***نویسندهٔ مسئول**

رایانامه: sajjadshahbaz@sku.ac.ir

نحوهٔ استناددهی:

شهباز قهفرخی، سجاد (۱۴۰۴). چالش‌های امنیتی فراروی پرداخت‌های موبایلی با مطالعهٔ تطبیقی در مقررات اتحادیهٔ اروپا. حقوق فناوری‌های نوین، ۶(۱۲)، ۱۹۵-۲۱۲.

ناشر: دانشگاه علم و فرهنگ https://www.usc.ac.ir

شاپای الکترونیکی: ۳۸۳۶-۲۷۸۳

مقدمه

«پرداخت‌های ابتکاری»[1] یکی از بازارهای نوپدید در پرداخت‌های جزئی هستند که به‌طور بالقوه سود کلانی را برای اقتصاد در پی دارند (Zandi et al., 2016, p 13). بااین‌حال از حیث پذیرش عمومی مصرف‌کنندگان، بیشتر ابزارهای پرداخت‌های ابتکاری به‌آرامی توانسته‌اند مقبولیت و نفوذ کسب کنند. دو عنصر در پذیرش عمومی ابزارهای پرداخت تأثیر چشمگیری دارند. از یک طرف «امنیت و احساس امنیت» مشتری نقش مهمی در پذیرش پرداخت‌های نوین ابتکاری بازی می‌کند و از طرف دیگر «دسترسی و قابلیت استفاده» پرداخت‌های نوین ابتکاری در فرایند پذیرش آن‌ها تعیین‌کننده است. هنگامی‌که مشتری از سامانه‌ای که فکر می‌کند امن نیست و با آن آشنا نیست استفاده می‌کند، فقدان «امنیت پایدار»[2] می‌تواند مانع دسترسی و استفاده از آن روش می‌شود. این شرایط سبب افزایش چالش‌های مقرره‌گذاری خواهد شد. این پرسش مطرح است که قانون‌گذار چگونه و تا چه میزان باید برای پرداخت‌های ابتکاری نوین مقرره‌گذاری کند که تعادل امنیت و قابلیت دسترسی به روش‌های پرداخت حفظ شود.

این مقاله در پی آن است که به چالش‌هایی بپردازد که مسائل امنیتی پرداخت‌های ابتکاری پرداخت‌های موبایلی برای مقرره‌گذار ایجاد کرده است و با تمرکز کردن بر مقررات اتحادیهٔ اروپا به دنبال پاسخ‌گویی به سؤالات ذیل است:

۱. چگونه مسائل امنیتی پرداخت‌های نوین ابتکاری مانند پرداخت‌های موبایلی، ضرورت تقویت و به‌روزرسانی قوانین و مقررات موجود را ایجاد کرده است؟

۲. آیا چهارچوب قانونی پیشنهادی اتحادیهٔ اروپا درمورد سیستم‌های پرداخت برای پاسخ‌دهی به مسائل امنیتی به وجود آمده توسط پرداخت‌های موبایلی کافی و مناسب است؟

این مقاله ضمن بررسی چالش‌های قانونی ناشی از ریسک‌های امنیتی پرداخت‌های موبایلی، به چالش‌های مربوط به رازداری و حریم خصوصی، یکپارچگی و قابلیت دسترسی سیستم‌های عملکرد تراکنش نیز می‌پردازد.

«قابلیت اعتماد»[3] به این معناست که اطلاعات تراکنش در برابر دسترسی غیرمجاز ایمن باشند؛ درحالی‌که مفهوم «یکپارچگی»[4] بدین معناست که اطلاعات تراکنش در زمان انجام فرایند دست نخورده باقی خواهند بود و نمی‌توان آن را تغییر داد. «قابلیت دسترسی»[5] عاملیت دستگاه‌ها را تمهید می‌کند و تضمین می‌دهد سرویس‌ها در دسترس و قابل استفاده خواهند بود.

چالش‌هایی که تاکنون برای حمایت از تراکنش‌ها و اطلاعات مشتری در برابر جرائم سنتی[6] مانند کلاهبرداری، سرقت و هک کردن مورد توجه قانون‌گذار بوده‌اند، متفاوت با چالش‌های جدید است. همچنین چالش‌های برآمده از ریسک‌های سامانه پرداخت متفاوت از تهدیدات امنیتی مانند پول‌شویی هستند و پرداختن به این چالش‌ها خارج از رسالت این مقاله است.

در این مقاله تلاش شده است بر عینی کردن و عینی شدن امنیت پرداخت‌ها تمرکز شود؛ اما به نظر می‌رسد هنوز هم در عمل، به‌دلیل پیچیدگی و سیال بودن بعد فنی، ضمانت‌اجراهای اداری و قانونی بیشتر از روش‌های فنی پاسخ‌گو خواهند بود. این مقاله نه‌تنها مقررات قانونی

---

۱. پرداخت‌های ابتکاری Innovative Payments جایگزین روش‌های پرداخت سنتی نظیر استفاده از پول نقد، چک و کارت‌های اعتباری است. در این روش‌ها، تراکنش‌های مالی با استفاده از فناوری‌ها و ابزارهای پیشرفته‌تر، سریع‌تر، آسان‌تر، امن‌تر و کارآمدتر به مشتریان عرضه می‌شوند. ازجمله پرداخت‌های ابتکاری می‌توان به پرداخت‌های موبایلی، پرداخت‌ها با استفاده از فناوری NFC یا بلوتوث، پرداخت‌های مبتنی بر کد QR، پرداخت‌های بیومتریک و ارزهای دیجیتال اشاره کرد. اپل پی (Apple Pay) و گوگل پی (Google Pay) دو نمونه از کیف پول‌های دیجیتالی هستند که به کاربران اجازه می‌دهند با استفاده از تلفن‌های هوشمند، فروشگاه‌ها و وب‌سایت‌ها پرداخت انجام دهند. همچنین PayPal و Venmo پلتفرم‌های پرداخت آنلاین هستند که به کاربران اجازه می‌دهند پول را به‌صورت آنلاین یا ازطریق برنامه‌های تلفن همراه برای یکدیگر ارسال و دریافت کنند (Rysman & Schuh, 2017, pp. 27-46). همچنین نک:
https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report

2. Rigid Security
3. Confidenitiality
4. Integrity
5. Availability
6. Conventional Cirmes

مرتبط با مقررات امنیتی را بررسی می‌کند؛ بلکه ترتیبات قانونی در دسترس برای مشتریان به‌منظور تعقیب دعوای جبران خسارت و به‌صورت کلی حمایت کافی از مشتری تحت چهارچوب قانونی اتحادیهٔ اروپا را نیز بررسی خواهد کرد.

در این مقاله، بعد از معرفی انواع روش‌های پرداخت موبایلی، به برخی از جنبه‌های امنیتی ایجاد شده ازطریق پرداخت‌های موبایلی پرداخته می‌شود و به‌صورت خاص در این بخش بر ریسک‌های امنیتی جدید پرداخت موبایلی تأکید می‌شود. در ادامه تحلیل می‌شود که چطور مسائل امنیتی به چالش‌های مقرره‌گذاری منجر می‌شود. آیا برای حمایت چندجانبه از مشتری، پرداخت موبایلی به مقررات بیشتر نیاز دارد؟ بدین‌منظور دستورالعمل خدمات پرداخت اتحادیهٔ اروپا[1] تحلیل شده و چالش‌های مرتبط با مسائل امنیتی پرداخت‌های ابتکاری بررسی می‌شود[2].

۱. تعریف پرداخت‌های موبایلی

پرداخت‌های موبایلی نمونهٔ کاملی از یک پرداخت ابتکاری نوین در اقتصادهای توسعه‌یافته است. هرچقدر هم که سامانه پرداخت امنیت داشته باشد، باز هم مسئلهٔ امنیت سیستم‌های پشتیبانی‌کننده مانند یک استفاده‌کننده از رایانهٔ شخصی یا سیستم مبادلاتی مطرح خواهد بود. پرداخت موبایلی عامل مهمی بعد از پرداخت آنی است که در راه‌اندازی موج بعدی ابتکارات در بازارهای اروپا تأثیرگذار بوده و طبق آمار سال ۲۰۱۵ شورای پرداخت اروپا[3] تخمین زده شده است که ۲۸درصد پرداخت‌ها توسط ابزارهای نوین پرداخت، انجام شده‌اند[4]. تلفن همراه به‌طور گسترده‌ای باعث توسعهٔ کشورها نیز شده است. امروزه ممکن است اشخاص کیف پول خود را فراموش کنند اما گوشی تلفن خود را کمتر فراموش خواهند کرد. امکانات فناورانهٔ گوشی تلفن همراه، ابزارهای پرداخت ساده‌تر و دقیق‌تری را برای توسعهٔ پرداخت آنلاین فراهم کرده است.

پرداخت‌های الکترونیکی[5] در معنای عام می‌توانند به پرداخت‌هایی که ازطریق الکترونیکی ایجاد، تجزیه، تحلیل، ارسال و دریافت می‌شوند گفته شود. از سال ۱۹۹۰، که شبکهٔ اینترنت توسعه پیدا کرد، نیاز به ابزارهای پرداختی که قادر باشند ازطریق این شبکه فرایندهای پرداخت مالی را انجام دهند، آشکار شد و انواع روش‌های پرداخت نوین که به‌طور کلی به آن‌ها E-payment گفته می‌شود، ایجاد شدند.

پرداخت موبایلی یکی از خدمات مالی تلفن همراه (MFS)[6] است که امروزه در دسترس بوده و به‌عنوان دروازه‌ای برای سایر خدمات مالی تلفن همراه مانند بانکداری تلفن همراه، بیمه و محصولات سرمایه‌گذاری دیده می‌شود. اخیراً مصرف‌کنندگان از ارزهای دیجیتال برای پرداخت، تجارت، پس‌انداز و سرمایه‌گذاری استفاده می‌کنند. پرداخت ازطریق تلفن همراه می‌تواند برای همه‌ی اشخاصی که نیاز به استفاده از تراکنش‌های مالی دارند، اعم از این‌که مصرف‌کننده یا فروشنده یا تاجر باشند یا نباشند، استفاده شود.

1. EU Payment Services Directive (PSD)

۲. لازم به بیان است که اتحادیهٔ اروپا به منظور ایجاد بازار واحد برای خدمات پرداخت در اتحادیهٔ اروپا و افزایش رقابت و نوآوری در صنعت خدمات پرداخت، در سال ۲۰۰۷ نخستین دستورالعمل خدمات پرداخت را به تصویب رسانید و قوانینی را برای ارائه‌دهندگان خدمات پرداخت (PSP) وضع کرد و الزاماتی را برای تراکنش‌های پرداخت از جمله شفافیت، امنیت و حمایت از مصرف‌کننده تعیین کرد. در سال ۲۰۱۳، کمیسیون اروپا برای رسیدگی به تحولات جدید در صنعت خدمات پرداخت، مانند افزایش استفاده از پرداخت‌های موبایلی و تجارت الکترونیک، تجدیدنظر در PSD را پیشنهاد کرد. نسخهٔ اصلاح شده، معروف به PSD2، در سال ۲۰۱۵ توسط اتحادیهٔ اروپا تصویب و در ژانویهٔ ۲۰۱۸ اجرایی شد. در حال حاضر نیز بحث اصلاح نسخهٔ اخیر مطرح است و موضوع در سطح کمیته‌هاي تخصصي درحال پیگیري است. آنچه در مقالهٔ حاضر مورد بحث و تحلیل قرار خواهد گرفت موضع هر دو نسخه دستورالعمل است تا از این طریق علاوه‌بر نمایاندن تحولات مقرره‌گذاري، خلأهای پاسخ داده شده نیز روشن‌تر بررسی شوند.

3. European Payment Council

4. European Payment Council. Summer Reading: Results of Latest EPC Poll Reveal that Instant Payments are Most Likely Trigger the Next Wave of Innovation (blog). 7 August 2015.

5. E-payment

6. Mobile Financial Services (MFS)

پرداخت‌های موبایلی شکل نوینی از سیستم پرداخت هستند که اقتصاد جدید بازارهای مالی را شکل می‌دهند (Rutledge, 2010, p.15). آن‌ها بخشی از پدیدهٔ فناوری‌های مالی[1] تلقی می‌شوند که به‌طور خاص در اتحادیهٔ اروپا، مقررات مربوط به آن‌ها در قالب دستورالعمل سیستم پرداخت[2] و مقررات مربوط به کارمزدهای مبادلهٔ چندجانبه[3]، تنظیم شده است.

۲. انواع پرداخت‌های موبایلی

پرداخت‌های موبایلی که در این مقاله به آن پرداخته می‌شود سه نوع است: پرداخت‌های بدون تماس[4]، پرداخت‌های برنامه‌محور[5] و پرداخت‌های کانال اپراتور شبکهٔ تلفن همراه MNO[6].

گونهٔ نخست به‌منزلهٔ روش پرداخت از نزدیک شناخته می‌شود؛ درحالی‌که دو راه دیگر پرداخت از راه دور هستند. در این روش، با استفاده از سامانه‌های مجاورتی هم پرداخت‌کننده و هم گیرندهٔ پرداخت، تراکنش را از یک محل فناورانه مانند اینفرارد[7] یا بلوتوث[8] و یا ارتباط از نزدیک[9] انجام می‌دهند. درحالی‌که در سیستم‌های از راه دور پرداخت‌کننده و گیرنده، تراکنش را ازطریق شبکه‌ها (چه یک شبکه مانند سیستم جهانی موبایل GSM و چه اینترنت) انجام می‌دهند[10].

در پرداخت‌های بدون تماس، پرداخت‌ها و تراکنش‌های مالی بدون نیاز به تماس فیزیکی کارت با دستگاه کارت‌خوان انجام می‌شود. در این روش، به‌جای استفاده از کارت فیزیکی، از فناوری‌های مختلفی مانند NFC، بلوتوث کم‌مصرف یا کدهای QR برای انتقال اطلاعات پرداخت به دستگاه کارت‌خوان استفاده می‌شود. محدودیت پذیرش، فقدان امنیت درصورت مفقودی تلفن همراه و دریافت هزینهٔ اضافی از سوی ارائه‌دهندهٔ خدمات پرداخت ازجمله معایب پرداخت‌های بدون تماس است (Van den Akker et al., 2023, p. 3).

پرداخت‌های برنامه‌محور نیز روشی برای انجام تراکنش‌های مالی ازطریق برنامه‌های تلفن همراه است. این روش به شخص امکان می‌دهد بدون نیاز به حمل کارت فیزیکی یا پول نقد، در فروشگاه‌ها و رستوران‌ها و وب‌سایت‌ها خرید کند. استفاده از این روش هزینهٔ مالی کمتری برای کاربر دارد و چه‌بسا از پاداش نیز بهره‌مند شود؛ اما به‌دلیل پشتیبانی نکردن بسیاری از فروشگاه‌ها از برنامه‌های مزبور و اشغال فضای ذخیره‌سازی در تلفن همراه، از این روش نیز انتقاد شده است. همچنین در این روش نیز درصورت مفقودی تلفن همراه، امکان سوءاستفاده برای یابنده یا سارق فراهم خواهد بود (Liao & Ho, 2021, p. 3-4).

پرداخت‌های کانال اپراتور شبکهٔ تلفن همراه (MNO) نیز روشی برای انجام تراکنش‌های مالی ازطریق حساب تلفن همراه است. این روش به شخص امکان می‌دهد با کسر مبلغ از اعتبار تلفن همراه خود، پرداخت هزینه‌ها یا خرید کالا و انتقال پول انجام دهد. این روش نیز همان مزایا و معایب روش‌های قبلی را دارد. تنها ویژگی مثبت این روش این است که کانال اپراتور شبکهٔ تلفن همراه به‌صورت مستقیم به حساب بانکی متصل نیست و حداکثر سوءاستفاده‌ای که ممکن است رخ دهد به اندازهٔ اعتبار حساب خط تلفن است.

۳. پرداخت‌های موبایلی و تهدیدات امنیتی جدید

در همهٔ روش‌های پرداخت موبایلی، دستگاه موبایل به‌عنوان یک ابزار دوطرفه[11] عمل می‌کند. بدین معنا که این دستگاه به‌عنوان ابزار ارتباطی به‌مانند یک سازوکار پرداخت برای انجام تراکنش با پول واقعی استفاده می‌شود. در نتیجه تهدیدات جدید امنیتی ایجاد خواهند شد. در این مقاله

1. financial technologies (‘Fintech’)
2. Payment System Directive
3. Regulation on Multilateral Interchange Fees
4. Contactless Payments
5. App-based Payments
6. Mobile Network OPERATOR Payments
7. Infrared
8. Bluetooth
9. Near Field Communication (NFC)
10. See European Payments Council. “Overview Mobile Payments Initiatives.” EPC091-14. Version 2.0. 2014.
11. Double-edged Tool

به دو گونهٔ این تهدیدات امنیتی جدید شامل تهدیدات امنیتی موجود در دستگاه موبایل و تهدیدات امنیتی مربوط به «بسترهای پرداخت»[1]، پرداخته خواهد شد.

۳-۱. تهدیدات امنیتی ناشی از خود دستگاه گوشی تلفن همراه

یک دستگاه گوشی تلفن همراه تهدیدات امنیتی نسبتاً بالایی برای انجام پرداخت‌ها دارد؛ چه این‌که ذات ساختمانی دستگاه گوشی تلفن همراه به‌منزلهٔ یک دستگاه سبک ارتباط تلفنی است و اساساً برای استفاده به‌عنوان پایگاه پرداخت طراحی نشده است. در یک دستگاه موبایل، تهدیدات مختلفی وجود دارد. ازجمل، این آسیب‌ها می‌توان به طراحی خاص آن که سرقت و مفقود شدن آن را آسان‌تر می‌کند و قابلیت محدود ورودی آن و بدافزارهای متعددی که ممکن است به تلفن همراه آسیب برسانند اشاره کرد.

اولین تهدید این است که دستگاه موبایل به‌منزلهٔ ابزاری سبک و قابل‌حمل طراحی شده است و همین‌گونه طراحی، سرقت یا گم شدن آن را آسان‌تر می‌کند[2]. گفته شده است که فقط در سال ۲۰۱۳ در آمریکا تقریباً ۳٫۱ میلیون دستگاه موبایل به سرقت رفته است. این آمار تقریباً دو برابر موبایل‌های سرقت شده در سال ۲۰۱۲ است که حدود ۱/۶ میلیون دستگاه بوده است. از ۳٫۱ موبایل دزدیده شده، حدود ۱٫٤ میلیون آن هیچ‌گاه پیدا نشده است[3]. مشابه این گزارش، گزارش دیگری است که سایت lookout (متعلق به یک شرکت امنیت سایبری متمرکز بر دستگاه‌های موبایل) تهیه شده و نشان می‌دهد در سال ۲۰۱۴ ده درصد افرادی که گوشی هوشمند داشته‌اند قربانی سرقت شده‌اند. اکثریت این قربانیان یعنی تقریباً ۶۸ درصد ایشان موفق نشده‌اند گوشی خود را پیدا کنند. ازآنجاکه دستگاه موبایل حاوی اطلاعات شخصی است، طبق گزارش مشابهی ۵۰ درصد قربانیان حاضر به پرداخت مبالغ نسبتاً بالایی، حدود ۵۰۰ دلار، برای بازگرداندن اطلاعات گران‌بهای موجود در دستگاه خود از قبیل عکس‌ها، برنامه‌ها، فیلم‌ها و اطلاعات شخصی مشتمل بر اطلاعاتی شده‌اند که مربوط به پرداخت بوده است[4].

دومین تهدید مربوط به این واقعیت است که دستگاه موبایل ذاتاً محدودیت ورودی دارد که عمدتاً مربوط به عوامل فیزیکی دستگاه موبایل است (Clarkson et al., 2006, p.18). در گوشی‌های غیرهوشمند این محدودیت‌ها شامل محدودیت اندازه، قابلیت‌های حسی محدود شده تا ۴۰ وضعیت دودویی و عوامل شکلی نظیر طرح صفحه دکمه استاندارد، که در مقایسه با آرایش صفحه‌کلیدهای مرسوم رایانه، به‌صورت نامناسبی جلوه کرده است. درنتیجه از منظر مصرف‌کنندگان، ورودی استفاده شده در دستگاه موبایل در مقایسه با دستگاه‌های بزرگ‌تر، مانند رایانه‌های شخصی، بسیار مشکل‌آفرین و کند است؛ البته با هوشمند شدن گوشی‌های تلفن و به‌وجود آمدن سیستم‌عامل‌های نوین نظیر اندروید و IOS و توسعه و افزایش برنامه‌های کاربردی[5]، این محدودیت‌ها تا حد زیادی مرتفع شده‌اند؛ هرچند آسیب‌های جدیدی نظیر حملات بدافزاری نیز هم‌زمان افزایش یافته است.

سومین تهدید مربوط به این است که از یک‌سو، استفاده‌کنندهٔ دستگاه موبایل هیچ کنترلی بر پیکربندی امنیتی[6] دستگاه خود ندارد و از سوی دیگر، محافظت از دستگاه موبایل در برابر استفاده‌کننده با سوءنیت[7] بسیار دشوار است (Scarfone & Souppaya, 2013, p. 124). کنترل نداشتن بر پیکربندی امنیتی گوشی ناشی از استفاده از منابع غیرایمن مشتمل بر دستگاه‌های موبایل، شبکه‌ها، نرم‌افزارها و محتواهای ناامن است. همچنین عدم امکان محافظت در برابر استفاده‌کننده با سوءنیت ناشی از این واقعیت است که استفاده‌کننده تسلط و کنترل کامل بر عملکرد دستگاه موبایل دارد.

---

1. Payment platforms

۲. اگرچه صرف سرقت گوشي تلفن همراه تهديد محسوب نمي‌شود، بسياري از افراد اطلاعاتي نظير نام كاربري و رمزها را در خود گوشي ذخيره مي‌كنند و همين امر سوءاستفاده از گوشي تلفن همراه را براي سارق بسيار آسان و كم‌هزينه خواهد كرد. همين امر باعث شده است در اين قسمت از مقاله، سرقت تلفن همراه را به عنوان تهديد مطرح كنيم.

3. consumerreports.org (last visited: 2023-01-12).
4. www.lookout.com
5. Application
6. Security Configuration
7. Malicious user

آخرین تهدید مرتبط به بدافزارهای دستگاه موبایل است که درحال رشد سریع هستند. طبق گزارش‌های موجود تقریباً ۵/۵میلیارد حملهٔ بدافزاری[1] به تلفن‌های همراه در سراسر جهان در سال ۲۰۲۲ صورت پذیرفته است[2]. اکثر این حملات موفقیت‌آمیز نبوده‌اند، اما وجود این تهدید بالقوه برای پرداخت‌های موبایلی که مستقیماً با وجوه نقدی ارتباط دارد ریسک بالایی ایجاد می‌کند.

۳-۲. تهدیدات امنیتی ناشی از بستر پرداخت

تهدیدات بستر پرداخت در پرداخت‌های موبایلی، شامل رمزنویسی ضعیف، به‌ویژه رمزنویسی‌های استفاده شده در سیستم NFC، تراکنش‌های کلاهبردارانه، حملات به برنامهٔ سیم‌کارت و سرویس‌های USSD و DSTK، خطرات سرورهای برنامهٔ موبایل و پایگاه داده و برنامهٔ اصلی امنیت پرداخت موبایلی می‌شود (Desai, 2014, p. 5).

پیچیدگی تهدیدات امنیتی با این واقعیت روبه‌روست که از طرفی بیشتر متقاضیان استفاده‌کننده از خدمات سرویس‌های پرداخت موبایلی آگاهی بسیار کمی از تهدیدات امنیتی دارند و از طرف عرضه‌کنندگان نیز بیشتر سرویس‌ها ازطریق ارائه‌دهندگان ثالث تهیه شده که بدیهی است تجربهٔ بسیار کمی درمورد مسائل امنیتی سیستم پرداخت دارند. اگر این تهدیدات به‌خوبی کاهش پیدا نکنند، نه‌تنها منافع تجاری به‌دلیل تراکنش‌های کلاهبرداری کاهش خواهد یافت، بلکه حریم خصوصی و حق ایمن‌سازی نیز نقض شده و از سرویس‌های ارتباطی سوءاستفاده می‌شود. ورودی‌های مطمئن و نامطمئن برای پرداخت‌های موبایلی برنامه‌محور می‌شود (Desai, 2014, p. 21).

پرداخت‌های موبایلی به تخصص و مهارت خاصی که مرکب از امنیت فنی بسترهای پرداخت و امنیت فنی دستگاه موبایل باشد نیاز دارد (Desai, 2014, p. 8). این تخصص شامل ذخیره‌سازی ایمن داده‌ها روی دستگاه موبایل، ارسال ایمن داده‌ها از دستگاه موبایل به سرور آپ و برعکس، اجرای قانونی قوی و خاص برای پرداخت‌های موبایلی برنامه‌محور، واسط‌های سایبری ایمن و خدمات برای پرداخت‌های موبایلی سایبرمحور و ارزیابی خلوت می‌شود.

۴. پرداخت‌های موبایلی: نیازمند مقرره‌گذاری مناسب

به‌دلیل رشد پیچیدگی فنی پرداخت‌های موبایلی، مستمر بودن توسعه‌یافتگی این ابزارها و پدید آمدن انواع جدید خدمات پرداخت در سرتاسر جهان، بند ۷ مقدمهٔ PDS2 مقررات اتحادیهٔ اروپا، امنیت و ایمنی سیستم‌های پرداخت را شرط لازم برای بازار پرداخت به‌منظور کارکرد بهینه پیرامون حمایت از یکپارچه‌سازی بازار دانسته است.

مسائل امنیتی پرداخت‌های موبایلی، که سبب چالش‌های مقرراتی شده، از بعد فنی و حقوقی نیازمند بررسی است. عامل فنی مشتمل بر کفایت سطحی از امنیت است که از یک‌سو، حمایت حداکثری از بازیگران را اقتضا می‌کند و از سوی دیگر، قابلیت استفاده از روش پرداخت را تقویت می‌کند و عامل حقوقی مبتنی بر چهارچوبی اساسی برای حمایت از مشتریان است که مشتمل بر ترتیبات جبران خسارت باشد؛ به‌نحوی که مشتری را برای تعقیب دعوای مطالبهٔ خسارت قادر سازد و مسئولیت مدنی مشتری را نیز کاهش دهد. این مطلب برآمده از این نکته است که اختلافات ناشی از عوامل فنی، مانند مسائل امنیتی هستند که با استفاده از ابزارهای حقوقی و اداری حل خواهند شد (Kasiyanto, 2016, p. 157).

۴-۱. امنیت کافی و مناسب تجهیزات پایه

در سیستم‌های پرداخت، حمایت کافی از مشتریان در برابر تهدیدات ایجاد شده توسط مسائل امنیتی نقش تعیین‌کننده‌ای دارد (European Parliament & Council, 2015, par. 7). به‌هرحال تأمین حداکثری امنیت از یک‌سو نیازمند سرمایه‌گذاری بسیار زیادی است و از سوی

1. malicious software (malware)
2. https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide (last visited: 2023-01-12).

دیگر، ازآنجاکه قابلیت استفاده از یک سیستم پرداخت برای تأمین قابلیت تاب‌آوری یک سیستم تعیین‌کننده را دارد، اقداماتِ امنیتی ارائه‌دهندگان سیستم‌های پرداخت باید با مسائل امنیتی مرتبط متناسب‌سازی شود؛ ازاین‌رو لازم است که مقررات ناظر بر اقدامات امنیتی، تعادل بین نگهداشت و کفایت سطح امنیتی را حفظ و قابلیت استفادهٔ سیستم را تأمین کنند. همچنین مقررات تأمین‌کنندهٔ اقدامات امنیتی باید به‌موقع و از نظر فنی خنثی باشند. ازآنجاکه روش‌های امنیتی با تهدیدات تکامل یافتهٔ پویا ارتباط دارند، باید به‌نحوی باشند که بتوانند ادامهٔ حیات دهند. پویایی فناوری‌های مرتبط با پرداخت‌های موبایلی اقتضا می‌کند قانون‌گذار مقرراتی وضع کند که به‌آسانی منسوخ نشوند؛ بنابراین مقرره‌گذاری باید به‌نحوی باشد که مقررات فنی خنثی بوده و قابلیت تطبیق با تحولات فناورانه را داشته باشند.

برای پاسخ‌گویی به این چالش‌ها، راه‌حل ممکن این است که مقررات به‌نحوی طراحی شوند که مجموعه‌ای از اصول کلی امنیت را مقرر کنند که به‌اندازهٔ کافی برای حمایت از مشتریان روشن و قوی باشد. در این روش، اصول کلی تضمین می‌کند که حتی با ارتقای سیستم نیز حمایت کافی از مشتریان اعمال خواهد شد. این اصول کلی مقرراتی، بی‌طرفی مقرره‌گذار و واقعیت‌گرایی کامل را تضمین می‌کند.

در مقام اجرا، برای پر کردن شکاف بین اصول کلی و جزئیات امنیتی، نیاز است که چنین مقرراتی با مقررات استانداردی که حاوی جزئیات فنی برای حفظ امنیت باشد، به‌صورت توأمان پیش‌بینی شود. ازآنجاکه منافع تجار نقش تعیین‌کننده‌ای در تعریف استاندارد ایفا می‌کند، استانداردهایی بهترین طراحی را خواهند داشت که با بازیگران بازار تطبیق داده شده باشند و نظر ایشان نیز در هنگام طراحی لحاظ شده باشد؛ نه این‌که توسط یک مقنن تحمیل شده باشند (Kasiyanto, 2016, p. 158).

برای مثال قابلیت همکاری دو سیستم پرداخت نه‌تنها با باز شدن و اشتراک‌گذاری مشخصات و امنیت فنی هرکدام از این دو ارتباط دارد، بلکه به آمادگی برای اشتراک‌گذاری با پلتفرم بازرگانان دیگر نیز ارتباط دارد. در وهلهٔ نخست، چهارچوب قانونی موجود در تعامل با نیازمندی‌های اساسی تحلیل خواهند شد.

در چهارچوب مقررات فعلی اتحادیهٔ اروپا، اصول کلی مرتبط با امنیت سیستم‌های پرداخت، که طبق مادهٔ ۵۷ PSD1 و متعاقباً در مادهٔ ۷۰ PSD2 تنظیم شده‌اند، مقرر داشته ارائه‌دهندگان سرویس‌های پرداخت مکلف‌اند تضمین کنند که ویژگی‌های امنیتی و شخصی‌سازی‌شدهٔ ابزارهای پرداخت برای دیگر اعضا قابل‌دسترس نیست[1]؛ ازاین‌رو تکلیف ارائه‌دهندگان به حفاظت از اطلاعات مشتریان در برابر دسترسی‌های بدون مجوز قانونی به‌روشنی در قانون بیان شده است.

در بند اول مادهٔ ۶۰ PSD1 و متعاقباً بند نخست مادهٔ ۷۳ PSD2 بیان شده اگر نتایج و تبعات این مقررات برای استفاده‌کنندگان خدمات پرداخت کافی نباشد، تأمین‌کنندگان خدمات پرداخت خسارت مشتریان را به‌اندازهٔ مبلغ تراکنش تأیید نشده به‌صورت پرداخت آنی جبران خواهند کرد.

مقررهٔ موجود در بند دوم مادهٔ PSD1۶۰، به مشتریان این امکان را داده بود که در مواردی که بین تأمین‌کنندگان خدمات پرداخت و مشتریان قرارداد منعقد شده است، دعوای جبران خسارت مالی اقامه نموده و جبران خسارت وارد به خود را بخواهند. در اصلاح بعدی، بند سوم مادهٔ PSD2۷۳، علاوه‌بر امکان استناد به قرارداد خصوصی، به مشتریان امکان استناد به قانون حاکم بر قرارداد فی‌مابین را نیز داده است[2]. بدین‌ترتیب لزوم جبران خسارت صرفاً مستند به قرارداد نبوده و مشتریان از حمایت قانون برخوردار می‌شوند.

اصول کلی، قواعد کافی را برای امنیت سیستم‌های پرداخت پوشش می‌دهد، بااین‌حال مشکلاتی در اجرایی کردن این قواعد برای سیستم‌های پرداخت همراه به چندین دلیل وجود دارد: نخست این‌که تأمین‌کنندگان سیستم‌های پرداخت همراه نه‌تنها متفاوت با بانک‌ها و کانال‌های MNO و شرکت‌های استارتاپی برنامه‌محورند؛ بلکه برخی از آن‌ها بازیگران جدیدی هستند که هنوز مشمول مقررات نشده‌اند. با توجه

---

۱. مادهٔ ۷۰: ۱. ارائه‌دهندهٔ خدمات پرداخت صادرکنندهٔ ابزار پرداخت باید: الف: مطمئن شود که اطلاعات امنیتی شخصی شده برای اشخاصی غیر از کاربر خدمات پرداخت که حق استفاده از ابزار پرداخت را دارند، بدون لطمه به تعهدات کاربر خدمات پرداخت مندرج در مادهٔ ۶۹، قابل دسترسی نباشد.

2. Further financial compensation may be determined in accordance with the law applicable to the contract concluded between the payer and the payment service provider or the contract concluded between the payer and the payment initiation service provider if applicable.

به نرخ سریع رشد تأمین‌کنندگان خدمات پرداخت، شورای پرداخت اتحادیهٔ اروپا برنامه‌ای را تهیه کرده که در ظرف فقط پنج ماه، یعنی از ژوئن ۲۰۱٤ تا اکتبر ۲۰۱٤، دست‌کم ۱۹ ابتکار جدید در منطقهٔ پرداخت یورو[1] از فناوری‌های استفاده شده در تراکنش‌های ماشین‌های فروش در انگلستان گرفته تا مخابرات ایتالیا برای پرداخت با دستگاه‌های pos را شامل شود (Conseil Européen des Paiements AISBL, 2014, pp. 21-25).

به‌علاوه در میان این بازیگران، آنچه تأمین‌کنندگان سرویس پرداخت سوم شخص[2] نامیده می‌شود، اساساً تهیه‌کنندهٔ سرویس پرداخت هستند که پلتفرم خود را به حساب سرویس‌دهی پلتفرم‌های استفاده‌کننده از برنامهٔ موبایل ارتباط می‌دهند. برای مشتریان، استفاده از سرویس‌های تازه ایجاد شده که هنوز مقررات آن‌ها را پوشش نداده‌اند، ریسک بالایی دارد.

همچنین تأمین‌کنندگان پرداخت موبایلی در ارتباط با امنیت و مسائل امنیتی سیستم‌های پرداخت کم‌تجربه یا بی‌تجربه هستند؛ به‌ویژه این‌که این موضوع درمورد شرکت‌های استارتاپی تهیه‌کنندهٔ سرویس‌های خدمات پرداخت برنامه‌محور صدق می‌کند. ازآنجاکه MNOها با سیستم‌های مخابراتی متفاوت هستند، مسائل امنیتی آن‌ها نیازمند تجربهٔ سرویس‌های پرداخت متفاوت است. سرویس‌های پرداخت، درگیر تبدیل کردن پول واقعی به پول الکترونیکی و برعکس هستند که در موارد لازم می‌توانند برای خرید کالا و خدمات در بسیاری از موارد یا اجرای هرگونه تراکنش آنلاین دیگر مانند انتقال شخص به شخص آنلاین استفاده می‌شوند؛ درحالی‌که سرویس‌های مخابراتی فعالیت محدودتری دارند (Kasiyanto, 2016, p. 160).

با در نظر گرفتن این شرایط و این‌که پرداخت‌های موبایلی تهدیدهای جدیدی ایجاد کرده‌اند، باید چهارچوب قانونی موجود برای حفاظت از مشتریان و درنهایت برای تضمین ماندگاری سامانه‌ها تقویت شود. سایر تکالیفی که طبق دستورالعمل PSD2 بر ارائه‌دهندگان تحمیل می‌شود برای این است که در مواقع ضروری، مدارک تراکنش پرداخت را به‌منظور پردازش داده‌های شخصی با هدف پیشگیری از تقلب و کلاهبرداری و یا کشف پرداخت‌های تقلبی انجام دهند[3]. کشورهای عضو باید درصورت لزوم برای محافظت، پیشگیری، بررسی و کشف تقلب در پرداخت، پردازش داده‌های شخصی توسط سیستم‌های پرداخت و ارائه‌دهندگان خدمات پرداخت را مجاز کنند. ارائهٔ اطلاعات به افراد دربارهٔ پردازش داده‌های شخصی، پردازش چنین داده‌های شخصی و سایر پردازش‌های داده‌های شخصی برای اهداف این دستورالعمل باید با رعایت دستورالعمل EC/46/95،[4] قوانین ملی که دستورالعمل EC/46/95 و مقررات (EC) شماره 2001/45 را پذیرفته‌اند، انجام شود.

همچنین به‌منظور حفاظت از حریم خصوصی اشخاص، PSD2 در بند دوم مادهٔ ۹٤، ارائه‌دهندگان خدمات پرداخت را مکلف کرده فقط باید با رضایت صریح کاربر خدمات پرداخت به داده‌های شخصی وی به‌منظور ارائهٔ خدمات پرداخت خود دسترسی داشته باشند و آن‌ها را پردازش و نگهداری کنند.

ازآنجاکه از یک طرف تکالیف اقدامات امنیتی تحت PSD بیش از حد گسترده و متنوع هستند و از طرف دیگر، درحالی‌که ارائه‌دهندگان پرداخت موبایلی مرکب از بازیگران مختلفی هستند نیاز به شفافیت در شروط تجهیزات امنیتی و استانداردهای عمومی وجود دارد. باوجوداین درحال‌حاضر چنین استانداردهای عمومی وجود ندارند؛ درنتیجه ارائه‌دهندگان مختلف سرویس‌ها برای سرویس یکسان پرداخت موبایلی سطوح امنیتی متفاوتی به‌کار می‌گیرند.

---

1. Single Euro Payments Area (SEPA)

۲. Third party payment service provider: شرکت یا سرویس‌دهنده‌ای است که به‌عنوان واسطهٔ بین فروشنده و خریدار در پرداخت‌های آنلاین عمل می‌کند. معروف‌ترین این ارائه‌دهندگان خدمات پرداخت شرکت‌هایی مانند PayPal، Stripe وSquare است.

۳. این تکالیف هم در مادهٔ PSD1۷۹ و مادهٔ ۹۴ PDS2 بیان شده‌اند.

٤. این دستورالعمل درحال تجدیدنظر در بسیاری از موارد آن است و اتحادیهٔ اروپا در قالب مقررات عمومی حفاظت از داده‌ها تحت عنوان General Data Protection Regulation از سال ۲۰۱۸ آن را اصلاح کرده است؛ اما به این دلیل که دستورالعمل PDS2 مصوب ۲۰۱۵ است به نسخهٔ مزبور اشاره شده است.

۴-۲. مقررات حمایتی از مشتریان

حمایت کافی از مشتریان حداقل دو جنبه را دربر می‌گیرد: ترتیبات منظم و مقررات کافی برای این‌که مشتریان امکان جبران خسارت را داشته باشند و مسئولیت محدود برای مشتریان. در ادامه براساس مقررات موجود در اتحادیهٔ اروپا این جنبه‌ها بررسی می‌شوند.

نخست به موضوع مقررات جبران خسارت برای مشتریانی که به دنبال تعقیب دعوای مطالبهٔ خسارت هستند پرداخته خواهد شد که در بند اول و دوم مادهٔ ٦٠ PDS1 بیان شده است. قوانین عموماً ارائه‌دهندگان خدمات پرداخت را مکلف می‌کنند که برای تراکنش‌های تأیید نشده، قابلیت استرداد فوری را پیش‌بینی کنند.

در مادهٔ ٧٣ PDS2 مقرر شده است که کشورهای عضو باید تضمین کنند درصورت تراکنش پرداخت غیرمجاز، ارائه‌دهندهٔ خدمات پرداخت، مبلغ تراکنش پرداخت غیرمجاز را فوراً و در هر صورت حداکثر تا پایان روز کاری بعدی، بعد از اعلامِ کاربر یا اطلاع از معامله، به‌استثنای مواردی که ارائه‌دهندهٔ خدمات پرداخت مربوطه، دلایل منطقی برای مشکوک به تقلب بودن تراکنش داشته باشد و آن دلایل را به‌صورت کتبی به مقام ملی مربوطه اعلام کند، به کاربر بازپرداخت می‌کند. درصورت لزوم، ارائه‌دهندهٔ خدمات پرداخت باید حساب پرداخت بدهکار شده را به حالتی بازگرداند که اگر تراکنش پرداخت غیرمجاز انجام نمی‌شد، در آن موقعیت قرار می‌گرفت.

بااین‌حال، برای اعمال این چهارچوب قانونی درمورد پرداخت‌های موبایلی چالش‌هایی وجود دارد: نخست این‌که برای مشتریان در سرویس‌های پرداخت موبایلی، مانند کسانی که از فنّاوری NFC یا کانال‌های MNO استفاده می‌کنند، اثبات تراکنش تأییدنشده مشکل خواهد بود. برای مثال اگر مشتری دستگاه موبایلی را که قبلاً از آن برای پرداخت موبایلی ازطریق NFC یا کانال MNO استفاده کرده است گم کند، انجام هرگونه معاملهٔ تأییدشده‌ای با استفاده از این دستگاه، که همهٔ اطلاعات حساس مهم را در خود دارد، برای سارق آسان است و اثبات غیرمجاز بودن تراکنش بسیار دشوار.

دوم این‌که ازآنجاکه برخی ارائه‌دهندگان سرویس خدمات پرداخت، به‌ویژه ارائه‌دهندگان سرویس خدمات پرداخت شخص ثالث، هنوز تحت مقررات موجود قرار نگرفته‌اند یا این سرویس‌ها به‌نحوی طراحی شده‌اند که اساساً خارج از نظارت مقامات رسمی باشند، اعمال مادهٔ ۶۰ PSD نسبت به آن‌ها مشکل خواهد بود. درنتیجه پیگیری و تعقیب دعوای جبران خسارت برای مشتریانی که «تراکنش تأییدنشده» داشته‌اند، مشکل خواهد بود.

ثانیاً چهارچوب قانونی مسئولیت محدود برای مشتریان تحت مادهٔ ۵۶ psd مقرره‌گذاری شده است. این چهارچوب شامل مسئولیت صفر برای مشتریان بعد از اعلام و انتشار آگهی مفقودی یا اعلام سرقت، مسئولیت محدود تا حداکثر ۱۵۰ یورو برای مشتری، که نتواند ابزارهای خود را ایمن سازد و مسئولیت کامل برای مشتری که درگیر کلاهبرداری یا تعدی و تفریط[1] شده باشد، می‌شود.

هنگامی‌که این نظام مسئولیت محدود برای مشتریان اعمال شود، چالش‌ها سر برمی‌آورند. اولین چالش با طرز فکر اصولی زیرساختی چهارچوب مسئولیت ارتباط دارد که مبتنی بر گم شدن یا به سرقت رفتن ابزار دستگاه گوشی است. اگر مشتری سرقت یا مفقودی گوشی خود را به ارائه‌دهندگان سرویس خدمات پرداخت اعلام کرده باشد، از هرگونه مسئولیتی (برابر با صفر) معاف خواهد شد. برعکس اگر از انجام این کار غفلت ورزیده باشد، به حداکثر میزان مسئول خواهد بود.

چالش اینجاست که پرداخت‌های موبایلی ازطریق دستگاه گوشی اتصال پیدا می‌کنند و دستگاه گوشی مانند کارت اعتباری ابزار پرداخت نیست. کارکرد اصلی دستگاه گوشی به‌منزلهٔ ابزار ارتباطی باقی خواهد ماند و در این حالت، برای مشتری غیرممکن است که به ارائه‌دهندگان خدمت اعلام کند گوشی وی دزدیده یا گم شده است. برای مثال درمورد پرداخت‌های موبایلی مبتنی‌بر mno، به‌لحاظ تئوری، تلاش‌های متعدد مشتری برای اعلام سرقت یا مفقودی به ارائه‌دهندگان خدمت متصور است. زمان زیاد بین مفقودی یا سرقت و اطلاع مالك از این موضوع و

1. Gross negligence

همچنین اعلام آن به مراجع ذی‌صلاح، فرصت بیشتری به متصرف غیرقانونی می‌دهد که با انجام معاملات غیرمجاز منافعی را تحصیل کند. این مسئله به‌ویژه درمورد پرداخت‌های موبایلی، که از فنّاوری nfc کانال‌های mno استفاده می‌کنند، پیش می‌آید.

دومین چالش با مسئولیت حداکثر تا ۱۵۰ یورو ارتباط دارد. پرداخت‌های موبایلی عمدتاً برای پرداخت‌های جزئی استفاده می‌شود که دارای ارزش مالی کم، تراکنش‌های شخصی و روزمره مانند خرید یک استکان قهوه یا تراکنش شخص به شخص ـ که عمدتاً بدون هرگونه معاملهٔ پایه انجام می‌شود ـ هستند. جدول پرداخت‌های موبایلی، که آیدن[1] تهیه کرده است، نشان می‌دهد متوسط ارزش تراکنش‌های خرید آنلاین استفاده شده با گوشی در سال ۲۰۱۴ فقط ۲۸٫۲۷ یورو بوده است. اگرچه همین میزان به‌نسبت سال قبل، که ارزشی حدود ۲۰٫۶ یورو داشته، ۳۷ درصد رشد داشته است. بااین‌حال هنوز این معامله در مقایسه با مبلغ مسئولیت محدود فاصله زیادی دارد؛ ازاین‌رو درحقیقت تحمیل مسئولیت ۱۵۰ یوروئی به مشتریان بسیار زیاد است. به عبارت دیگر، لازم است سقف این مسئولیت به مبلغی کاهش یابد که عموماً مشتریان در پرداخت‌های روزمره استفاده می‌کنند. این سقف را می‌توان براساس متوسط ارزش معاملات یک‌روزهٔ خود همان مشتری تعیین کرد؛ بدین‌ترتیب کسی که متوسط پرداخت‌هایش حدود ۳۰ یورو در روز است باید به همین اندازه مسئولیت داشته باشد. بدیهی است قانونگذار ایرانی باید در مقام تعیین مبلغ مزبور با در نظر گرفتن وجه رایج و نرخ تورم و تجویز تعدیل وجه مزبور ازطریق آیین‌نامه یا دستورالعمل اقدام به مقرره‌گذاری کند.

۵. تحولات مقرره‌گذاری در اتحادیهٔ اروپا از PSD1 تا PSD2

دستورالعمل PSD2 چهارچوب‌های قانونی مربوط به امنیت سیستم‌های پرداخت موجود را با چندین اصلاحیه برای تقویت برخی نقاط ضعف حفظ کرد. برمبنای آنچه در تاریخ ۲۰ نوامبر ۲۰۱۳ بانک مرکزی اروپا (ECB) معرفی کرد، پیش‌نویس توصیه در واقع توسط مجمع اروپایی امنیت پرداخت‌های جزئی،[2] با هدف تعیین حداقل الزامات استفاده شده برای سیستم‌های پرداخت موبایلی توسعه داده شد. در این بخش، ابتدا به بررسی توصیه‌های مجمع اروپایی امنیت پرداخت‌های جزئی و سپس به بررسی اصلاحات دستورالعمل PDS2 پرداخته خواهد شد.

گفتنی است نسخهٔ PDS3 نیز از ۲۳ آوریل ۲۰۲۴ در اتحادیه مطرح شده است و کشورهای عضو باید تا ژوئن ۲۰۲۴ نظرات خود را دربارهٔ آن مطرح کنند. این نسخه با هدف حمایت از مشتریان درصدد ارتقای سطح امنیتی تأیید هویت کاربران و افزایش رقابت‌پذیری در صنعت خدمات پرداخت است[3].

۵-۱. الزامات امنیتی تحت توصیهٔ پیشنهادی

بانک مرکزی اتحادیهٔ اروپا در نوامبر ۲۰۱۳ به‌منظور تبیین اصول کلی حاکم بر پرداخت‌های موبایلی اقدام به تهیه و انتشار توصیه‌نامهٔ مهمی کرد (European Banking Authority, 2013). این توصیهٔ پیشنهادی شامل پنج اصل هدایت‌کننده و چهارده توصیهٔ اجرایی است. پنج اصل هدایت‌کننده از این قرارند که ارائه‌دهندگان خدمات پرداخت موبایلی باید: ۱) خطرات موجود در خدمات خود را شناسایی و ارزیابی کنند و کاهش دهند؛ ۲) مکانیسم احراز هویت قوی‌ای را اجرا کنند؛ ۳) از اطلاعات کاربر، هم در حالت انتقال و پرداخت و هم در حالت عدم استفاده و استراحت حفاظت کنند؛ ٤) از مدیریت ایمن برای دادن جواز و نظارت بر انتقالات به‌منظور جلوگیری از تقلب و کلاهبرداری استفاده کنند؛ ٥) اطلاعاتی را درمورد موضوع امنیت به کاربر ارائه دهند و در آموزش مشتری سهیم باشند.

1. Ayden
2. The European Forum on the Security of Retail Payments (SecuRe Pay)

۳. با توجه به این‌که نسخهٔ موجود تاکنون به تصویب نرسیده است، درحال حاضر قابلیت استناد ندارد؛ اما ضرورت دارد پژوهشگران دیگر هنگام پژوهش به تصویب یا عدم تصویب این نسخه توجه ویژه داشته باشند. آخرین اطلاعات ازطریق سایت پارلمان اتحادیهٔ اروپا قابل دسترس است. www.europarl.europa.eu

این پنج اصل هدایت‌کننده به‌تفصیل در چهارده توصیه بیان شده‌اند. این توصیه‌ها شامل سه حوزه هستند: الزامات کنترل و امنیت عمومی، کنترل خاص و اقدامات امنیتی قابل اجرا برای پرداخت موبایلی و آموزش و ارتباطات مشتری. چهارده توصیه به‌طور جزئی برای رسیدن به سطح بالایی از استانداردهای مربوط به امنیت پرداخت‌های موبایلی بسیار مستحکم‌اند. چنین توصیه‌هایی شامل موارد ذیل است: ۱. اداره کردن؛ ۲. ارزیابی ریسک؛ ۳. نظارت و گزارش حادثهٔ امنیتی؛ ٤. کنترل ریسک و کاهش دادن؛ ٥. ردیابی؛ ٦. شناسایی اولیهٔ مشتری و اطلاعات؛ ۷. احراز هویت قوی؛ ۸. مقررات ابزارها و نرم‌افزارهای احراز هویت؛ ۹. تلاش‌های احراز هویت و احراز هویت خارج از زمان؛ ۱۰. نظارت بر انتقالات؛ ۱۱. حفاظت از اطلاعات حساس و شخصی؛ ۱۲. آموزش کاربر و ارتباطات وی؛ ۱۳. اعلانات و تنظیم محدودیت‌ها؛ ١٤. دسترسی کاربر به اطلاعات وضعیت و اجرای پرداخت.

۵-۲. مقررات امنیتی تحت PSD2

دستورالعمل PSD2 اصولی کلی را، که تحت PSD1 اعمال می‌شوند، با تفاوت‌هایی جزئی ابقا کرد. مقررات مربوط به تدابیر امنیتی تحت فصل پنجم در خصوص مدیریت ریسک‌های عملیاتی و امنیتی، ضرورت ارائهٔ گزارش رویدادهای عملیاتی و امنیتی عمده، لزوم احراز هویت مشتریان توسط ارائه‌دهندگان خدمات پرداخت و بیان استانداردهای فنی نظارتی درمورد احراز هویت و ارتباطات، در مواد ۹۵ تا ۹۸ پیش‌بینی شده‌اند.

اولین مقرره مربوط به مدیریت ریسک‌های عملیاتی و امنیتی است. در مادهٔ ۹۵ کشورهای عضو مکلف شده‌اند اطمینان حاصل کنند که ارائه‌دهندگان خدمات پرداخت، چهارچوبی را با اقدامات کاهش ریسک و سازوکارهای کنترل مناسب برای مدیریت ریسک‌های عملیاتی و امنیتی مرتبط با خدمات پرداختی که ارائه می‌دهند، برقرار کنند. به‌عنوان بخشی از این چهارچوب، ارائه‌دهندگان خدمات پرداخت باید رویه‌های مؤثر مدیریت رویداد را، ازجمله شناسایی و طبقه‌بندی رویدادهای عملیاتی و امنیتی عمده، ایجاد و نگهداری کنند (PSD2. 95.1). همچنین کشورهای عضو باید اطمینان حاصل کنند که ارائه‌دهندگان خدمات پرداخت، ارزیابی به‌روز و جامعی از ریسک‌های عملیاتی و امنیتی مرتبط با خدمات پرداختی که ارائه می‌دهند و کفایت اقدامات کاهش ریسک و سازوکارهای کنترل اجرا شده در پاسخ به آن ریسک‌ها، به‌صورت سالانه یا با فواصل کوتاه‌تر، بنا به تشخیص مقام ذی‌صلاح، به مقام ذی‌صلاح ارائه دهند (PSD2. 95.2).

مقررهٔ دوم مربوط به ضرورت ارائهٔ گزارش رویدادهای عملیاتی و امنیتی عمده است. درصورت بروز هرگونه رویداد امنیتی عمده، ارائه‌دهندگان خدمات پرداخت باید بدون تأخیر، موضوع را به مقام ذی‌صلاح در کشور متبوع خود اطلاع دهند. درصورتی‌که این حادثه در منافع مالی کاربران خدمات پرداخت تأثیر داشته باشد یا امکان تأثیر در آن را داشته باشد، ارائه‌دهنده خدمات پرداخت باید بدون تأخیر غیرضروری، کاربران خدمات پرداخت خود را از حادثه و کلیهٔ اقداماتی که برای کاهش تأثیرات منفی حادثه انجام دهند، مطلع کند (PSD2. 96.1). پس از دریافت اطلاعیهٔ مذکور در بند ۱، مقام ذی‌صلاح کشور عضو مبدأ باید بدون تأخیر غیرضروری، جزئیات مربوط به حادثه را در اختیار سازمان مستقل بانکداری اروپا[1] و بانک مرکزی اروپا (ECB) قرار دهد. مقام ذی‌صلاح، پس از ارزیابی ارتباط حادثه، مطابق با ضوابط، مقامات ذی‌صلاح آن کشور را در جریان امر قرار خواهد داد. دو نهاد مزبور با مشارکت مقام ذی‌صلاح کشور عضو مبدأ، ارتباط حادثه را با سایر نهادهای مرتبط در سطح اتحادیه اروپا و ملی ارزیابی نموده و مطابق با آن، اطلاع‌رسانی خواهند کرد. بانک مرکزی اروپا، اعضای نظام اروپایی بانک‌های مرکزی را درمورد موضوعات مرتبط با سامانهٔ پرداخت. مطلع خواهد کرد. براساس آن اطلاع‌رسانی، مقامات ذی‌صلاح درصورت لزوم، تمامی اقدامات لازم را برای حفاظت از امنیت فوری سامانهٔ مالی انجام خواهند داد (PSD2. 96.2).

1. European Banking Authority (EBA)

مادهٔ ۹۷ دستورالعمل، کشورهای عضو را مکلف کرده که اطمینان حاصل کنند ارائه‌دهندگان خدمات پرداخت، برای تراکنش‌های پرداخت الکترونیکی از راه دور، از احراز هویت قوی مشتری استفاده کنند (بند ۲ مادهٔ ۹۷) و اقدامات امنیتی کافی برای محافظت از محرمانه‌بودن و صحت اعتبارنامه‌های امنیتی شخصی کاربران خدمات پرداخت در نظر گرفته شده باشد (بند ۳ مادهٔ ۹۷).

آخرین مقرره مربوط به استانداردهای فنی نظارتی درمورد احراز هویت و ارتباطات است. مادهٔ ۹۸ دستورالعمل، سازمان مستقل بانکداری اروپا را مکلف کرده با همکاری نزدیک بانک مرکزی اروپا و پس از مشورت با همهٔ ذی‌نفعان مرتبط، ازجمله بازیگران بازار خدمات پرداخت، با در نظر گرفتن منافع همهٔ طرف‌های درگیر، پیش‌نویس استانداردهای فنی نظارتی خطاب به ارائه‌دهندگان خدمات پرداخت را تنظیم کند. این پیش‌نویس باید شامل نکات ذیل باشد: الف) اطمینان از سطح مناسب امنیت برای کاربران خدمات پرداخت و ارائه‌دهندگان خدمات پرداخت ازطریق اتخاذ الزامات مؤثر و مبتنی بر ریسک؛ ب) تضمین امنیت وجوه و اطلاعات شخصی کاربران خدمات پرداخت؛ ج) تأمین و حفظ رقابت عادلانه بین همهٔ ارائه‌دهندگان خدمات پرداخت؛ د) تضمین بی‌طرفی فناوری و مدل کسب‌وکار؛ هـ) امکان توسعهٔ روش‌های پرداخت کاربرپسند، در دسترس و نوآورانه (بند ۲ مادهٔ ۹۸).

نتیجه‌گیری

تضمین دو عنصر «امنیت» و «دسترسی و قابلیت استفاده» در ابزارهای پرداخت موبایلی باعث ارتقای سطح استفاده از این نوع ابزارها و درنتیجه تحقق زمینه‌های توسعهٔ اقتصادی خواهد شد. بدین‌منظور توجه به مشکلات و چالش‌های خاص و ویژهٔ دستگاه‌های گوشی تلفن همراه نظیر نوع طراحی فیزیکی، محدودیت ورودی و امکان حملهٔ بدافزارها از یک‌سو و چالش‌های امنیتی مرتبط با ناآگاهی استفاده‌کنندگان و کم‌تجربگی ارائه‌دهندگان خدمات پرداخت از سوی دیگر، ضرورت تأمین امنیت را دوچندان کرده است. مقنن باید در هنگام قانون‌گذاری، با در نظر گرفتن این چالش‌ها و با توجه به ارتقای هر روزهٔ فناوری این‌گونه پرداخت‌ها، بین تعیین حداقلی از سطح امنیتی و قابلیت استفاده از سامانه‌های پرداخت، تعادل ایجاد کند. روش‌های امنیتی باید پویایی ارتقای فناوری و همچنین تکامل‌یافتگی تهدیدات را پوشش دهند. قواعد حقوقی حمایتی از مشتریان و بیان تکالیف ارائه‌دهندگان خدمات سرویس پرداخت و دولت‌ها، که در دستورالعمل صادره از سوی اتحادیهٔ اروپا به‌نحو قابل قبولی پیش‌بینی شده‌اند، برای قانون‌گذار ایرانی نیز الگوی مناسبی است تا با در نظر گرفتن مقررات موجود و ظرفیت بومی کشور اقدام به قانون‌گذاری در این زمینه کند.

منابع

Clarkson, E. C., Patel, S. N., Pierce, J. S., & Abowd, G. D. (2006). *Exploring continuous pressure input for mobile phones*. Link

Conseil Européen des Paiements AISBL. (2014). *Overview of mobile payments initiatives* (EPC091-14).

Desai, S. (2014). *Mobile payment services: Security risks, trends and counter measures*. RSA Conference 2014. Asia Pacific & Japan. Link

European Banking Authority. (2013). *Recommendations for the security of mobile payments draft document for public consultation*.

European Central Bank. (2013). Recommendations for mobile payments. Link

European Parliament and Council. (2007). Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC. *Official Journal of the European Union, L 319*, 1-36. Link

European Parliament and Council. (2015). Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market. *Official Journal of the European Union, L 337*, 35-127. Link

European Payment Council. (n.d.). *Summer reading: Results of latest EPC poll reveal that instant payments are most likely trigger the next wave of innovation* (blog).

European Payments Council. (2010). *White paper mobile payments version 2.0 final doc* (EPC492-09).

European Payments Council. (2014). *Overview mobile payments initiatives* (EPC091-14). Version 2.0. Link

Kasiyanto, S. (2016). Security issues of new innovative payments and their regulatory challenges in Bitcoin and mobile payments: Constructing a European framework. In G. Gimigliano (Ed.), *Bitcoin, and mobile payments: Constructing a European Union framework* (pp. 123-145). Palgrave Macmillan.

Liao, S-H., & Ho, C-H. (2021). Mobile payment and mobile application (App) behavior for online recommendations. *Journal of Organizational and End User Computing (JOEUC), 33*(6). https://doi.org/10.4018/JOEUC.20211101.oa2

Mckinsey. (2023). *The 2023 mckinsey global payments report*. Link

Rutledge, S. L. (2010). *Consumer protection and financial literacy: Lessons from nine country studies* (Policy and Research Working Papers, 26-53).

Rysman, M., & Schuh, S. (2017). New innovations in payments. *Innovation Policy and the Economy*, *17*(1), 27-48. https://doi.org/10.1086/688843

Souppaya, M., & Scarfone, K. (2013). *Guidelines for Managing the Security of Mobile Devices in the Enterprise* (NIST Special Publication 800-124).

Statista. (n.d.). *Malware attacks per year worldwide*. Link

Van den Akker, M., Stewart, N., & Isoni, A. (2023). *Tapping out: The effect of contactless payments on expenditure recall*. http://dx.doi.org/10.2139/ssrn.4497598

Zandi, M., Koropeckyj, S., Singh, V., & Matsiras, P. (2016). *The impact of electronic payments on economic growth*. Link