



EMV Smart Cards: Legal Status and Fraud-Related Liability

Maisoon Al-Masri

Faculty of Law, Sohar University, Sohar 311, Oman.
MMasri@su.edu.om

Abstract. This study highlights the legal validity of smart chip payment cards operating under the EMV standard, which is no longer merely a technological innovation but has become a pivotal shift in how liability and evidence are handled in bank transactions. The technological features EMV cards provide — such as encryption, dynamic authentication, and data verification — offer stronger security and greater evidentiary value than those of traditional magnetic stripe cards. However, the rise of sophisticated cyber fraud—especially phishing—has revealed the limitations of technical safeguards alone, prompting renewed legal debates over the duties and liabilities of banks, cardholders, and merchants, especially in the absence of clear legislation that precisely defines the concept of “gross negligence” and specifies the obligations of banks in addressing cyber risks. The research adopts a descriptive method to clarify the concept of EMV cards and an analytical method to examine legal systems and judicial rulings to determine liabilities among parties and the legal bases on which these liabilities are founded. This study concludes that conventional liability is inadequate in today’s digital landscape and advocates for integrating modern legal principles, such as Risk Bearing and the Liability-Shift rule.

Keywords: Banking Fraud, EMV standard, Gross Negligence, Liability-Shift, Risk Bearing.

1 Introduction

In recent decades, the financial sector has witnessed a profound digital transformation, with electronic payment methods becoming the cornerstone of global commerce and personal finance [1]. Among these innovations, the EMV smart payment card has emerged as a significant advancement over traditional magnetic stripe cards [2]. This card creates a special code for every transaction, which makes it much harder for fraudsters to copy or use the card information in fraud. EMV cards were developed to reduce the risk of payment fraud and protect users [3].

As electronic payments continue to replace cash and checks, the legal systems around the world are increasingly challenged to respond to the complexities arising from these technologies. The introduction of EMV cards has reshaped liability frameworks and raised questions about how responsibility is allocated when fraud occurs. While EMV cards are widely recognized for their technical advantages [4], the legal consequences of using them are still unclear in many jurisdictions.

This research explores the link between financial technology and legal responsibility. It aims to understand how legal systems have dealt with the challenges of EMV technology, especially in cases of unauthorized or fraudulent transactions. The move from magnetic stripe cards to chip-based cards was not just a technical improvement [5]; it also shifted the burden of liability among stakeholders—banks, merchants, and consumers.

One of the central issues that has emerged is the concept of the “liability shift,” which reallocates responsibility for fraudulent transactions under certain conditions, particularly when merchants fail to adopt EMV-compatible terminals. While this shift was intended to incentivize the adoption of more secure technologies, it has also raised concerns about fairness and the protection of consumer rights, especially in situations where the cause of the fraud remains unclear.

Additionally, the implementation of EMV authentication standards has created new evidentiary challenges. Banks often claim that a transaction is legitimate as long as EMV protocols were followed, thereby shifting the burden of proof onto consumers who may lack the technical means to challenge such claims. In legal disputes, this imbalance of power may undermine the principles of due process and fair adjudication.

Given the global spread of EMV adoption and the divergent legal approaches, this study employs a legal analysis to examine legal principles, legislative frameworks, and judicial developments to assess the consistency and effectiveness of the legal protections available to the parties.

The importance of this study lies not only in highlighting the legal gaps in regulating the use of EMV cards, but also in calling for a fairer system of liability. As financial technologies continue to develop, the laws that govern them must also keep up—making sure that innovation does not come at the expense of legal certainty or consumer protection.

We will begin by clarifying the concepts of the Smart Chip Card and the EMV standard, and outlining their advantages and disadvantages, before moving on to examine the scope of liability for the main parties involved in their use.

1.1 Definition of the EMV Smart Card

The EMV Smart Chip Card is a plastic payment card equipped with an electronic chip that serves as a central processing unit (CPU) [6]. This chip can securely store and process data much more efficiently than traditional magnetic stripes. It allows for data to be updated after each transaction [7], thereby enhancing both the security and speed of banking operations. These smart chip cards contain a miniature computer that systematically stores and processes information [8].

These smart cards are classified into three types: 1) contact cards, contactless cards, and 3) dual interface cards. The contact cards require physical insertion into a smart card reader to initiate communication, while the contactless cards use wireless technologies such as NFC or RFID to transmit data without physical contact [9],[10]. Other than that, the dual interface cards contain a chip that supports both contact and contactless reading, allowing data to be accessed either by direct insertion into a reader or through near-field wireless communication [11].

1.2 Definition of the EMV Standard

The EMV (Europay, MasterCard, and Visa) standard is an international security protocol for payment cards, developed by three leading companies: Europay, MasterCard, and Visa [12]. It relies on advanced encryption protocols that prevent manipulation, thereby enhancing the security of banking transactions [13].

The EMV standard is managed by an independent entity, EMVCo, established in 1999 [14], which is responsible for developing global technical specifications for smart card usage. EMVCo is jointly owned by six major global payment networks: American Express, Discover, JCB, Mastercard, UnionPay, and Visa [14]. "EMV" is a registered trademark jointly owned by these companies.

This collaborative framework reflects a global commitment to securing and standardizing payment systems across borders [15]. Today, EMV technology is widely adopted by banks worldwide, including in Europe, the United States, Saudi Arabia (via the Mada network), and Egypt (via the Fawry/Vera network). France implemented EMV as early as 2006, while the United States began its transition in 2012 [16].

1.3. Advantages of EMV Smart Cards

Enhancing Security and Fraud Resistance. Smart cards significantly reduce the risk of financial fraud through advanced encryption technologies [2]. They employ a dynamic authentication code unique to each transaction, making data cloning or interception significantly more difficult [17].

Protection of Personal and Financial Information. The chip securely encrypts and processes customer data, unlike magnetic stripe cards. This thus reduces the risk of data breaches or theft [18].

Compliance with Global Standards. EMV cards are widely accepted across the globe and operate seamlessly on point-of-sale systems and ATMs in most countries, facilitating international travel and cross-border transactions [19].

Two-Factor Authentication (2FA). These cards support multifactor verification by combining the card with PIN or biometrics [20]. This provides an added layer of protection against fraud and identity theft [21].

Accelerating Banking Transactions. Smart chip cards speed up financial operations, particularly with modern contactless payment technologies. They also support multi-currency transactions, allowing users to make payments abroad with ease, without needing manual intervention or third-party services [22].

The Analysis of Authorization Requests Using an AI System. Mastercard and other financial institutions have adopted sophisticated artificial intelligence systems to analyse authorization requests globally. This AI system generates risk-based approval or rejection decisions without requiring complex infrastructure [23]. It adapts to evolving fraud patterns and builds updated behavioural profiles of cardholders and merchants, enhancing the detection of unusual activity [24], and enabling the halting of suspicious transactions at the stage of authorisation [25]. This system also supports regulatory compliance, such as anti-money laundering efforts and risk management.

1.4 Disadvantages of EMV Smart Cards

Despite their numerous advantages, smart chip cards face several drawbacks:

High Cost of Manufacturing and Implementation. The production and deployment of smart cards and compatible infrastructure are significantly more expensive than magnetic stripe systems [11].

Infrastructure Limitations in Some Countries. Inadequate infrastructure in certain countries, such as Egypt, hampers the effectiveness and widespread adoption of smart chip cards.

Complexity for Non-Specialist Users. The sophisticated systems and procedures associated with EMV cards pose challenges for users lacking technical expertise, which may reduce adoption rates [11].

2 Problem Statement

Despite the widespread adoption of EMV smart payment cards as a global standard for secure financial transactions, their integration into the legal landscape remains

fraught with challenges. While the EMV chip was introduced as a technological solution to the persistent problem of card-based fraud—particularly card cloning and counterfeiting—it has inadvertently created new legal complexities concerning liability, standards of proof, and consumer protection.

At the core of the issue is a fundamental legal ambiguity: who should be held liable when fraud occurs despite the use of EMV-enabled cards? In principle, EMV technology is designed to enhance transaction security by generating dynamic, transaction-specific data, making it virtually impossible to replicate a card as was done with magnetic stripe cards. Nevertheless, instances of fraud persist in practice, particularly in the form of data breaches resulting from techniques such as skimming, hacking, and phishing.

Banks and card issuers often claim that if the EMV protocol was followed—particularly if the transaction was authenticated through a chip and PIN—then the transaction must have been authorized by the legitimate cardholder. However, this presumption unfairly shifts the burden of proof to consumers, who usually lack the technical ability to show that they didn't authorize the transaction or that the EMV system failed. In legal disputes, courts may find it difficult to weigh these opposing arguments, especially when neither side has clear technical evidence.

Moreover, in many countries, there are no specific laws that directly regulate the use of EMV cards. Instead, courts rely on general legal principles such as contract law, negligence, and consumer protection to resolve disputes, which often leads to inconsistent outcomes. This lack of clear, unified regulations or court guidelines increases legal uncertainty and weakens public confidence in digital payment systems.

The situation becomes even more complicated with the introduction of the “liability shift,” a policy adopted by major payment networks such as Visa and Mastercard. Under this policy, responsibility for certain types of fraud is transferred from banks to merchants if the merchants have not upgraded their systems to support EMV technology. Although this encourages businesses to modernize their payment equipment, it has raised legal and ethical concerns. Merchants may be held responsible even if they had no control over the fraud or if the fraud was technologically sophisticated. At the same time, consumers may find themselves between banks denying responsibility and merchants who may not fully understand their legal duties.

Additional challenges arise in cross-border transactions, where legal systems may handle liability differently and require varying levels of proof. This inconsistency in how EMV-related fraud is addressed weakens attempts to build a unified legal framework for securing digital financial transactions.

Thus, the central legal problem this study addresses is twofold:

The absence of a clear, consistent legal framework to govern liability in cases involving EMV-related fraud.

The potential for unfair allocation of responsibility, particularly where consumers are held accountable without access to adequate technical or legal recourse.

These issues raise important questions about fairness, legal certainty, and the proper allocation of risk in an increasingly digitized financial ecosystem. There is a pressing need to reassess whether current liability models adequately protect consumers and merchants, or whether they serve primarily to shield financial institutions from responsibility in technologically complex disputes.

3 Research Questions

This study explores the legal and regulatory implications of EMV smart payment cards, particularly regarding liability allocation in cases of electronic fraud. As EMV technology becomes increasingly prevalent across global financial systems, important legal questions arise about how responsibility is distributed among banks, merchants, and consumers when fraudulent transactions occur.

To that end, the study is guided by the following core research questions:

3.1 What is the Applicable Legal Framework that Governs the Liability of Issuing Banks in Cases of Electronic Fraud Involving EMV Cards?

Here, the study seeks to identify relevant statutory provisions, case law, and regulatory standards that define the circumstances under which banks may be held liable for fraudulent EMV transactions.

3.2 Can Customers be held Legally Responsible for Losses Arising from Fraud, Particularly When Banks Allege Negligence or User Error, even in the Absence of Technical Proof that the EMV Transaction Complied with the Required Security standards?

This question critically addresses the evidentiary challenges faced by consumers and whether existing legal systems adequately protect their rights in the event of disputes with financial institutions.

3.3 To what extent can Merchants be held Liable in Cases of Fraud Involving EMV Cards, and what is the legal basis and Validity of the 'Liability Shift' Principle in such Contexts?

The question seeks to examine the extent of merchant responsibility and assess whether liability-shifting measures are legally sound and justifiable.

3.4 How Fair and Enforceable are Liability Shift Policies in Practice, and to What Extent Do They Align with Principles of Consumer Protection and Contractual Justice

The final question focuses on evaluating merchant responsibility, examining the fairness and enforceability of liability-shifting policies introduced by payment networks, and assessing their alignment with consumer protection and contractual justice.

Through these questions, the study aims to provide a comprehensive legal analysis of EMV smart card usage, with the broader goal of promoting a more balanced and just allocation of responsibility in the digital payments ecosystem.

4 Purpose of Study

The primary aim of this study is to critically examine the legal status and liability issues surrounding the use of EMV smart payment cards in electronic financial transactions. It analyses the security features of EMV technology to assess their legal implications, particularly regarding the liability of issuing banks in cases of fraud. The study also explores when consumers may be held accountable for fraudulent losses, especially where banks allege negligence without clear technical proof, and evaluates merchant liability under the ‘liability shift’ principle. Ultimately, it seeks to clarify the distribution of liability among stakeholders and propose recommendations for fairer legal frameworks.

5 Research Methods

This study adopts a descriptive-analytical approach to define EMV smart payment cards and highlight their advantages and disadvantages. It analyses the legal liabilities arising from their use. The research focuses on relevant laws, recent French judicial precedents, expert legal writings, and regulatory frameworks such as those in the United Arab Emirates. Data was collected through an extensive review of legal texts, rulings, and scholarly sources. By combining description with legal analysis, the study aims to clarify the liabilities associated with EMV cards and to propose recommendations to strengthen consumer protection and fraud-prevention laws.

6 Findings

These sections explore the legal foundations of liability in financial fraud cases, focusing on the responsibilities of banks, cardholders, and merchants.

6.1 Instances of Bank Liability and Its Legal Basis

Various forms of fraud are associated with bank cards, most notably skimming, which involves duplicating card data without the customer’s knowledge [26], hacking of banking databases [27] and phishing, whereby a third party impersonates a trusted entity to deceive the customers and obtain their confidential information [28].

The bank is deemed liable for skimming or hacking [29], particularly when a deficiency in its cybersecurity infrastructure is proven—provided that no gross negligence can be attributed to the customer [30].

In cases of phishing, even though the fraud is perpetrated by a third party, the issuing bank remains obliged to reimburse the debited funds unless it can prove that the customer acted with gross negligence [31].

Bank liability for electronic fraud is grounded in a set of integrated legal principles designed to protect customer rights and ensure the security of banking operations. These bases can be summarised as follows:

First Basis: Duty to Ensure Cybersecurity. The bank's liability for fraud involving smart cards stems from its breach of the duty to ensure cybersecurity and protect customer data [34]. This obligation is based on the principle of professional diligence [32], requiring the bank to implement all necessary technical and organizational measures. As a professional entity, the bank is held to a higher standard of care than an ordinary person [62].

The American case *Western State Bank v. DataGuard Inc.*, a technology service provider, highlights a bank's duty to maintain strong cybersecurity. The court ruled in (2023) that the duty of reasonable security is not just about using tools like firewalls and encryption. It also includes being able to respond quickly to cyber incidents—such as rapid breach detection, reporting, damage mitigation, and system recovery. The court emphasized that cybersecurity must be dynamic, requiring regular updates to address emerging threats. Failure to maintain or upgrade systems may constitute negligence [33]. This court ruling helps us analyze and deduce the forms of breach of the duty to ensure cybersecurity imposed on banks toward their customers, including:

Case One: Bank Error Due to Failure to Protect Customer Data. The bank is liable if it fails to implement necessary security measures such as data encryption or monitoring and reporting breaches. These are considered a violation of its professional duties [34]. If such failure leads to sensitive data disclosure through a cyberattack causing financial harm to customers, the bank bears legal responsibility and must compensate for damages.

Case Two: Bank Error Due to Negligence in Protecting Customers from Phishing Attacks. The bank is liable for damages caused by phishing if it fails to adequately educate customers or enhance security. Bank liability is especially clear if its name or logo is used in fraudulent communications without proper warnings to customers or verification enhancements [35]. The French Court of Cassation confirmed in **2020** that the bank is a “guarantor” of digital security and is exempt from liability only if the customer's gross negligence is proven [36].

In a recent judicial ruling by the French Court of Cassation, the court confirmed in **2024** the bank's liability in phishing cases, holding that mere customer error in disclosing banking data to a fraudster impersonating a bank employee does not constitute the customer's gross negligence excusing the bank [37]. In **2025**, the French Court of Cassation expanded bank liability to protect even professional clients from “spoofing” attacks unless fault on the clients' part is demonstrated [38]

Case Three: Bank Error Due to Technical Malfunction in the Electronic Banking System. If a technical failure leads to fraudulent transactions, the bank is legally liable and obligated to compensate, based on its duty to provide a secure electronic system [39]. Liability here may be contractual for acts of the thing (such as ATM and banking electronic systems) under the bank's custody. Some jurists also support tort liability due to negligence in system maintenance or supervision, which is considered a harmful act.

For instance, the Paris Court of Appeal [40] ordered a bank to compensate a client for fraud transactions on her account, despite the use of 3D Secure authentication [41]. The bank failed to prove that the client received verification codes or expressly consented, and did not demonstrate banking system integrity or client fault. The court held that the burden of proof is on the bank to show that the transactions were authorised and that the security system was faultless, reinforcing customer protection against technical failures.

Case Four: Bank Error in Failing to Regularly Update Security Systems. The bank is responsible for damages from account breaches if it neglects to regularly update its security systems [42]. Continuous updates constitute a legal obligation to safeguard customer data and funds from cyber threats. This failure is classified as gross negligence, giving rise to contractual or tort liability, especially if attacks could have been prevented by regular updates [43].

Case Five: Breach of Banking Confidentiality. Breach of banking confidentiality caused by employee negligence or inadequate internal controls is considered gross misconduct by the bank and entails legal liability [44]. Banks have a legal and professional duty to protect customers' financial data, and any data leakage reflects failures in employee training or enforcement of internal security protocols [45]. This breach violates contractual obligations, making the bank liable for compensating affected customers.

Case Six: Bank Error in Failing to Secure ATMs Against Skimming Devices. Banks are liable to compensate customers if their accounts are compromised due to ATM security weaknesses, such as the installation of skimming devices that steal card data and PINs [46]. The bank must provide a secure, tamper-proof environment and implement technical and supervisory measures to prevent manipulation or misuse of ATM machines [30].

Second Basis: Theory of Risk Bearing (Strict Liability). Traditional tort liability, which requires establishing fault, damage, and causation, is no longer sufficient alone to impose liability on banks, especially given the rapid technological and industrial advancements and the increasing complexity of electronic transactions [47].

The theory of risk bearing—sometimes referred to as strict liability—imposes liability solely on the occurrence of damage to the injured party, regardless of the entity's fault in causing the harm [48].

This theory is based on the premise that every activity inherently involves risks and may cause harm to others, thereby obligating the party engaging in the activity to bear its consequences, even if no fault is proven [48]. . This liability particularly applies when the activity yields profit or benefit to the responsible party or involves extraordinary or unusual risks.

Thus, responsibility under this theory becomes strict liability, meaning that fault need not be proven; hence, it is sometimes called no-fault liability [49]. This theory embodies the principle of "loss and gain," whereby anyone who profits from a certain activity must also bear the damages resulting from it [50].

For this liability to apply, two essential conditions must be met [51] :

The activity must be inherently dangerous by nature or in the manner of its execution, and the activity must constitute a source of benefit or profit for the liable party.

Accordingly, the scope of this strict liability is limited to activities characterized by high risk and significant benefit, aiming to achieve a balance and social solidarity by ensuring effective protection for the harmed parties, even in the absence of fault by the liable party [52].

6.2 Instances of Cardholder Liability and Its Legal Basis

In the evolving legal landscape surrounding EMV smart card use, the liability of the cardholder—typically the consumer—remains a central subject of legal, judicial, and scholarly debate. Although EMV technology was designed to reduce fraud through secure authentication methods such as chip-and-PIN, it has not completely eliminated all forms of fraud associated with unauthorized transactions. Consequently, questions persist about the extent to which consumers may be legally held responsible for fraud committed with EMV cards.

Generally, legal systems tend to protect cardholders, particularly under consumer protection frameworks that presume the consumer's innocence unless gross negligence or intentional misconduct can be proven [25]. This means that the cardholder's liability is based on a balance between the general protection afforded to clients by banking institutions and the client's duty of care and caution in handling their banking data. French jurisprudence has firmly established this balance by distinguishing between ordinary conduct and cases where the client's gross negligence justifies holding them liable for losses resulting from fraud.

However, the concept of "gross negligence" remains legally ambiguous. It is inherently a relative and flexible concept, and its assessment may sometimes favour the client and other times not [53]. Thus, it is interpreted differently across jurisdictions, creating challenges for consistent application.

French laws and regulations oblige clients to maintain the confidentiality of their banking data and consider gross negligence to include acts like: 1) the fraud was clearly identifiable by a reasonable person, such as spelling errors or incorrect bank names, 2) keeping authorization data near the payment device, such as writing the

PIN on the card, and 3) passing authorization data to a third party or disclosing it during withdrawal [54],[55].

On the other hand, the French court of Cassation affirmed that accidental and unintentional disclosure of banking data does not constitute gross negligence that would deprive the client of compensation [36]. For example, a 2017 ruling by the commercial, financial, and economic chamber held that the victim could not reasonably have identified the fraudulent nature of the email received, and thus, providing banking data did not amount to negligence or gross negligence.

That means simply disclosing banking credentials in response to a phishing attempt does not necessarily amount to gross negligence. The burden of proof in such cases typically lies with the bank, as affirmed by the French court of cassation in several decisions. The court of cassation, in a judgment [37], established two fundamental principles reaffirming this bank's obligation, particularly in cases of electronic fraud such as phishing.

- *Principle One:* The burden of proving gross negligence lies with the bank, which must demonstrate that the client acted with severe negligence that inevitably led to fraud. Gross negligence means conduct that shows a severe disregard for the duties of vigilance. Simply the client handing over data to a fraudster impersonating a bank employee does not constitute gross negligence-unless it is proven that the client was aware of the deception.

- *Principle Two:* The bank is obligated to prove the integrity of the technical authentication procedures. If it fails to demonstrate that transactions were executed securely and followed standard procedures, its liability remains even if there is client error-unless such error rises to the level of gross negligence.

Courts have linked these principles to technological developments, noting the increased difficulty clients face in distinguishing fraudulent messages, especially given the widespread use of digital communication following the COVID-19 pandemic [56]. Thus, the court of Riom held that banks must actively educate and warn the clients in such circumstances.

Finally, a critical question arises within the broader discussion of customer negligence: What is the time frame within which a customer may contest withdrawals from their account resulting from fraudulent transactions? Moreover, does a delay in reporting such incidents constitute gross negligence that would disqualify the customer from receiving compensation?

Article L.133-24 grants clients a 13-month period to contest unauthorized transactions [57]. The court has confirmed that initiating a claim within this time frame preserves the client's right to compensation, and that a delay within the limit does not negate eligibility for redress [40].

6.3 Merchant Liability and the Principle of Liability Shift

With the widespread adoption of the EMV standard, merchants have increasingly been implicated in discussions of liability for fraudulent transactions. Traditionally,

merchants bore limited legal responsibility for unauthorised card payments, as the burden primarily rested on issuing banks [12]. However, the introduction of the “liability shift” principle by global payment networks—such as Visa, Mastercard, and American Express—has significantly altered this paradigm.

The liability shift refers to a policy mechanism that transfers the financial responsibility for fraudulent card transactions to the party that has not adopted EMV-compliant infrastructure [58]. If a merchant fails to install EMV-enabled point-of-sale (POS) terminals and accepts a fraudulent transaction using a magnetic stripe card, that merchant—not the bank—is held liable for the resulting financial loss [58]. This mechanism was formally implemented in several regions between 2012 and 2015, most notably in the United States on October 1, 2015 [41].

From a legal standpoint, the liability shift is not derived from statutory law but rather from contractual arrangements between merchants, acquiring banks, and payment networks [25]. It is part of a broader form of private regulatory governance, where commercial terms are enforced through service agreements rather than public legislation. Nevertheless, these terms have binding legal effect and may be enforced in courts as part of the contractual obligations governing payment processing services.

The practical effect of the liability shift has been twofold. First, it incentivized merchants to upgrade their payment infrastructure by tying legal and financial liability directly to compliance [16]. Second, it reallocated risk in a way that some legal scholars argue may be unfair to small merchants, particularly those lacking the resources or awareness to quickly adapt to new technologies [59].

The courts have begun to grapple with the fairness and enforceability of this principle. For instance, in disputes where merchants are held liable despite using alternative security measures, the question arises whether rigid adherence to EMV standards alone should determine liability [60]. Some judgments have shown a willingness to examine whether the merchant took reasonable precautions, even if not technically EMV-compliant, before assigning liability. مرجع

Furthermore, merchants are now legally required to perform due diligence to verify card authenticity and secure their POS environments [25]. Failure to monitor for skimming devices, to update firmware, or to train staff in fraud detection may all be construed as negligence, further exposing merchants to legal liability.

In conclusion, while the liability shift has successfully promoted EMV compliance and reduced overall card fraud [59], it has also raised complex legal issues regarding contractual fairness, unequal bargaining power, and the appropriate distribution of risk. Moving forward, clearer judicial guidelines and, if necessary, legislative interventions may be needed to ensure that the burden placed on merchants is reasonable, proportionate, and consistent with broader principles of contractual justice and consumer protection.

7 Conclusion

This study has addressed the complex legal dimensions of EMV smart payment cards and the distribution of liability in cases of electronic payment fraud. The transition from magnetic stripe cards to EMV technology represents a qualitative leap in securing financial transactions, as EMV provides enhanced protection through dynamic authentication mechanisms and advanced encryption. However, technological innovation alone is insufficient to resolve the intricate legal questions surrounding liability and fairness among banks, merchants, and consumers.

The study emphasizes that banks bear a fundamental obligation to establish and maintain effective cybersecurity systems, and they carry the burden of proving that disputed transactions were lawfully and securely executed. In the absence of proven fault on the part of any cardholder, the bank should be held liable for compensation under the strict liability theory or risk-bearing doctrine. As professional institutions that derive financial gain from their services, banks are expected to bear the associated risks, thereby contributing to the security and stability of the electronic payment system. Conversely, consumers are granted legal protection against liability, except in cases of clearly established gross negligence. Nevertheless, the ambiguity surrounding the concept of “gross negligence” necessitates legislative intervention to define it with precision, ensuring a fair balance between consumer protection and legal certainty for all parties.

The “liability shift” principle has significantly expanded merchants’ liability. While it has encouraged the adoption of EMV-compliant payment terminals, it has simultaneously raised concerns about the fair distribution of risk—particularly for small merchants who may lack the resources to comply. The absence of codified rules governing this principle in many jurisdictions underscores the need for clearer legal frameworks.

Moreover, the study points to a fragmented and inconsistent legal landscape across different legal systems, undermining consumer trust and complicating the enforcement of rights in cross-border transactions. There is an urgent need for unified international standards and collaborative regulatory efforts to address these challenges in the increasingly globalised digital payments environment.

In conclusion, establishing a balanced and effective legal framework for EMV-related fraud liability calls for a multifaceted approach. This includes legislative reforms to codify the rights and duties of all stakeholders, stronger regulatory oversight of cybersecurity practices, and public awareness initiatives to educate both consumers and merchants. Through such comprehensive measures, the intended benefits of EMV technology—both technical and legal—can be fully realized, thereby fostering trust, security, and justice in modern electronic payment systems.

Finally, this study lays the groundwork for a broader analysis of liability shift and risk-bearing theories in banking cards, focusing on their legality and fairness. It

also examines whether the liability shift clause can be viewed as an adhesion contract that enables courts to protect the weaker party and prevent abuse of rights.

References

1. Singh, P., Kumar, N., Gupta, B.: Smart card ID: An evolving and viable technology. *International Journal of Advanced Computer Science and Applications* 9(3), 115–124 (2018).
2. Taherdoost, H., Sahibuddin, S., Jalaliyoon, N.: Smart card security: Technology and adoption. *International Journal of Security (IJS)* 5, 74–84 (2011).
3. Cross, C.: Meeting the challenges of fraud in a digital world. In: *The Handbook of Security*, pp. 217–238. Springer International Publishing (2022).
4. Basin, D., Sasse, R., Toro-Pozo, J.: The EMV standard: Break, fix, verify. In: *IEEE Symposium on Security and Privacy (SP)*, pp. 1766–1781 (2021).
5. Rankl, W., Effing, W.: *Smart Card Handbook*. Wiley & Sons (2004).
6. Walvekar, H., Gautam, S., Patil, C.: Smart card: A single card solution for multiple activities. In: *2nd National Level Students' Research Conference on Innovative Ideas and Invention with Sustainability in Computer Science and IT-2021*, pp. 105–108. *International Journal of Engineering Research* 8 (2021).
7. Al-Hashimi, S.I.: *E-Commerce and Its Rulings in Islamic Jurisprudence*. Vol. 1. Dar Kunooz Ishbiliya, Riyadh (2011). (In Arabic)
8. Ghanem, S.M.: Electronic wallet (e-purse). In: *Proceedings of the Conference on Electronic Banking Between Sharia and Law*. Dubai (2003). (In Arabic)
9. Selmi, S., Seghir, S.: *Étude et Réalisation d'un Programmeur de Carte à Puce et Son Lecteur*. University of Biskra (2010).
10. Emms, M., Arief, B., Little, N., van Moorsel, A.: Risks of offline verify PIN on contactless cards. In: *International Conference on Financial Cryptography and Data Security*, pp. 313–321. Springer, Berlin, Heidelberg (2013).
11. Jordovic Pavlovic, M.: Advantages and disadvantages in implementation of smart cards in payment system. In: *4th International Conference Science and Higher Education in Function of Sustainable Development*, pp. 65–70 (2011).
12. Ahuja, A.: A comprehensive review of EMV compliance in cloud-native architectures: Challenges and frameworks. In: *ACM Symposium on Cloud Computing (SoCC '19)*, Santa Cruz, California (2019).
13. Ouerdi, N., Azizi, M., Lanet, J., Azizi, A., Ziane, M.: EMV card: Generation of test cases based on SysML models. In: *International Conference on Electronic Engineering and Computer Science*, pp. 133–138. Elsevier (2013).
14. Merschen, T.: The impact of EMV migration on the global cards payments infrastructure: How it will change and expand card use. *Journal of Payments Strategy & Systems* 1, 104–115 (2007).
15. Povey, I.: Assessing the impact of EMV migration: A pragmatic delivery approach. *Journal of Payments Strategy & Systems* 2, 349–363 (2008).
16. Figliola, P.M.: The EMV chip card transition: Background, status, and issues for Congress. *CRS Report*, pp. 1–19 (2015).
17. Sood, S.: An improved and secure smart card based dynamic identity authentication protocol. *International Journal of Network Security* 14, 39–46 (2012).
18. Barker, E.: Guideline for using cryptographic standards in the federal government: Cryptographic mechanisms. *NIST Special Publication* 8 (2020).

19. Alleyne, N.: From Paperless to Plasticless: EMV Card Security and the Future of Payments in the USA. ProQuest, Utica College, pp. 1–78 (2016).
20. Hartoneva, M.: Contactless Payments with Inherence: Strong Customer Authentication and Biometrics. Master's Thesis, Haaga-Helia University of Applied Sciences, Information Systems Management, pp. 1–77 (2020).
21. Smart Card Alliance: Smart Cards and Biometrics, pp. 1–26 (2011).
22. Kithinji, A.: EMV Chip Cards and Operational Response to Payment Card Fraud by Commercial Banks in Kenya. Dissertation, University of Nairobi, pp. 1–54 (2016).
23. Ait Said, M., Hajami, A.: Zero trust security for card-not-present transactions: Extending EMV-like continuous authentication and adaptive risk validation across payment networks. *Journal of Theoretical and Applied* 103, 3110–3123 (2025).
24. Asmar, M., Tuqan, A.: Integrating machine learning for sustaining cybersecurity in digital banks. *Heliyon* 10, e37571, 1–18 (2024).
25. Dhameja, S., Jacob, K.: Clarifying liability for twenty-first-century payment fraud. *Economic Perspectives*, Federal Reserve Bank of Chicago, 107–129 (2013).
26. Scanio, S., Glasgow, J.: Payment card fraud, data breaches, and emerging payment technologies. *Fidelity Law Journal*, 59–94 (2015).
27. Cerrudo, C., Fayó, E.: Hacking databases for owning your data. In: *Black Hat Conference Proceedings*, pp. 1–30. Argeniss Information Security (2007).
28. Tanti, R.: Phishing attack: A case study and their prevention techniques. *International Journal of Scientific Research in Engineering and Management* 6, 1–43 (2024).
29. French Court of Cassation, Commercial Chamber: Decision No. 15-18.102. Published in the *Bulletin. France* (2017).
30. Anugraha, F., Febriani, H.: Bank customer protection law from skimming crimes: According to the consumer law and the banking law. In: *Proceedings of the International Conference on Restructuring and Transforming Law* 2, pp. 543–548 (2023).
31. Legifrance: Article L133-23 of the French Monetary and Financial Code, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000020861573, last accessed 2025/07/08.
32. Agrawal, A., Agrawal, S.: Cyber crime in banking sector. *Udgam Vigyati* 3, 1–19 (2016).
33. Ramazonov, I.: The role of civil liability in shaping bank cybersecurity standards: Analyzing judicial interpretation of “reasonable security measures”. In: *International Scientific Online Conference*, Poland, pp. 36–41 (2025).
34. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 6). Abu Dhabi (2020).
35. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Sections 6-2-2-6). Abu Dhabi (2020).
36. French Court of Cassation, Commercial Chamber: Decision No. 19-12.112. Published in the *Bulletin. France* (2020).
37. French Court of Cassation, Commercial Chamber: Decision No. 23-15.099. Published in the *Bulletin. France* (2024).
38. French Court of Cassation, Commercial Chamber: Decision No. 24-13.777. Published in the *Bulletin. France* (2025).
39. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 6-2). Abu Dhabi (2020).
40. Paris Court of Appeal: Division 4 – Chamber 9, Case No. 20/08109. Paris (2022).
41. Sawant, S., Ghodke, S., Ghuge, D., Ghodake, K., Ghodake, S., Ghuge, A., Ghuge, D.: Single smart card for identity and authentication using data analytics. In: *International Conference on Soft Computing: Theories and Applications*, pp. 117–127. Springer Nature, Singapore (2023).

42. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 6-2-1). Abu Dhabi (2020).
43. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 6-2-2-5). Abu Dhabi (2020).
44. UAE Federal Decree-Law No. 14. United Arab Emirates (2018).
45. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 5-1-2-7). Abu Dhabi (2020).
46. Central Bank of the UAE: Consumer Protection Regulation: Protection of Consumer Data and Assets (Circular No. 8/2020, Section 6-2-10-1). Abu Dhabi (2020).
47. Jabbara, N.: The theory of risk and its impact on civil liability. In: National Symposium on the Future of Civil Liability (2020). (In Arabic)
48. Alhajeri, M.: The risk concept on modern tort map: An analytical approach to English law. *Journal of Law, Kuwait University* 43 (2001).
49. McCarthy, D.: Liability and risk. *Philosophy & Public Affairs* 25, 238–262 (1996).
50. Zita, A.: The historical and legislative development of civil liability. In: *Study Day: Modern Trends in the Theory of Civil Liability*, p. 92. University of Adrar, Algeria (2013). (In Arabic)
51. Koussem, Y., Farah, S.: The theory of risk and its impact on fault as a basis for tort liability. *ASJP* 7, 1189–1200 (2022). (In Arabic)
52. Abdel-Maqoud, M.: Objective liability in terms of foundation and application. *Journal of Economic and Legal Studies*, Sadat City University, 1–33 (2021). (In Arabic)
53. Pretorious, J.: Negligence of a bank customer, and its liability for the wrongdoing of its employees. *Juta's Business Law Journal* (2002).
54. French Monetary and Financial Code: Article L133-16, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035430501, last accessed 2025/07/08.
55. Belin, B.: Question from Mr. Belin Bruno (The Republicans – R). Response from the Ministry of Economy, Finance and Industrial and Digital Sovereignty, p. 87 (2023).
56. Saghir, W., Kaferanis, D.: The applicable law on digital fraud. In: *Finance, Law, and the Crisis of COVID-19: An Interdisciplinary Perspective*. Springer International Publishing (2022).
57. French Monetary and Financial Code: Article L133-24, https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000035430562, last accessed 2025/07/08.
58. Douglass, D.: An examination of the fraud liability shift in consumer card-based payment systems. *Economic Perspectives*, 43–49 (2009).
59. Hayashi, F., Markiewicz, Z.: The initial effects of EMV migration on chargebacks in the United States. *Federal Reserve Bank of Kansas City Working Paper*, 1–53 (2018).
60. French Court of Cassation: Decision No. 1327 (16-11.644). France (2017).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.

