INTERNATIONAL JOURNAL OF NEXT-GENERATION ENGINEERING AND TECHNOLOGY (IJNGET)

eISSN: 3087-4319

Volume. 03, Issue. 02, pp. 14-20, February 2026"

Cybersecurity in Networks Supporting Card Payment Systems

Aghasi Gevorgyan
Head of Network Infrastructure, Armenian Card CJSC

Article Received: 01/04/2026, Article Accepted: 02/21/2026, Article Published: 02/24/2026
DOI: https://doi.org/10.55640/ijnget-v03i02-03

ABSTRACT

The article examines cybersecurity in networks supporting card payment systems, which serve as a distributed critical infrastructure characterized by high transaction volumes, dense data concentration, and escalating cyber threats. The study aims to conceptualize the payment card environment not merely as a set of isolated components, but as interdependent domains of trust through which a single transaction simultaneously traverses terminals, gateways, processors, schemes, and issuing and acquiring banks. The relevance is grounded in the structural dominance of card payments in retail and remote commerce, the documented growth of ransomware, data exfiltration, and DDoS campaigns against financial institutions, as well as the tightening regulatory focus on cardholder data protection and operational resilience. The novelty of the work lies in its tri-layered analytical design, which combines the architectural decomposition of the payment chain, a normative–taxonomic reading of PCI DSS concepts related to cardholder data, sensitive authentication data, and controlled environments, and a threat-oriented mapping of prevalent attack classes onto this architecture. This perspective enables the authors to demonstrate that excessive network connectivity and poorly defined trust boundaries simultaneously expand the formal scope of compliance and increase the number of lateral movement paths for attackers. The main conclusions emphasize the necessity of multi-layer, mutually constraining security controls, strict access and privilege management, cryptographic governance, environmental minimization, zero–trust–oriented segmentation, and response capabilities, where time to detection and recovery becomes the decisive parameter. The article will be particularly useful for payment system architects, banking cybersecurity practitioners, regulators, and researchers in the field of financial infrastructure resilience.

KEYWORDS

cybersecurity, cardholder data environment, data breaches, payment card systems

Introduction

Payment card systems have become the foundational means of exchange for everyday transactions among households, businesses, and the state. They serve mass purchases, remote commerce, subscriptions, service payments, and interbank settlements, linking merchants, banks, processing centers, and digital channels into a unified network. The scale of such operations is clearly illustrated by the euro area: in the first half of 2024, the total number of cashless transactions reached 72.1 billion, with card payments accounting for 56% of all transactions. Their count amounted to 40.1 billion, with a total value of approximately 1.5 trillion euros. Contactless transactions increased to 25.8 billion, underscoring the economy's accelerating dependence on the stable functioning of card infrastructure (European Central Bank, 2025).

The economic role of card payments is not exhausted by convenience: they reduce exchange friction (time, costs, access barriers), support the growth of e-commerce, and provide financial institutions with a governed environment for risk control, compliance, and analytics, thereby turning the payment circuit into a meaningful component of banking revenue and competitiveness. According to a global payment review, as early as 2023,

the industry processed around 3.4 trillion transactions totaling roughly 1.8 quadrillion dollars, forming a revenue pool of about 2.4 trillion dollars; this renders payment networks not an auxiliary service but an autonomous economic system upon which the resilience of commerce and consumer trust depend (Bruno et al., 2024).

This concentration of turnover and data explains why payment networks become a priority target for attacks: compromise of even a limited segment of infrastructure may yield either direct monetization through fraudulent operations and leaks, or coercive leverage through service disruption and extortion. The financial sector is characterized by a high density of cyber risk. A study on cybercrime risks notes that the financial industry occupies one of the leading positions in terms of attack share (estimated at 22.4% among industries in the cited statistics) and also bears substantial incident costs (Kuzior et al., 2022). Additional emphasis is imposed by the dynamics of extortion campaigns: according to a governmental trend analysis, for the period 2022–2024, more than 2.1 billion dollars in ransomware-related payments were recorded in reporting linked to bank oversight requirements, with a significant portion of incidents and payments attributable to financial organizations (FinCEN, 2025).

Materials and Methodology

The research materials were formed as a compact body of complementary sources reflecting both the macro-level functioning of card payment networks and the thin points of their cyber resilience: statistics on the structure and intensity of cashless transactions in the euro area were used to substantiate infrastructure criticality and the magnitude of potential damage (European Central Bank, 2025); global industry estimates were used to contextualize payment networks as an autonomous economic system with high concentrations of turnover and data (Bruno et al., 2024); and materials on cybercrime and ransomware were used to anchor threats in the observed dynamics of attacks and the adversary's financial motivation (Kuzior et al., 2022; FinCEN, 2025).

Methodologically, the work relied on a three-contour analytical design: (1) an architectural–functional decomposition of a card transaction and of trust domains, with identification of nodes where security becomes a systemic property of the network (terminal/POS, gateways, processing, issuer/acquirer, clearing) (Geçer & Akgiray, 2025); (2) a normative–taxonomic analysis of data and controlled-environment boundaries, where the distinction between cardholder data and sensitive authentication data and the prohibition on storing the latter after authorization were employed as formal criteria for defining the protection scope and for assessing the effect of excessive connectivity on attack surface and compliance cost (PCI, 2024); (3) a threat-oriented alignment of attack classes and their scaling mechanisms (ransomware/double extortion, leaks, DDoS, phishing), considering empirical evidence from the financial sector and the behavioral speed of compromise via social engineering (Theocharidou et al., 2024; FS-ISAC, 2024; Naqvi et al., 2023), as well as the protocol layer, where vulnerability may arise not from a defect but from a mismatch between implementation assumptions and the logic of the standard (Lan et al., 2023).

Results and Discussion

The shift from cash to cashless payments has transformed card transactions into a distributed infrastructure, where one operation simultaneously spans multiple trust domains: the merchant side, payment intermediaries, the acquiring bank, the payment scheme, and the issuing bank. A typical flow runs through a terminal or software cash register and acceptance channel (including e-commerce), then a gateway and processing/routing per scheme rules, issuer authorization, and finally clearing and settlement (Geçer & Akgiray, 2025). Importantly, these participants don't just forward messages: each node adds validation, constraints, anti-fraud controls, and logging, while consumer wallets and mobile apps reshape the front end via tokenization and device binding without changing the overall transaction life-cycle logic (Geçer & Akgiray, 2025).

Because processing is inherently multi-layered, merchant/app interfaces on top, transport and message transformation below, then authorization and fraud controls, alongside parallel clearing/reconciliation/settlement circuits, security cannot be added in only one place. Terminals and mobile devices are the primary attack surface; gateways and APIs become scalable mass-access points; and inside banks/processors, segmentation, privilege management, and fault tolerance are decisive. Complexity is further increased by strict protocols and rules governing card operations (e.g., chip standards), where implementation mistakes or misunderstandings of protocol assumptions can create real vulnerabilities, even when systems appear formally compliant (Lan et al., 2023).

Risk concentrates around flows of account and personal data whose value emerges when pieces are combined, and industry standards distinguish cardholder data from sensitive authentication data: the former includes PAN, cardholder name, expiration date, and service code; the latter includes full track data (or chip equivalents), CVC/CVV, and PIN-related values (PCI, 2024). Storing sensitive authentication data after authorization is prohibited, even if encrypted, and the presence of a PAN typically signals a controlled cardholder data environment (CDE) with strict protection requirements and shared responsibility implications under outsourcing (PCI, 2024). From 2022–2024, observed threats align with monetization (ransomware plus exfiltration and multi-channel extortion) and service disruption (DDoS), with sector analyses documenting ransomware and data-related threats across hundreds of European incidents, and noting that ransom demands under double extortion can reach millions of euros before negotiations reduce them (Theocharidou et al., 2024); DDoS activity against financial firms also surged sharply between 2022 and 2023, with geopolitical drivers raising the likelihood of repeated waves (FS-ISAC, 2024), while phishing and the human factor remain persistent initial-access channels, motivating sustained training plus technical safeguards that absorb user error (Naqvi et al., 2023). The main Financial Sector Cyberthreats are shown in Figure 1.

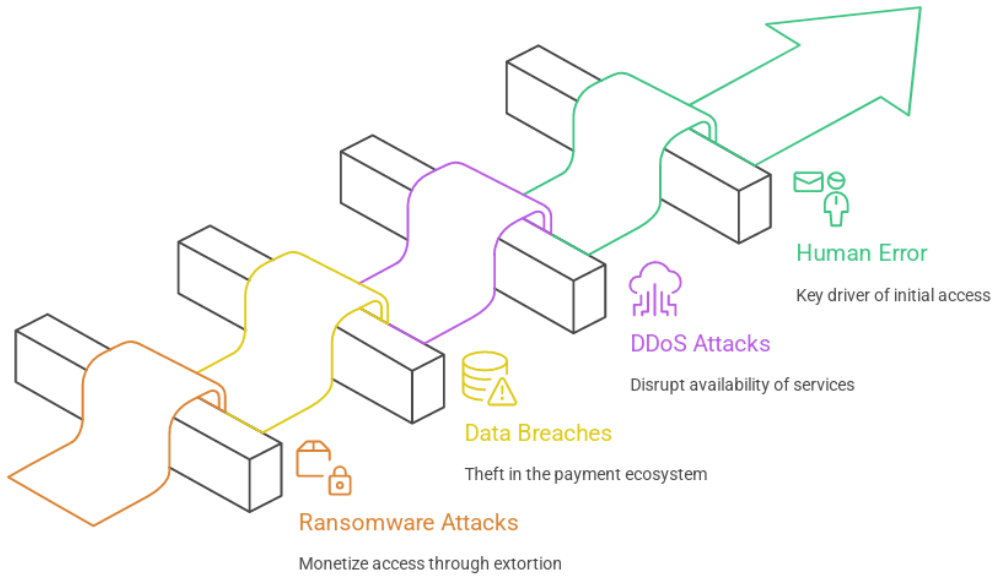

Fig. 1. Financial Sector Cyberthreats

Vulnerabilities in networks servicing card payments rarely exist in isolation: they manifest as a consequence of high ecosystem connectivity, blurred trust boundaries, and the constant need to sustain availability. What in a conventional corporate network would be considered a local error rapidly acquires systemic scale in the payment circuit, because transactional services, merchant interfaces, mobile channels, and internal banking segments are linked by continuous message flows and data that are difficult to fully stop for repair. Therefore, vulnerability analysis should begin here, not with an individual defect, but with the question of how a defect becomes a pathway for cardholder data and control of processing.

At the application level, web application and API vulnerabilities are among the most damaging, because they constitute both the showcase of payment services and the most convenient entry point. Query injection enables not only the extraction of information from stores but also the covert alteration of business logic by substituting transaction parameters and bypassing checks presumed at the application layer. Cross-site scripting shifts risk to the user and operator: it is sufficient to replace page content or inject a script into the context of a trusted domain to hijack a session, compel the browser to perform unwanted actions, or obtain information sufficient for further compromise. File upload vulnerabilities are particularly dangerous when personal accounts, document exchange, support forms, and refund logs are involved: a validation error in file type and content can readily turn storage into a foothold for malicious code insertion.

Code execution and configuration errors typically become the bridge that connects a vulnerability on the

front to access inside the controlled cardholder data environment. Often, not a single critical defect, but a combination of weaknesses, is exploited: an exposed administrative interface, excessive privileges of a service account, misconfigured network rules, and secrets stored in a manner that makes them easily retrievable. Under high load and frequent changes, configuration errors become especially insidious: they do not appear as an attack until used as a ladder for privilege escalation and lateral movement, and by the time they are detected, the adversary may already be embedded in the infrastructure and have masked traces within the normal noise of transactions. The correspondence between typical vulnerabilities and baseline protection measures in the payment network is shown in Table 1.

Table 1. Correspondence between typical vulnerabilities and basic security measures in the payment network

Vulnerability / Attack Vector	Typical Exposure Point	Likely Impact	Baseline Mitigation Measure
Query Injection	Payment forms, point-of-sale (POS) interfaces, APIs	Data reading and tampering, business-logic bypass	Parameterized queries, strict input validation, account isolation
Cross-Site Scripting (XSS)	User portals, operator/admin panels, support pages	Session hijacking, action tampering	Input/output sanitization, security headers, script restrictions (e.g., CSP)
Insecure File Upload	Forms, document uploads, reports	Injection of malicious objects	Content validation, storage isolation, execution disabled
Misconfiguration	Cloud, containers, network rules, logs	Unauthorized access to data/services, privilege escalation	Hardened baseline configurations, change control, regular audits
Privilege Escalation	Application servers, identity/account directories	System takeover	Role separation, least privilege, monitoring/controls for privileged actions

Zero-day vulnerabilities and the problem of patch management are especially acute in payment environments due to the conflict between security and operational continuity. When a component cannot be stopped without noticeable service impact, the temptation emerges to postpone updating until a window that never arrives, and accumulated vulnerability becomes a long-term risk. Conversely, without disciplined testing and deployment, organizations develop dependence on legacy versions, where even previously fixed errors return in the form of incompatible libraries, incorrect builds, and outdated protocol settings. Therefore, patch management in payment networks should be treated as a continuous process in which asset inventory, criticality assessment, compatibility verification, and deployment planning are linked to real transaction flows rather than to calendar convenience.

Supplier attacks amplify ecosystem vulnerability by expanding the attack surface beyond an organization's own infrastructure. Payment services inevitably rely on external components: software libraries, cloud platforms,

integration gateways, message delivery services, analytics modules, and providers of terminal infrastructure. Supplier compromise may appear as a legitimate update, a correct integration, or an ordinary network exchange, which complicates detection and creates a cascading effect where one incident impacts multiple participants simultaneously. An additional

complexity lies in distributed responsibility: even under strict contractual requirements, real security is determined by development practices, change control, and key management at each participant in the chain.

Insider threats in payment networks have a dual nature: some cases involve malicious actions, but errors and bypasses that arise from operational pressure are equally significant. Privileged users, technical support personnel, administrators, and developers possess access that, in other contexts, would be considered exceptional. Yet, in payment environments, it often becomes a daily necessity. This creates a paradox: the higher the maturity of automation and monitoring, the more subtle abuses become, and the more the role of procedures, separation of duties, and action verifiability increases. Moreover, an insider threat rarely manifests as a single act. More often, it is a chain of small deviations that individually look acceptable, but together form a corridor to compromise.

Theft and leaks of cardholder data rely on a predictable adversary motivation: the most valuable targets are those that can be quickly monetized or used as keys to further access. Primary interest attaches to the primary account number and related details, enabling initiation of transactions in remote channels, as well as verification codes and authentication values that turn a string of digits into an operational fraud instrument. Personal data is no less important because it increases the credibility of social engineering and enables attacks on account recovery, duplicate issuance, and account takeover. In payment networks, situations are especially dangerous when data is spread across logs, reports, temporary files, and test environments, where access is easier than in the primary store.

The consequences of leaks are rarely limited to direct losses from fraudulent transactions, because the payment ecosystem is sensitive to trust and continuity. A leak leads to an increase in chargebacks and disputed transactions, overloads support services, raises the cost of fraud counteraction, and forces urgent changes to processes that were previously considered stable. Simultaneously, regulatory mechanisms are activated: audits, orders, restrictions on data processing, and notification obligations, which create additional costs and the risk of temporary service degradation. Reputational damage here is particularly nonlinear: customers may forgive a single technical malfunction, but loss of control over data is perceived as a trust defect, and trust in the payment sphere is restored slowly.

Typical compromise scenarios share a regularity: the attacker seeks to establish persistence at a point where data and control intersect. This may be a phishing message after which the adversary obtains access to an operator account and, through a privilege chain, reaches administration; it may be malware injection into a merchant web interface, where details are collected on the fly even before encryption; it may be a misconfigured storage or logging setup that turns service data into convenient loot. Variability of details does not negate the general logic: first, initial access is obtained; then persistent presence is ensured; after which one of two paths is selected, data theft or availability disruption, followed by extortion. The generalized compromise chain of the payment circuit and the attack breakpoints are shown in Figure 2.

Fig. 2. Generalized payment circuit compromise chain and attack breakpoints

A multi-layer defense of payment networks should be constructed as a system of mutual constraints, in which failure at one layer does not automatically lead to the capture of the entire circuit. At the access level, multi-factor authentication and a strict privilege model are pivotal, where administrative actions are separated from routine actions, and access is granted precisely to the extent and for the time required for the task. At the data level, mechanisms such as encryption on disk and key management are key to prevent both unauthorized

access and abuse, such as developer key logging or storage in a development environment. At the network and application levels, a good system must provide filtering and control to define the normal, API protection, intrusion detection, and event monitoring to detect

anomalies before they become incidents. Organizational measures do not replace technical ones, yet they provide shape and durability. Policies and procedures impose predictability of actions in both normal and crisis conditions, training reduces the success of social engineering, and penetration testing and exercises identify gaps between the intended and actual architecture. Risk management enables prioritization not by incident loudness but by probability and damage, and process maturity transforms security from a set of scattered tools into a governed practice. As a skeleton, industry and international requirements discipline handling of cardholder data, set minimum control levels, and create a shared language for interaction among banks, merchants, and suppliers.

Enhancing the resilience of payment networks logically continues the idea of a controlled cardholder data environment: the more precisely this environment is delineated and the more strictly its connections are limited, the smaller the attack surface and the easier verifiability becomes. Segmentation and the principle of least privilege should be supported by a zero-trust approach, under which security by virtue of being inside the network is not assumed and every request is evaluated in the context of user, device, and task. Supplier management should include integration control, update verifiability, and logging requirements to prevent the supply chain from becoming a hidden tunnel. Finally, incident response should be evaluated through measurable indicators linked to detection and recovery speed. In the payment domain, time is often what determines whether an attack remains an isolated incident or escalates into a prolonged crisis.

Conclusion

Payment card systems, as the transport of everyday value exchange, become a critical distributed infrastructure in which the scale of turnover and concentration of data render cyber resilience not a derivative of convenience but a condition of economic stability and trust. The growth of cashless operations and the dominance of card transactions in the settlement structure, combined with the enormous global volume of payments, creates an environment in which the compromise of even a limited segment can provide the adversary with either direct monetization through fraud and leaks or a lever of systemic pressure through service stoppage and extortion. At the same time, the architecture of the payment circuit, multi-node, multi-domain, and multi-layer, creates a complex geometry of risk: a single transaction passes through the merchant, gateways, and processing, payment scheme rules, issuer authorization, and clearing and settlement circuits, while each node is simultaneously a control mechanism and a potential point of error. In such an environment, security is not reducible to a strong perimeter: protocol assumptions, implementation imperfections, vulnerabilities of mass-access interfaces, and the human factor form a nonlinear dynamic in which a local defect can become a trajectory to cardholder data or to control of processing, and the observed 2022–2024 statistics on extortion, leaks, and DDoS only reinforce the regularity of attacks gravitating toward payment networks.

Accordingly, the scientifically grounded conclusion is that the object of protection in networks supporting card payments should be formulated through governable trust boundaries and the controlled cardholder data environment, rather than through a set of fragmented measures by components. The separation of cardholder data and sensitive authentication data, the prohibition on storing the latter after authorization, and the interpretation of the controlled environment as a set of components, people, and procedures (including systems that do not process data directly but have unrestricted connectivity) impose a strict logic: excessive connectivity expands the compliance scope while simultaneously multiplying lateral movement routes. In this context, application-layer vulnerabilities (injections, XSS, insecure file upload), configuration errors, and privilege escalation function not as a list of typical problems but as recurring mechanisms coupling the facade to critical segments. Therefore, the resilience of payment networks should be built as a mutually constraining multi-layer system, with strict access and privilege management, encryption and key governability, segmentation and zero-trust logic, control of supplier integrations, and measurable readiness for incident response, where the decisive parameter becomes time to detection and recovery.

References

1. Bruno, P., Jeenah, U., Gandhi, A., & Gancho, I. (2024, October 18). *Global payments in 2024: Simpler interfaces, complex reality*. McKinsey & Company. https://www.mckinsey.com/industries/financial-services/our-insights/global-payments-in-2024-simpler-interfaces-complex-reality

2. European Central Bank. (2025, January 30).

Payment Statistics: First Half of 2024. European Central Bank. https://www.ecb.europa.eu/press/stats/paysec/html/ecb.pis2024h1~5263055ced.en.html

3. FinCEN. (2025, December 4). *FinCEN Issues Financial Trend Analysis on Ransomware*. FinCEN. https://www.fincen.gov/news/news-releases/fincen-issues-financial-trend-analysis-ransomware

4. FS-ISAC. (2024). *DDoS Attacks on Financial Services Industry Up 154%, According to New FS-ISAC/Akamai Report*. FS-ISAC. https://www.fsisac.com/newsroom/pr-akamai-ddos-report-2024

5. Geçer, T., & Akgiray, V. (2025). Payment Card Systems. In *The Financial Technology Revolution* (pp. 63–89). Springer,Cham. https://doi.org/10.1007/978-3-031-92048-6_4

6. Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*, *15*(12), 613. https://doi.org/10.3390/jrfm15120613

7. Lan, X., Xu, J., Zhang, Z., Chen, X., & Luo, Y. (2023). A systematic security analysis of the EMV protocol. *Computer Standards & Interfaces*, *84*, 103700. https://doi.org/10.1016/j.csi.2022.103700

8. Naqvi, B., Perova, K., Farooq, A., Makhdoom, I., Oyedeji, S., & Porras, J. (2023). Mitigation Strategies against the Phishing Attacks: A Systematic Literature Review. *Computers & Security*, *132*. https://doi.org/10.1016/j.cose.2023.103387

9. PCI. (2024). *Payment Card Industry Data Security Standard Requirements and Testing Procedures Version 4.0.1*. PCI. https://www.middlebury.edu/sites/default/files/2025-01/PCI-DSS-v4_0_1.pdf

10. Theocharidou, M., Lella, I., Naydenov, R., & Malatras, A. (2024). *ENISA Threat Landscape for the finance sector*. European Union Agency for Cybersecurity (ENISA). https://doi.org/10.2824/5410466