# Risks, Losses and Challenges of Non-Compliance to Security Standards for Payment Infrastructure Systems

**A Report from NewNet Secure Transactions, Inc.**

NewNet SECURE TRANSACTIONS

STC SECURE TRANSACTION CLOUD

NEWNET WHITE PAPER

## Overview

Modern payment ecosystems depend on a foundation of trust, security, and regulatory alignment. When a payment processor, acquirer, or financial institution continues to operate systems that are outdated, unsupported, or non-compliant with established security standards, that foundation begins to erode. What initially appears to be a manageable technical debt quickly transforms into a systemic threat that touches every dimension of the business from compliance exposure and security vulnerabilities to financial losses, reputational collapse, and regulatory sanctions. This document explores the full scope of these risks and illustrates why modernization is no longer optional but essential for organizational survival.

## Compliance Risk

The first and most visible warning sign emerges in the form of PCI-DSS non-compliance notifications, which signal that the organization's systems no longer meet the baseline requirements for protecting cardholder data. These warnings are not merely advisory; they represent formal findings that place the organization under heightened scrutiny. As card networks tighten enforcement, the grace periods that once allowed companies to delay upgrades are rapidly disappearing. When these grace periods expire, the organization faces escalating consequences, beginning with monthly fines and culminating in the most severe outcome: the loss of processing privileges. Losing the ability to process card transactions is not a temporary inconvenience it is an operational shutdown that halts merchant acquiring, disrupts settlement flows, and effectively removes the organization from the payments ecosystem.

The compliance dimension is therefore not simply a matter of meeting audit checklists. It is a structural requirement for maintaining access to the global card networks and preserving the organization's license to operate. Every day spent running non-compliant systems increases the likelihood of forced intervention by networks, banks, or regulators, each of which has the authority to suspend or terminate processing rights.

## Security Risk

Beyond compliance, the security implications of outdated systems are profound. Legacy platforms that have gone two to three years without security patches accumulate vulnerabilities that attackers can exploit with ease. These systems often remain in production long after their vendors have declared them end-of-life, meaning no further patches, no security updates, and no remediation for newly discovered weaknesses. Meanwhile, detailed exploit information circulates openly, giving fraudsters a precise roadmap for attacking these environments.

Operating such systems is comparable to playing Russian roulette, where each passing day increases the probability of a catastrophic breach. Attackers specifically target outdated payment systems because they know the vulnerabilities are well-documented and unpatched. Once inside, they can extract cardholder data, manipulate transaction flows, or compromise cryptographic keys—each of which can trigger a full-scale security incident with far-reaching consequences.



## Financial Exposure

The financial impact of operating non-compliant systems is staggering. Card networks impose monthly fines that typically range from $5,000 to $100,000, depending on the severity and duration of non-compliance. If a breach occurs, the financial burden escalates dramatically. A mid-size processor can expect $3 to $5 million in breach remediation costs alone, covering forensic investigations, emergency patching, infrastructure rebuilds, and third-party consulting. Legal exposure compounds the damage. Lawsuits, settlements, and regulatory actions typically cost between $2 million and $10 million, depending on the scale of the breach and the jurisdictions involved.

Perhaps the most devastating financial impact comes from operational downtime. During incident response, processors often lose $100,000 to more than $1 million per day in lost transaction revenue, merchant attrition, and SLA penalties. For many organizations, the cumulative financial impact of a single breach can exceed $10 to $50 million, pushing even established companies into insolvency.

- Card network fines: $5K-$100K per month of non-compliance
- Breach remediation: $3-5M average for mid-size processor
- Customer notification costs: $500K-$2M
- Legal fees and settlements: $2-10M
- Card reissuance costs: $5-10 per card × number of compromised accounts
- Revenue loss during incident response: $100K-$1M+ per day

## Reputational Damage

While financial losses can be quantified, reputational damage is far more difficult to repair. Merchants tend to abandon processors immediately after a security incident, seeking safer alternatives to protect their own customers and brand. Banking partners, who must maintain strict regulatory compliance, may terminate relationships with processors that demonstrate systemic security failures.

The long-term brand impact can be devastating. Once trust is broken, it is exceedingly difficult to regain. Negative media coverage, social amplification, and industry scrutiny can permanently alter the organization’s standing. In extreme cases, executives may face personal liability, especially if investigations reveal that they knowingly operated insecure systems or ignored compliance warnings.

## Regulatory Penalties

Regulators worldwide have strengthened their enforcement posture, particularly in the wake of high-profile breaches. Under GDPR, organizations that mishandle personal data—including payment information—can face penalties of up to 4% of global annual revenue. Banking regulators may impose additional fines, mandate remediation programs, or place the organization under enhanced supervision.

In the most severe cases, regulators may revoke the organization's banking or payment institution license, effectively ending its ability to operate in the financial sector. When combined with the direct financial losses, legal exposure, and reputational harm, a single successful fraud attack can result in $10 to $50 million in total damages, making it one of the most destructive events a payment organization can experience.

## NewNet Solutions for Banks, Acquirers, Processors, PSPs, FinTechs with full Conformance to PCI DSS Standards

When choosing payment infrastructure solutions, it becomes very crucial to select vendors with proven reputation in terms of security standards meeting the global requirements and including local requirements like NewNet Secure Transactions which ensures that the payment systems have the security standards certification for the best-in-class operations.

NewNet ensures that the security and integrity of payment transactions are paramount to protecting the entire payment ecosystem including payment service providers, merchants, Banks, and consumers.

- Payment technology systems operated with the Acquirers, Processors, Banks etc. must have strict conformance with the PCI DSS 4.0.x compliance standards like the NewNet solutions of AG1000, STG, STC etc.
- NewNet solutions have the implementation of TLS 1.3 and utilize the state of the hardware & software solutions which are most current.
- The NewNet solutions are most modern and offer protection for the customers with robust roadmaps and continued support and upgrade capabilities with latest security patches & software features.
- NewNet solutions employ the latest Operating Systems, ensuring sustainability and resilience against evolving cyber threats.

By following these security best practices that NewNet mandatorily conforms to, organizations can safeguard payment transactions, minimize financial risks, and maintain trust in the digital payment ecosystem.

NEWNET WHITE PAPER

## About NewNet Secure Transactions, Inc.

NewNet Secure Transactions Inc. offers Digital Payment Infrastructure solutions for aggregation & acquiring payments with intelligent routing, switching, secure transport functions, and Cloud transformation, standards compliant Modernization for full spectrum of entities in the payment ecosystem. NewNet solutions provide integrated capabilities for Payment Transaction Routing, Secure Network Access, Real Time Payments, Payment Data Security, Transaction Analytics, AI Augmentation etc.. by smart utilization of flexible APIs enabling Omnichannel, Multimode, Integrated payments.

NewNet Secure Transaction delivers reliable and scalable solutions to Acquirers, Processors, Banks, PSPs, Payment Gateways, PayFacs, MNOs, NSPs, FinTechs, CSPs as well as Telco, Retail, ISV, GigEconomy, Hospitality Enterprises for Real Time Payments, A2A/P2P Payments, Aggregation, Acquiring, Processing of Payments, and Emerging Payments in the areas of Open Banking, CBDC etc.. in all geographic regions globally.

For further information, visit
www.newnet.com
or email
traxcominfo@newnet.com

NewNet SECURE TRANSACTIONS

STC SECURE TRANSACTION CLOUD