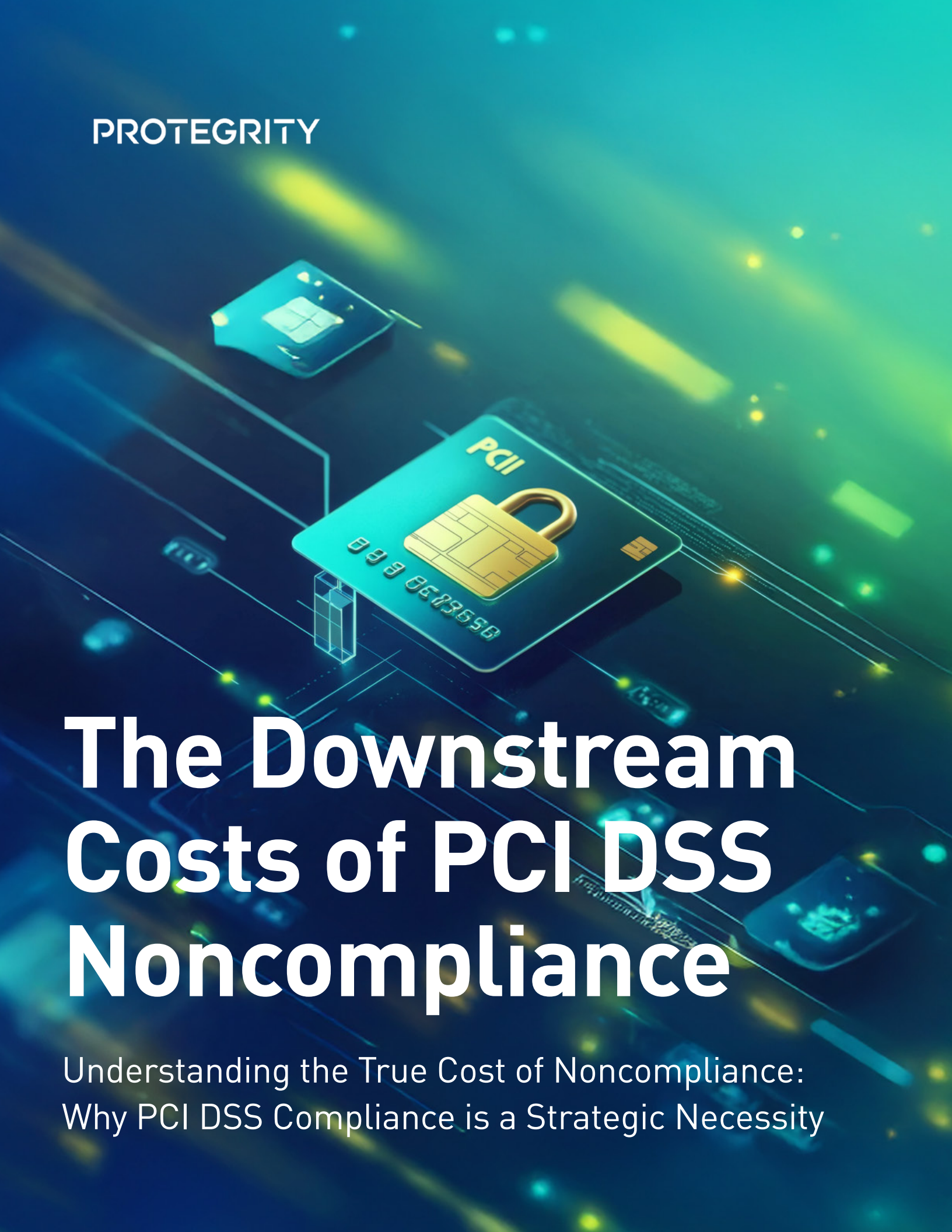
PROTEGRITY



The Downstream Costs of PCI DSS Noncompliance

Understanding the True Cost of Noncompliance: Why PCI DSS Compliance is a Strategic Necessity

INTRODUCTION

As digital transactions grow in complexity and volume, the need for secure payment processing has never been greater. The Payment Card Industry Data Security Standard (PCI DSS) was designed to mitigate the risks associated with handling sensitive cardholder data. Yet, as PCI DSS requirements evolve and expand — and as the volume and complexity of in-scope data grows within most organizations — the costs of PCI compliance threaten to overwhelm many organizations from both a financial and operational perspective.

Moreover, the skyrocketing costs of achieving full PCI compliance present a temptation to gamble on non-compliance — hoping to avoid penalties and betting that any non-compliance fines will remain far lower than the alternative costs of compliance.

But the costs of PCI DSS non-compliance extend far beyond the immediate monetary fines. This white paper explores these broader, often hidden costs of PCI DSS non-compliance, including significant downstream consequences like operational disruption, lost customer trust, remediation costs, and potential legal action. With PCI DSS v4.0 introducing steeper penalties and additional requirements, the cost-benefit analysis for non-compliance may be shifting for many organizations.

Why Noncompliance is a Costly Gamble

The Immediate Financial Impact

Non-compliance with PCI DSS can quickly lead to costly fines and penalties. Payment card networks can impose fines ranging from thousands to millions of dollars based on the number of records compromised or the duration of non-compliance.

For example, credit card companies can fine merchants between $50 and $90 per set of stolen financial data, even for those initially certified as PCI-compliant.[1] These penalties often increase with repeated infractions and vary significantly depending on the organization's size and transaction volume.

With the introduction of PCI DSS v4.0, penalties are set to increase as compliance requirements become more rigorous. Fines are just the beginning; the broader consequences of non-compliance often extend far beyond initial penalties.

The Looming Threat of Data Breach

While organizations may maintain a strong security posture outside of PCI DSS requirements, opting out of PCI DSS compliance typically means opting for a lower level of data protection for an organization's most sensitive and at-risk data.

This is a tremendous gamble given the now near-inevitability of data breaches. Case in point: While security spending has increased by 14% year over year, data compromises have surged by a staggering 78% in the same period.[2] As Eva Velasquez, CEO of the Identity Theft Resource Center, highlighted, "The sheer scale of the 2023 data compromises is overwhelming. Just the increase from the past record high to 2023's number is larger than the annual number of events from 2005 until 2020 (except for 2017)."[3]

And given the rising cost of breaches, a single data breach can quickly erase any theoretical savings from voluntary non-compliance. A study by IBM Security reported that the average cost of a data breach in 2024 reached $4.88 million, marking a 10% increase from the previous year.4 For financial services organizations, this figure can be even higher due to the sensitive nature of customer data and the extensive regulatory requirements they face.

In cases of non-compliance, these costs are compounded by fines, legal fees, and operational disruptions, turning what may seem like a short-term savings strategy into a substantial financial burden.

Hidden and Downstream Costs of Noncompliance

While immediate fines and breach costs are a more obvious consideration, the hidden costs of non-compliance can be just as damaging, if not more so. Yet, organizations frequently overlook these downstream costs when considering non-compliance as a cost-saving measure.

1. **Operational Disruption**
   Non-compliance can lead to operational disruptions that impede a company's ability to serve customers effectively. Following a breach, businesses are often required to halt operations temporarily to conduct forensic investigations, address vulnerabilities, and implement corrective measures. For financial institutions, these disruptions can translate into severe loss of productivity, directly impacting revenue.

   According to a recent Forbes Technology Council article, network downtime can cost large organizations an average of $9,000 per minute, with higher-risk enterprises in industries like finance and healthcare facing potential losses of up to $5 million per hour.5 These disruptions not only drain resources but also divert attention from strategic initiatives, significantly impacting long-term business growth and resilience.

2. **Remediation Costs**
   Once an organization experiences a data breach due to a security compromise or non-compliance, remediation costs begin to accrue. These costs include system upgrades, enhanced security measures, and new compliance audits to prevent recurrence. For many businesses, the process of implementing these retroactive measures far exceeds the costs of proactively maintaining PCI compliance.

   Additionally, remediation often involves hiring third-party cybersecurity experts, conducting security training for employees, and investing in new technologies. These unplanned expenses can strain resources and delay other essential projects.

3. **Reputational Damage and Loss of Customer Trust**
   A data breach resulting from PCI DSS non-compliance can have a lasting impact on customer trust and brand reputation. Financial institutions and commercial businesses alike rely heavily on trust to retain their customers. A 2023 PwC report indicated that 85% of consumers would stop doing business with a company after a data breach involving sensitive information. Rebuilding this trust is not only challenging but also costly. Organizations must invest in public relations efforts, customer support, and, in some cases, financial restitution to affected customers.

4. **Legal and Regulatory Consequences**
   Non-compliance with PCI DSS can lead to significant legal and regulatory repercussions. In addition to fines from payment processors, organizations may face lawsuits from affected customers or class-action cases for negligence. Regulators may also impose additional penalties, especially if non-compliance is seen as a willful neglect of required security standards.

   Legal expenses, settlements, and regulatory fines can accumulate quickly, representing a severe financial strain on an organization's resources. The ongoing costs of legal counsel, potential settlements, and prolonged litigation can surpass the cost of initial compliance by a wide margin.

5. **Higher Insurance Premiums and Increased Compliance Costs**
   After experiencing a breach due to PCI DSS non-compliance, companies often face higher insurance premiums and may risk being dropped by their cyber-insurance provider. Insurers view non-compliant businesses as higher-risk entities and adjust their rates accordingly. Additionally, non-compliance may result in increased audit and compliance costs, as regulators may subject these businesses to more frequent and rigorous scrutiny.

   These added expenses compound the financial strain on non-compliant organizations, reducing their long-term financial viability and detracting from growth initiatives.

The Case for Proactive Compliance

While some organizations may weigh the cost of PCI DSS compliance against non-compliance penalties, the long-term financial risks associated with non-compliance – and inadequate security of cardholder data – make a compelling case for more modern, proactive measures.

Moreover, compliance with PCI DSS does more than prevent fines; it establishes a security foundation that safeguards against costly data breaches and operational disruptions.

Reducing the PCI compliance burden: De-risking data to reduce PCI scope

Given the heavy lift of achieving PCI DSS compliance, organizations are actively looking for ways to reduce that compliance burden. Today, those efforts largely focus on finding ways to streamline processes — to do the same amount of work, but do it faster.

An emerging strategy offers a much simpler value proposition: do less work, smarter. Using advanced data-centric protection methods – including approved approaches to de-identify cardholder data such as tokenization – are far more efficient and practical. Leading organizations are de-risking the majority of their cardholder data and dramatically reducing the scope of their PCI compliance.

How Data Centric Security Reduces the Cost of PCI Compliance

Protegrity provides solutions designed to simplify and strengthen PCI compliance. By leveraging advanced de-identification techniques and privacy-enhancing technologies, Protegrity helps organizations reduce the scope of PCI audits and implement compliance cost-effectively. Protegrity's solutions are tailored to secure sensitive data without disrupting core operations or negatively impacting data utility, ensuring that businesses can maintain PCI compliance with minimal administrative burden and empower business innovation without fear of security, audit or compliance challenges.

How Protegrity Helps Mitigate Downstream Costs

1. **Reduced Audit Scope:** Through tokenization, format-preserving encryption, and other fit-for-purpose data protection methods, Protegrity minimizes the scope of systems and environments subject to PCI audits, cutting compliance costs significantly.

2. **Streamlined Data Protection:** Protegrity's data-centric security solutions that embed protection into the data itself ensure that sensitive data is secured at every stage — at-rest, in-transit, and in-use — reducing the risk of breaches and associated downstream costs.

3. **Flexible Compliance Solutions:** Protegrity enables a scalable, future-proof approach to compliance, allowing organizations to adapt as PCI standards – or other industry regulations or regional data privacy laws – evolve and as business needs change.

PCI DSS Compliance: A Strategic Investment, Not Just a Cost

As this white paper has demonstrated, the cost of non-compliance with PCI DSS extends far beyond immediate fines. Organizations face a complex web of downstream consequences, including operational disruptions, reputational damage, remediation expenses, and potential legal action. With the introduction of PCI DSS v4.0 and its more stringent requirements, expanded scope, and steeper penalties, the cost-benefit analysis of non-compliance is shifting dramatically.

Rather than viewing PCI DSS compliance as a burden, organizations should embrace it as a strategic investment in data security, business resilience, and competitive differentiation. By proactively implementing robust security measures and leveraging advanced technologies like tokenization, organizations can:

- **Minimize the Risk of Data Breaches:** Strengthen your security posture and protect sensitive cardholder data from unauthorized access.
- **Reduce Compliance Costs:** Streamline compliance efforts, reduce audit expenses, and avoid costly fines and penalties.
- **Enhance Operational Efficiency:** Improve payment processing, reduce manual effort, and enhance overall operational efficiency.
- **Empower Business Innovation:** Unblock cardholder data for analytics, AI, and Machine Learning.
- **Increase Data Utility:** Unlock real-time, internal data consumption and external data sharing.

Unlocking Business Value with Data-Centric Security

Protegrity's comprehensive suite of data protection solutions empower organizations to achieve and maintain PCI DSS compliance while maximizing the value of their data. Our solutions include:

- **Tokenization and Format-Preserving Encryption:** Replace sensitive cardholder data with non-sensitive tokens, reducing your PCI DSS scope and minimizing the risk of data breaches.
- **Data Discovery and Classification:** Identify and classify sensitive data to ensure appropriate protection measures are in place within cardholder data environments.
- **Access Control:** Implement robust access controls to restrict access to sensitive data and prevent unauthorized access.
- **Monitoring and Auditing:** Continuously monitor and audit your data security environment to ensure ongoing compliance.

READY TO DE-RISK YOUR DATA AND REDUCE YOUR PCI DSS SCOPE?

Visit www.protegrity.com/demo to see how fit-for-purpose data protection can transform your business.