PAYTIA NEXT-GENERATION PAYMENTS

The Ultimate Guide to PCI-DSS Compliance

PCI DSS Certified
LEVEL 1 SERVICE PROVIDER

1. WHAT IS PCI-DSS AND WHEN DOES IT APPLY TO YOUR BUSINESS?

What is PCI-DSS?

The Payment Card Industry Data Security Standard (PCI-DSS) is a set of security standards designed to ensure that ALL companies that accept, process, store or transmit credit card information maintain a secure environment.

When Does It Apply?

PCI-DSS applies to ANY business that:

- Accepts credit or debit card payments (online, in-person, or over the phone)
- Stores cardholder data (even temporarily)
- Transmits cardholder data across networks
- Processes card payments through third-party providers

This includes:

- E-commerce websites
- Retail stores
- Restaurants and hospitality
- Healthcare providers
- Professional services
- Non-profit organizations
- Call centers taking phone payments

Size doesn't matter - Whether you process 1 transaction or 1 million per year, PCI-DSS compliance is mandatory if you handle card data.

2. What Happens If Card Data is Compromised?

Under **PCI-DSS regulations**, businesses must **never store, process, or transmit cardholder data insecurely**. If a data breach occurs due to improper handling, the business—not the payment provider—bears full liability.

Financial and Compliance Risks

Failing to comply with PCI-DSS and GDPR regulations can result in:

- Hefty fines (ranging from £4,000 to £500,000 per violation, depending on severity).
- Reputational damage and loss of customer trust.
- Higher processing fees or merchant account termination by Visa, Mastercard, and other providers.
- Legal consequences, including lawsuits from affected customers.

> "**PCI-DSS APPLIES TO ALL MERCHANTS, PAYMENT GATEWAYS, PAYMENT PROCESSORS, AND SERVICE PROVIDERS THAT HANDLE PAYMENT CARD DATA, REGARDLESS OF THEIR SIZE OR TRANSACTION VOLUME.**"

3. Current PCI-DSS Version 4.0.1

Latest Standards

- Current Version: PCI-DSS 4.0.1 (released March 2022)
- Transition Period: Until March 2025 for full implementation
- Previous Version: 3.2.1 (still acceptable until March 2025)

> "MORE CHANGES THAN YOUR IT TEAM MIGHT HAVE EXPECTED"

Key Changes in Version 4.0.1

- Enhanced authentication requirements
- Stricter network segmentation standards
- Regular penetration testing mandatory
- Customized approach options for compliance
- Enhanced vulnerability management
- Updated encryption standards

Compliance Timeline

- Now - March 2025: Version 3.2.1 OR 4.0.1 acceptable
- After March 2025: Version 4.0.1 MANDATORY

4. Why a Fixed-Cost, PCI-Compliant Payment System Like Paytia Is the Smarter Choice

A system like Paytia eliminates these financial uncertainties by removing all card data from business people, processes, and systems for a fixed cost per year.

> **"FINANCE DIRECTORS CAN CUT COSTS, SIMPLIFY COMPLIANCE, AND PROTECT THE BUSINESS FROM FINANCIAL PENALTIES."**

✓ Predictable Budgeting – No unexpected compliance costs or fines.

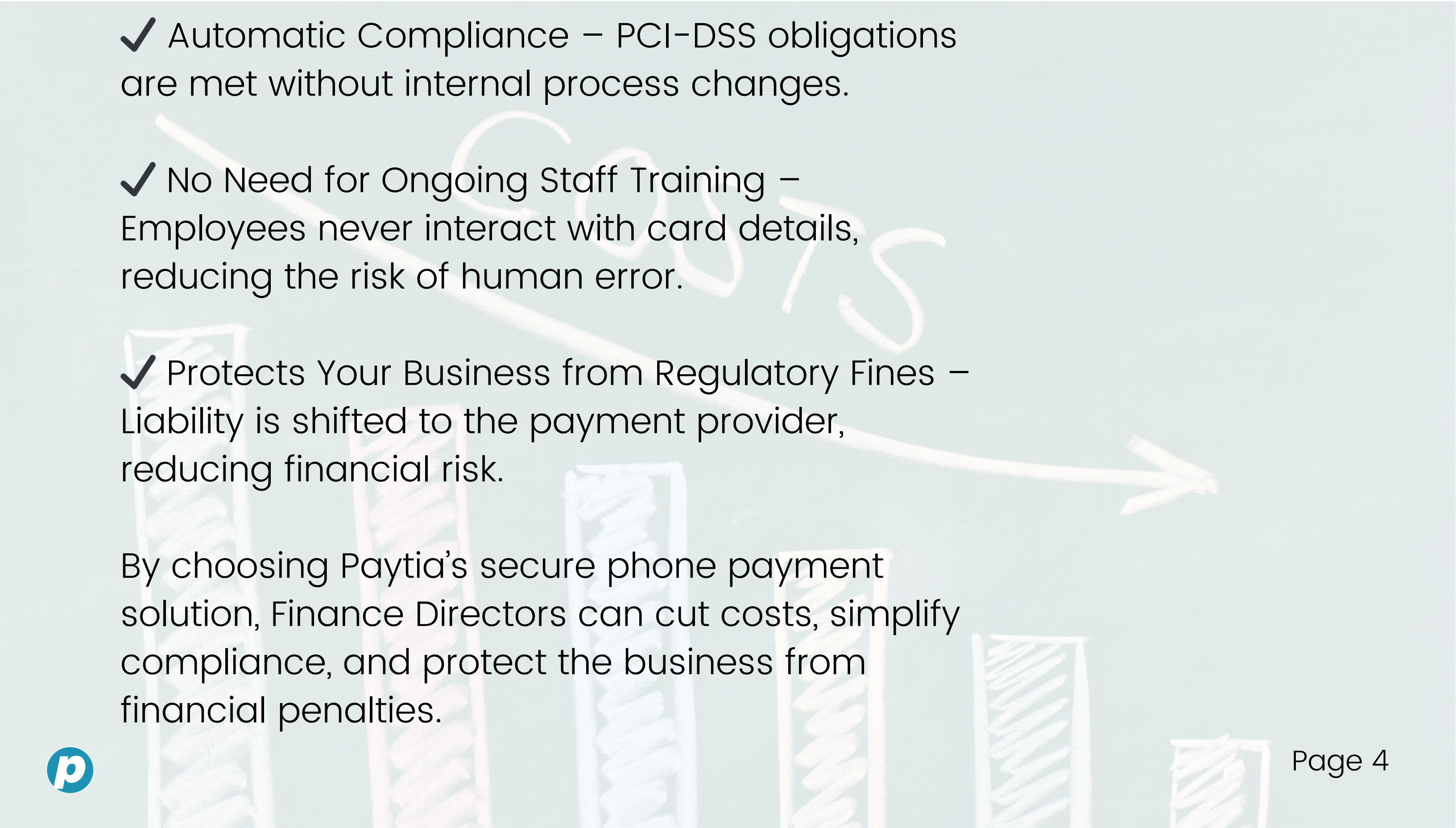
✓ Eliminates Security Risks – No need for manual data handling, audits, or compliance headaches.

✓ Automatic Compliance – PCI-DSS obligations are met without internal process changes.

✓ No Need for Ongoing Staff Training – Employees never interact with card details, reducing the risk of human error.

✓ Protects Your Business from Regulatory Fines – Liability is shifted to the payment provider, reducing financial risk.

By choosing Paytia's secure phone payment solution, Finance Directors can cut costs, simplify compliance, and protect the business from financial penalties.



5. PCI-DSS Myths That Could Land You in Hot Water

Myth 1: "We use a payment processor, so we're automatically compliant"

Reality: You're still responsible for your part of the payment process and must validate your compliance annually.

Myth 2: "Small businesses don't need to worry about PCI compliance"

Reality: ALL merchants accepting card payments must comply, regardless of size. Fines start at £5,000-£50,000 per incident.

Myth 3: "Our website is hosted by a third party, so they handle compliance"

Reality: You remain liable for any part of the payment process you control, including web forms and data handling.

Myth 4: "We don't record our calls so we are compliant"

Reality: Any people or hardware that hears, sees of touches card number and security codes is non-compliant until proved otherwise. The recordings are just another system you don't have to worry about in your PCI scope.

Myth 5: "We use a virtual terminal so the bank says we are PCI Compliant"

Reality: The Virtual terminal is compliant and transmits the card data to your bank/processor. Your business had the card data to type into the virtual terminal and so your staff and business systems are in scope and have to be proved to be compliant.

6. How Paytia Reduces PCI Compliance Costs and Risks

Businesses can eliminate the risks and extra stress payment security adds by NOT having access to payment card data at ALL. Paytia provides exactly that service. You can't be accused of losing information you never had.

> "WITH PAYTIA, BUSINESSES CAN CONTINUE TAKING SECURE PHONE PAYMENTS WITHOUT THE RISKS OF VERBAL CARD DATA EXPOSURE."

How Paytia Works

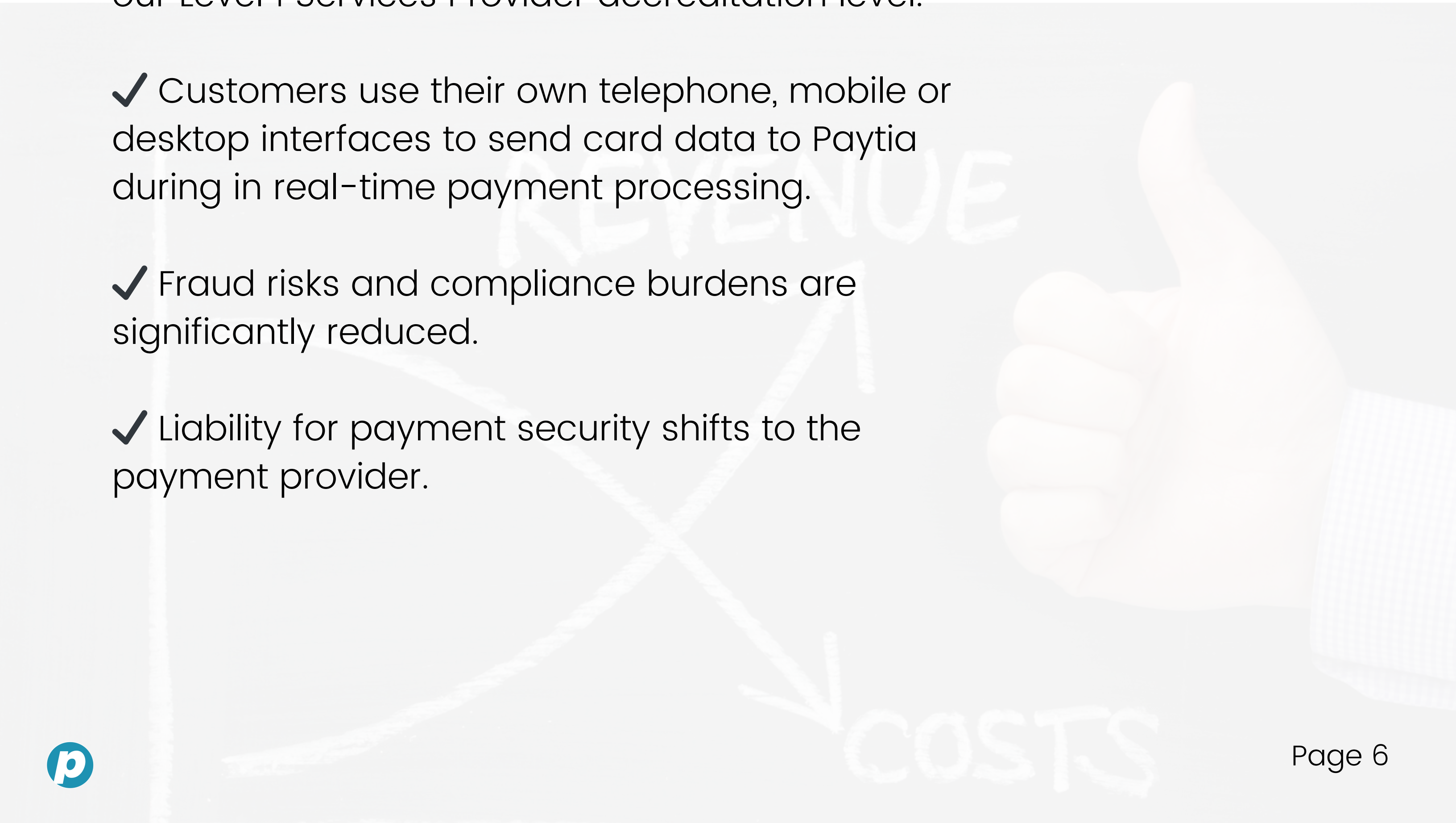
✓ Staff never see, hear, or store payment information.

✓ Payments are fully PCI-DSS compliant under our Level 1 Services Provider accreditation level.

✓ Customers use their own telephone, mobile or desktop interfaces to send card data to Paytia during in real-time payment processing.

✓ Fraud risks and compliance burdens are significantly reduced.

✓ Liability for payment security shifts to the payment provider.



7. Comparison: Handling Card Data vs. Secure Payment Processing

Scenario	Your Business Handles Card Data	Your Business Does Not Handle Card Data
PCI-DSS Compliance	Full compliance burden, including audits and security controls.	PCI-DSS scope reduced or eliminated.
Financial Liability	Liable for data breaches, fines, and fraud losses.	Liability shifts to the payment provider.
Security Risks	High risk of data leaks, fraud, and theft.	No risk, as card details are never seen or stored.
Legal Compliance	Must comply with PCI-DSS, GDPR, and financial data security laws.	Compliance burden is significantly reduced.
Reputation Impact	Loss of customer trust after a security breach.	Builds customer trust with a secure payment process.

8. Take Action: Reduce Costs & Secure Your Phone Payments Today

3 Steps to Protect Your Business

Assess your current payment process – Are you still asking customers to read out card details?

Review PCI-DSS compliance requirements – Are you meeting the latest security standards?

Implement a secure phone payment solution – Eliminate compliance risks with a secure keypad payment system like Paytia.

Don’t wait for a security breach to happen. Take action today to protect your business, your customers, and your reputation.

Let

paytia

take responsibility on behalf of your business for PCI-DSS

CONTACT US