



DEMO

First chapter only

The CISO's Guide to Agentic Commerce Risk

Risk Assessment Framework for AI Agents in Financial Transactions

The CISO's Guide to Agentic Commerce Risk

© 2026 Pragma Vision LLC. All rights reserved.

Trademark Notice

Google, Google Pay, Google Cloud, and Android are trademarks of Google LLC. Stripe is a trademark of Stripe, Inc. Cloudflare and Cloudflare Workers are trademarks of Cloudflare, Inc. Supabase is a trademark of Supabase, Inc. OpenAI and ChatGPT are trademarks of OpenAI, Inc. Claude is a trademark of Anthropic, PBC. W3C is a trademark of the World Wide Web Consortium. Visa is a trademark of Visa International Service Association. OWASP is a trademark of the OWASP Foundation. Midjourney is a trademark of Midjourney, Inc. Canva is a trademark of Canva Pty Ltd. Etsy is a trademark of Etsy, Inc. Amazon is a trademark of Amazon.com, Inc. All other trademarks are the property of their respective owners.

No Affiliation

This book is an independent publication. It is not authorized, sponsored, or endorsed by any of the companies or organizations whose products or services are mentioned herein.

No Professional Advice

The information in this book is provided for educational purposes only. It does not constitute legal, financial, investment, tax, or other professional advice. Readers should consult qualified professionals for guidance specific to their situation.

Code Examples

Code examples in this book are provided for illustration only. They may not be suitable for production use without additional validation, error handling, and security review.

Published by Pragma Vision LLC

First edition, 2026.

Contents

1	When AI Agents Handle Money	7
1.1	The New Attack Surface You Were Not Briefed On	8
1.2	About Pragma.Vision	9
1.3	What This Book Covers	10
2	The 3-Layer Protocol Security Model	12
2.1	Why One Protocol Is Never Enough	13
2.2	Layer 1: Identity (Visa TAP)	14
2.3	Layer 2: Authorization (Google AP2)	15
2.4	Layer 3: Execution (Stripe ACP + x402)	16
2.5	Hybrid Signature Architecture	17
2.6	Layer Interaction: A Complete Transaction Flow	19
3	21 Attack Vectors in Agentic Commerce	20
3.1	The Agentic Threat Landscape	21
3.2	Identity Layer Attacks (Vectors 1–7)	21
3.2.1	Vector 1: Agent Identity Spoofing	21
3.2.2	Vector 2: Credential Theft and Replay	22
3.2.3	Vector 3: Privilege Escalation Through Credential Manipulation	22
3.2.4	Vector 4: Orphaned Agent Exploitation	23
3.2.5	Vector 5: Supply Chain Agent Compromise	23
3.2.6	Vector 6: DID Resolution Poisoning	24
3.2.7	Vector 7: Trust Score Manipulation	24
3.3	Authorization Layer Attacks (Vectors 8–14)	24

3.3.1	Vector 8: Mandate Forgery	25
3.3.2	Vector 9: Mandate Scope Expansion	25
3.3.3	Vector 10: Nonce Reuse / Replay Attack	26
3.3.4	Vector 11: Prompt Injection for Financial Authorization	26
3.3.5	Vector 12: Memory Poisoning for Delayed Financial Exploitation . .	27
3.3.6	Vector 13: Consent Phishing	27
3.3.7	Vector 14: Cascading Authorization Failure	28
3.4	Execution Layer Attacks (Vectors 15–21)	28
3.4.1	Vector 15: Amount Tampering	28
3.4.2	Vector 16: Duplicate Charge Exploitation	29
3.4.3	Vector 17: Webhook Forgery	29
3.4.4	Vector 18: Commission Manipulation	30
3.4.5	Vector 19: Stablecoin Settlement Manipulation	30
3.4.6	Vector 20: Cross-System Data Exfiltration	30
3.4.7	Vector 21: Autonomous Spend Escalation	31
3.5	Attack Vector Summary Matrix	32
4	Risk Assessment Framework	34
4.1	Adapting NIST AI RMF for Financial Transactions	35
4.2	Risk Scoring Methodology	35
4.3	Risk Matrix: All 21 Vectors	36
4.4	Interpreting Residual Risk	38
4.5	Building Your Organization’s Risk Register	38
5	The Board Presentation: Communicating AI Agent Risk	40
5.1	Why the Board Cares Now	41
5.2	The Three-Slide Framework	42
5.2.1	Slide 1: The Exposure	42
5.2.2	Slide 2: The Three-Layer Defense	42
5.2.3	Slide 3: The Roadmap	43
5.3	Objection Handling	43

6	Compliance Mapping: SOC 2 Controls for AI Agents	45
6.1	SOC 2 Trust Services Criteria and Agentic Operations	46
6.2	CC1: Control Environment	47
6.3	CC2: Communication and Information	47
6.4	CC6: Logical and Physical Access Controls	48
6.5	CC7: System Operations	49
6.6	CC8: Change Management	50
6.7	PI1: Processing Integrity	50
7	Compliance Mapping: GDPR and PCI DSS Considerations	52
7.1	GDPR and AI Agent Data Processing	53
7.1.1	Lawful Basis for Agent Data Processing	53
7.1.2	Data Subject Rights in Agent Contexts	54
7.1.3	Data Protection Impact Assessment (DPIA)	55
7.1.4	International Data Transfers	55
7.2	PCI DSS 4.0 and AI Agent Payment Processing	56
7.2.1	Requirement 3: Protect Stored Account Data	56
7.2.2	Requirement 6: Develop and Maintain Secure Systems	56
7.2.3	Requirement 7: Restrict Access by Business Need	57
7.2.4	Requirement 8: Identify Users and Authenticate Access	57
7.2.5	Requirement 10: Log and Monitor All Access	57
7.2.6	Requirement 12: Organizational Policies	58
7.3	EU AI Act: The Coming Regulatory Layer	58
8	Incident Response for Agent-Related Breaches	60
8.1	Why Agent Incidents Are Different	61
8.2	The Agent Incident Response Lifecycle	62
8.2.1	Phase 1: Detection (Minutes, Not Days)	62
8.2.2	Phase 2: Containment (Automated, Not Manual)	63
8.2.3	Phase 3: Investigation	64
8.2.4	Phase 4: Eradication and Recovery	64

8.2.5	Phase 5: Post-Incident Review	65
8.3	Incident Severity Classification	66
8.4	Communication Templates	66
9	Building Your Agentic Commerce Security Program	68
9.1	The Four-Phase Maturity Model	69
9.1.1	Phase 1: Visibility (Months 1–3)	69
9.1.2	Phase 2: Identity Controls (Months 4–6)	70
9.1.3	Phase 3: Authorization and Execution Controls (Months 7–12)	71
9.1.4	Phase 4: Continuous Improvement (Months 12+)	72
9.2	Budget Estimation	73
9.3	Organizational Structure	73
9.4	Quick Wins: Actions You Can Take This Week	74
9.5	Closing Perspective	75
	What’s Next	76
	About Pragma.Vision	78

1

When AI Agents Handle Money

When AI Agents Handle Money



Figure 1. A comparison of traditional human-speed e-commerce (session keys lasting minutes) against machine-speed agentic commerce (keys persisting months to years, moving 16x more data)—where 13% of orgs had AI breaches, 97% lacked AI access controls, and shadow AI added \$670K to breach cost

1.1 The New Attack Surface You Were Not Briefed On

Your organization already has AI agents in production. Whether your security team deployed them, approved them, or even knows about them, autonomous software agents are making decisions, accessing data, and—increasingly—spending money on behalf of your employees and your customers. The question is no longer whether to allow AI agents into your financial operations. The question is how to manage the risk they have already introduced.

The numbers are stark. According to IBM's 2025 Cost of a Data Breach Report, 13% of organizations reported breaches involving AI models or applications—and of those, 97% lacked proper AI access controls. Shadow AI—unauthorized agent deployments outside IT governance—costs organizations an average of \$670,000 more per breach

than standard incidents. The global average breach cost stands at \$4.44 million, while US companies face an average of \$10.22 million per incident.

97%

of organizations breached through AI models lacked proper AI access controls¹

Meanwhile, agentic commerce is accelerating. Global digital commerce is projected to surpass \$11 trillion by 2026, with AI agents processing an increasing share of those transactions. Agents now negotiate vendor contracts, approve purchase requisitions, process expense reports, and execute financial trades. Each of these operations introduces attack vectors that traditional security frameworks were never designed to address.

Key Insight

The agentic commerce threat is fundamentally different from traditional cybersecurity threats. Agents operate autonomously, maintain persistent memory, chain actions across multiple systems, and move 16x more data than human users. A compromised agent does not just steal data—it actively transacts, and it does so at machine speed with machine-scale access.

1.2 About Pragma.Vision

This book draws from the security architecture of Pragma.Vision, an AI-native commerce ecosystem model spanning a growing family of interconnected platforms. The ecosystem uses a three-layer protocol security model—identity verification (Visa TAP), user authorization (Google AP2), and payment execution (Stripe ACP)—all secured with quantum-safe hybrid cryptography (ML-DSA-65). The 21 attack vectors cataloged in Chapter 3 come from penetration testing and security hardening patterns

¹IBM Security, *Cost of a Data Breach Report*, 2025.

across 306 test cases. The risk framework in Chapter 4 is derived from NIST AI RMF 1.0 principles adapted for financial transaction contexts.

1.3 What This Book Covers

This guide is structured for CISOs and security leaders who need to:

1. **Understand the threat model:** The three-layer protocol security model that separates identity, authorization, and execution concerns (Chapter 2).
2. **Catalog the attack surface:** 21 attack vectors specific to AI agents handling financial transactions, categorized by protocol layer (Chapter 3).
3. **Assess risk systematically:** A likelihood-by-impact risk matrix calibrated for agentic commerce, with quantified financial exposure estimates (Chapter 4).
4. **Communicate to the board:** A ready-to-present risk narrative that translates technical threats into business language (Chapter 5).
5. **Map to compliance frameworks:** SOC 2 Trust Services Criteria, GDPR data processing requirements, and PCI DSS 4.0 controls as they apply to AI agent operations (Chapters 6 and 7).
6. **Respond to incidents:** An agent-specific incident response playbook that accounts for autonomous behavior, persistent memory, and cross-system chaining (Chapter 8).
7. **Build a security program:** A phased roadmap for establishing agentic commerce governance within your organization (Chapter 9).

Every chapter ends with a concrete deliverable—a matrix, a checklist, a template, or a policy document—that you can adapt for your organization immediately.

Get the complete book — <https://shop.pragma.vision>

DEMO

This is a free preview of the full edition.

Get the complete book at:

<https://shop.pragma.vision>