PCI Security Standards Council®

2025 NORTH AMERICA COMMUNITY MEETING

2025 NORTH AMERICA COMMUNITY MEETING

The Double - Edged Sword:

AI Implications for Payment Fraud

Christine Jones

PCIP, CISSP, CISA

Assistant Managing Director

CASH & CREDIT MANAGEMENT

TEXAS TECH
Administration & Finance
Financial & Business Services

Preston DuBose

ISA

Director of Merchant Security & Services

Texas Tech University

- 5 Universities
- 41,000 Students
- 272 Merchant Accounts
- FY 2024 Transactions
  - 1,151,596 Transaction
  - $427 Million

Texas A&M University

- 20 universities & state agencies
- >160,000 Students
- 445 Merchant Accounts
- FY 2024 Transactions
  - 2,119,550 Card Transactions
  - $295 Million

Agenda

Positives

AI is revolutionizing payment security and fraud detection

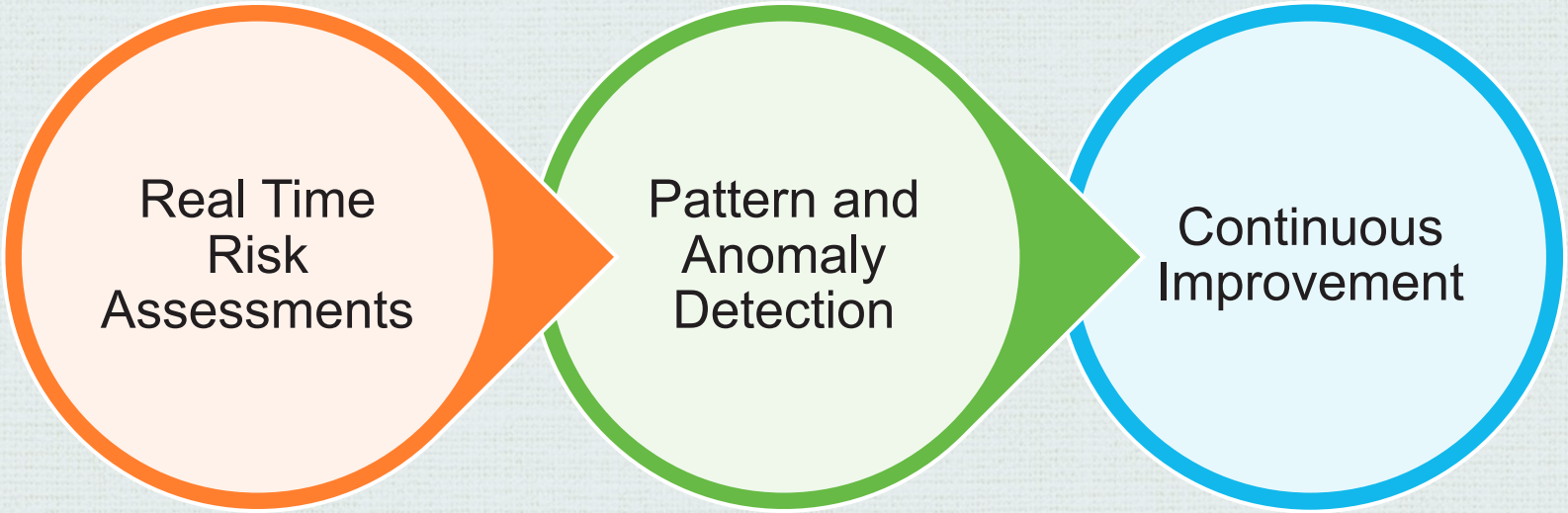
Dark Side

AI is also empowering criminals to exploit new vulnerabilities

Best Practices

Balance Technology with Education and Compliance

How Is AI Transforming Payment Security



Successes in AI-Driven Defense

Significant Reduction in Fraud and Chargebacks

Lower False Positives and Improved Accuracy

Increased Payment Conversion Rates

Global Fraud Risk Reduction

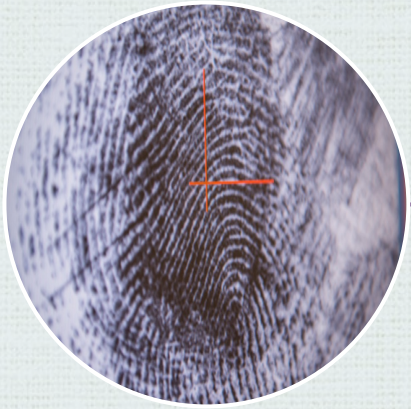
Advanced Behavioral Biometrics and Continuous Authentication

Efficient Integration with Existing Payment Infrastructure

Proactive Adaption to Emerging Threats

Future Trends in AI for Payment Security

- Frictionless
- Real-Time Payments at Scale
- Minimal Delays
- Higher level of Personalization

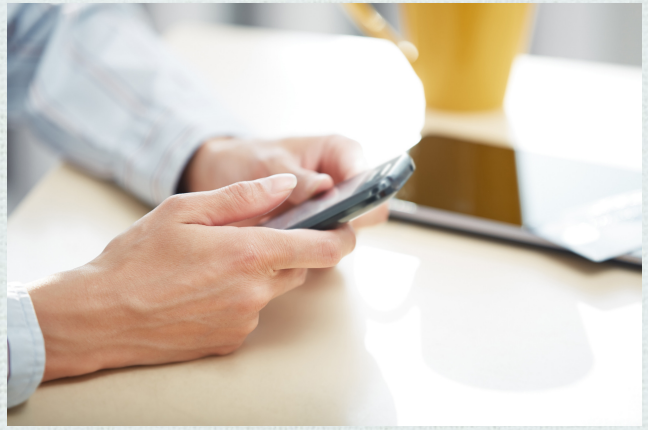


- AI-based threat intelligence

- Identify fake identities
- Prevent fake identities

The Dark Side – How Fraudsters Use AI

- DeepFake Identity Theft
- AI Phishing
- Bot-Driven Fraud



Challenges

False Positives
AI-Generated Synthetic Data Risks
High Implementation and Integration Costs
Rapidly Evolving Fraud Tactics\Risk of AI Manipulation and Evasion

Case Study

AI in DeepFake Attacks

Human Factor

Importance of Consumer Education

Ethical & Regulatory Challenges

Bias in AI Algorithms

- Bias and Fairness
- Transparency and Explainability
- Accountability and Human Oversight
- Privacy and Data Use
- Security Risks and Manipulation

Compliance with Regs

- Compliance with Evolving Laws
- Data Protection and Consent
- Auditability and Model Governance
- Ethical Use Mandates

Emerging Threats

Chatbots

- Automated bots can mimic human behavior and bypass CAPTCHAs

AI Connectors / Agents

- The more access AI agents are given, the greater the attack surface.

Social Engineering Evolution

- Phishing and spear phishing remain central attack methods
- Business Email Compromise (BEC)
- Social engineering in open banking
- Mass creation of synthetic identities

Best Practices for Organizations

Layered Security

Model Training

Regular Updates

Key Takeaways

AI is essential for modern payment security, but not foolproof

Vigilance, transparency, and adaptive strategies are crucial

Balance technology with education and compliance

Preston DuBose

ISA

Director of Merchant Security & Services

Christine Jones

PCIP, CISSP, CISA

Assistant Managing Director

CASH & CREDIT MANAGEMENT

TEXAS TECH
Administration & Finance
Financial & Business Services