ALTA inSIGHTS

REAL TIME | ON-DEMAND

Today's ALTA Insights Featured Sponsor

Today's Speakers

Shawn Fox

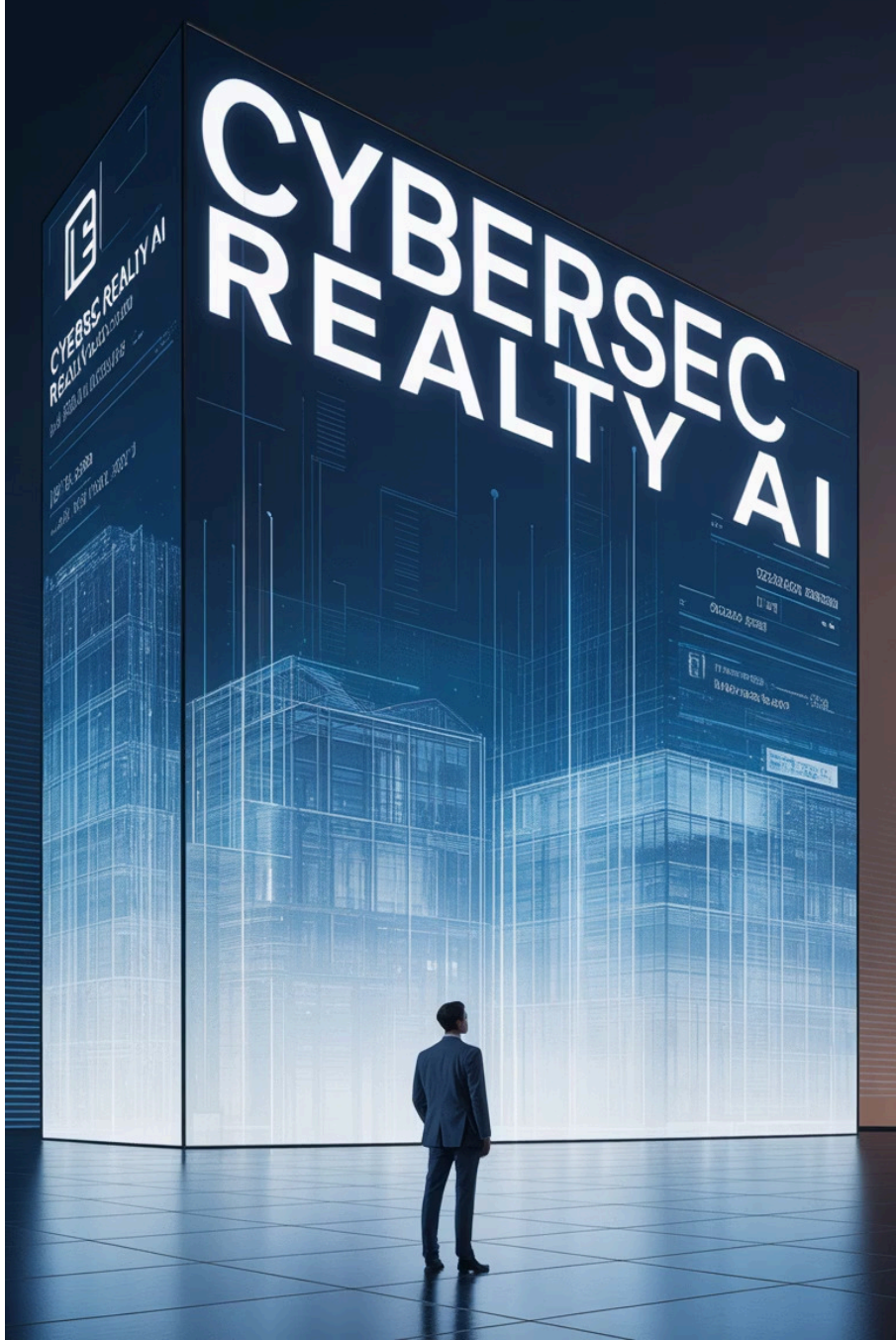
Premier One - Chief Revenue Officer

Jonathan Holfinger, Esq.

Northwest Title - CEO, Attorney, OLTP, NTP

The Dark Side of AI in Real Estate Transactions

Protecting Title Companies and Lenders from AI-Enhanced Fraud



Why Talk About This Now?

AI Adoption Exploding

500-500 Million active users daily. Every industry is racing to implement AI solutions.

Title & Banking Targeted

High-value transactions and sensitive data make our industries prime targets for sophisticated attacks.

Perfect Storm

Human error combined with AI misuse creates an unprecedented high-risk environment requiring immediate attention.

Our objective today: Build awareness and establish practical safeguards before threats become losses.

The Double-Edged Sword of AI

Opportunities

- Document automation and processing efficiency
- Enhanced customer engagement and communication
- Predictive analytics for risk assessment
- Streamlined compliance and reporting

Threats

- Automated Hacking & Reconnaissance
- AI-powered fraud schemes at unprecedented scale
- Sophisticated misinformation and deepfakes
- Automated social engineering attacks
- Quality control failures in critical processes

> **"AI doesn't just accelerate business—it accelerates crime."**

Everyday Risks Title Companies Face

Wire Fraud & Phishing

AI-generated emails that perfectly mimic legitimate communications, targeting high-value wire transfers with devastating accuracy.

Seller Impersonation Fraud

Fraudsters leveraging AI to create fake identities, forge documents, and impersonate property owners in transactions.

Social Engineering Scams

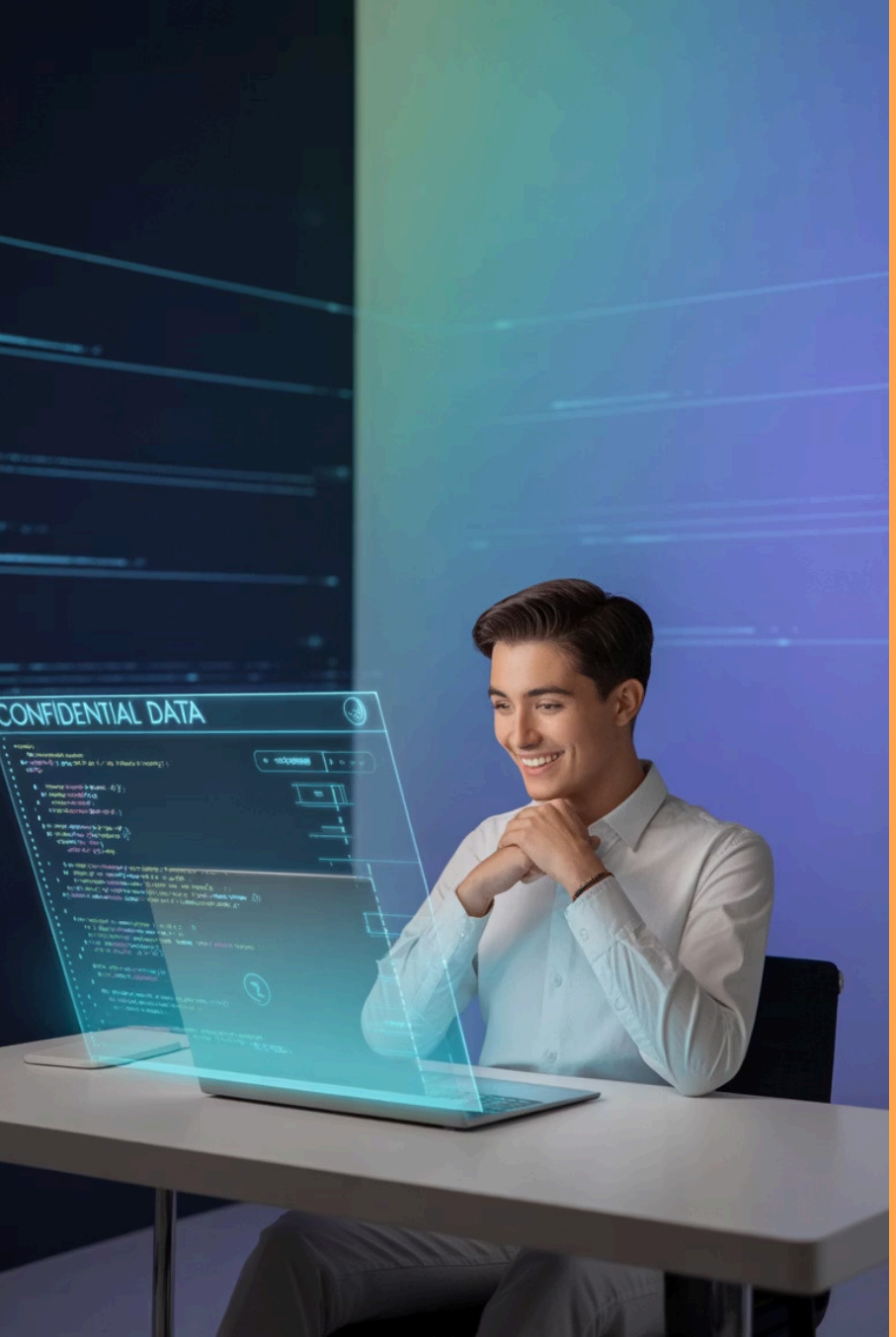
Sophisticated manipulation tactics enhanced by AI research and personalization capabilities.

Internal AI Misuse

Staff using AI tools improperly for sensitive content, creating compliance risks and potential data breaches.

Quality Control Failures

Over-reliance on AI-generated work without proper human oversight leading to critical errors in documentation.



Wire Fraud Risk Increased

AI-Crafted Phishing

Advanced language models create perfectly written emails that pass traditional spam filters and human skepticism.

Voice Cloning Technology

Fraudsters can now clone voices from just a few seconds of audio, impersonating escrow officers and closing agents.

Real-Time Translation

AI translation tools allow international crime rings to target English-speaking markets with unprecedented accuracy.

Real Example: A fraudster used voice cloning to impersonate a closing officer, calling clients to "confirm" wire instructions that diverted $485,000 to an offshore account.

Seller Impersonation Fraud

01

AI-Fueled Property Research

A fraudster's work to identify quality target properties, owners, realtors, and title companies are easier than ever.

02

AI-Generated Fake IDs

Sophisticated document forgery using AI image generation and text manipulation tools.

03

Deepfake Video Verification

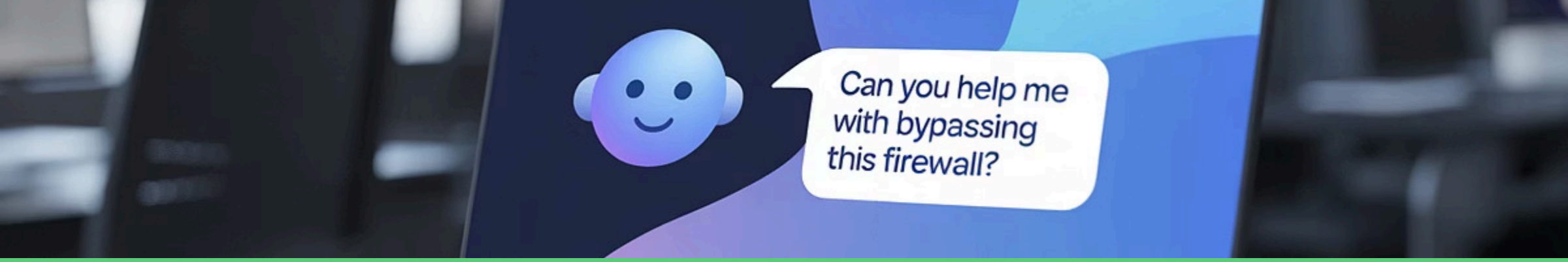
Face-swap technology enables fraudsters to appear as legitimate sellers in video calls.

04

Digital Signature Forgery

AI learns signature patterns to create convincing forged signatures on closing documents.

⚠ **Alert:** Vacant lot and investment property fraud has increased 340% since 2020, with AI-enhanced schemes driving the surge.



Social Engineering Supercharged

AI Chatbot Conversations

Advanced chatbots conduct hours-long conversations, building trust and gathering intelligence for future attacks.

Data Mining & Profiling

AI scrapes LinkedIn, email signatures, company websites, and public records to build detailed target profiles.

Personalized Attack Campaigns

CEO fraud and vendor spoofing schemes customized with AI-researched personal details and company-specific language.

> **Critical Insight:** AI makes bad actors scalable. What once required manual research now happens instantly, enabling mass personalized attacks.

AI Without Quality Control

1

Legal Content Risks

Title agents using AI for contracts, disclosures, and legal documents without proper review create liability exposure.

2

AI "Hallucinations"

AI generates convincing but factually incorrect information, potentially corrupting critical transaction documents.

3

Data Exposure

Confidential client information accidentally shared with public AI tools, creating privacy breaches and compliance violations.

4

Regulatory Compliance

FTC, CFPB, and ALTA best practices require human oversight of AI-generated content affecting consumers.

Banking Sector Overlap

Account Takeovers

AI-driven credential stuffing and social engineering target bank accounts linked to real estate transactions.

Synthetic Identities

AI helps create fake loan applications using combinations of real and fabricated personal information.

Wire System Vulnerabilities

Shared banking infrastructure means breaches at one institution can compromise multiple title company relationships.

Coordinated Fraud Rings

Criminal organizations use AI to coordinate sophisticated attacks across multiple institutions simultaneously.

Banks and title companies share interconnected risk. A breach at your lending partner can quickly become your problem through compromised wire instructions or fraudulent loan documentation.

What's at Stake

$538M

Wire Fraud

In 2023, FBI RAT successfully placed holds on $538.39 million of the $758.05

340%

Fraud Increase

Growth in seller impersonation cases since AI tools became widely available

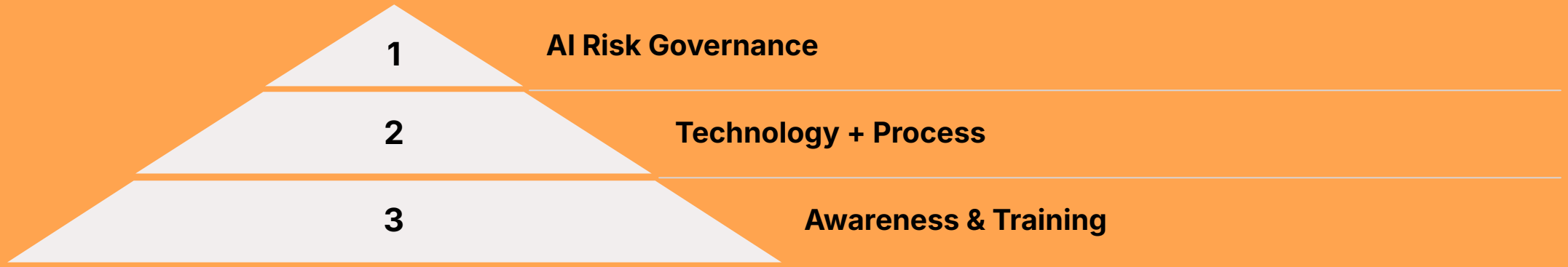
72hrs

Detection Window

Average time to discover wire fraud - often too late for recovery

- **E&O and Claims Exposure:** Increased liability for AI-related errors and security failures
- **Reputation Damage:** Lost trust with clients, underwriters, and business partners
- **Regulatory Penalties:** CFPB and state regulatory actions for inadequate consumer protection
- **Operational Disruption:** Investigation costs, system shutdowns, and business interruption

Building Resilience: The Big Picture



Effective AI risk management requires a comprehensive approach combining governance, technology, and human awareness. Success depends on building multiple layers of defense that work together.

Governance

Establish AI usage policies, risk committees, and clear accountability structures for AI-related decisions.

Technology

Deploy security tools, monitoring systems, and verification platforms designed for the AI era.

People

Train staff to recognize AI-enhanced threats and implement human verification processes.

Defenses Against Wire Fraud

1 Advanced Email Security

Deploy AI-driven email security platforms like Avanan, Proofpoint, or Microsoft Defender to detect sophisticated phishing attempts that traditional filters miss.

2 Out-of-Band Verification

Establish mandatory call-back procedures using pre-verified phone numbers for ANY wire instruction changes, regardless of apparent source legitimacy.

3 Staff Training Programs & Share Stories

Educate employees on AI-enhanced phishing red flags: perfect grammar in unusual contexts, urgent requests with tight deadlines, and subtle changes in communication patterns.

4 Dual Authentication (is this where we're heading?)

Since you cannot trust voice anymore, are you able to add secondary verification through encrypted messaging, in-person confirmation, biometric authentication, or security OTP codes for high-value or higher-risk transactions?

Combating Seller Impersonation

01

Robust ID Verification

Implement multi-layered identity verification platforms with biometric checks, document authentication, and real-time validation against government databases.

02

Pattern Recognition

Monitor for vacant lot fraud indicators: rushed timelines, out-of-state sellers, cash transactions, and properties with minimal improvement history.

03

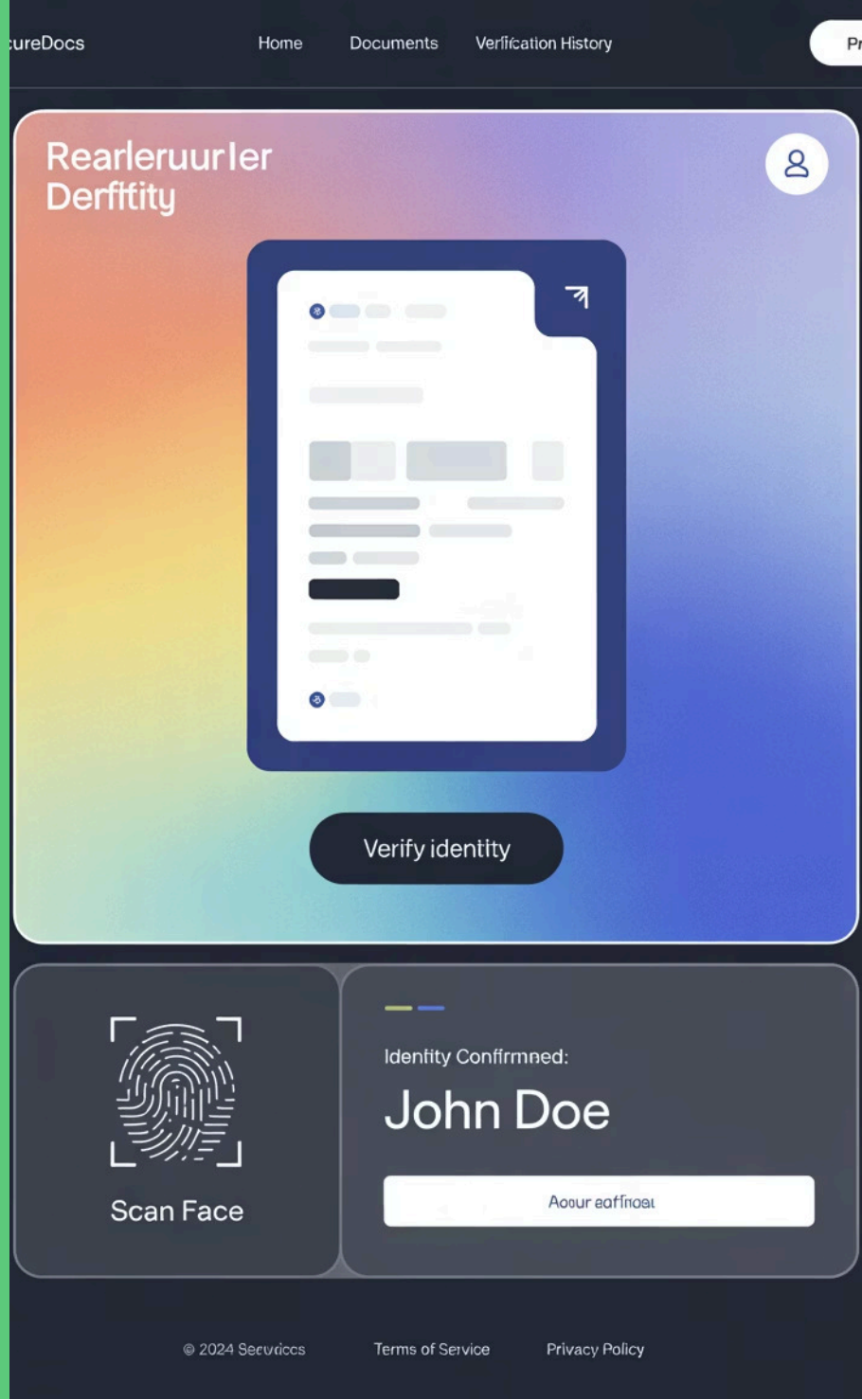
Enhanced Verification

Require in-person appearances or notarized verifications for high-risk transactions, especially involving investment properties or absentee owners.

04

Underwriter Collaboration

Work closely with underwriters to establish clear flagging criteria and investigation protocols for suspicious transactions.



Defenses Against Social Engineering

Reduce Attack Surface

- Limit public exposure of staff information including email formats and direct phone lines
- Review social media policies for employees handling sensitive transactions
- Implement generic contact methods for initial client communications

Internal Controls

- Establish strict approval workflows for unusual requests
- Require supervisor confirmation for vendor payment changes
- Create "cooling off" periods for urgent financial requests

Automated Response & Orchestration

- **SOAR platforms with AI** (Security Orchestration, Automation, and Response) can isolate accounts or block transactions within seconds of detecting a likely social engineering attempt.
- **Real-time transaction scanning**: For wire transfers or title payouts, AI models can validate recipients against approved patterns or historical records.

Red Team Testing: Regularly simulate attacks internally to identify vulnerabilities and test employee responses to sophisticated social engineering attempts.

Key Training Focus: Teach employees to recognize "pretexting" tactics where attackers use AI research to build credible cover stories and manipulate emotional responses.

Safe AI Use Inside Companies

AI Usage Policy - What to put in it?

- What tools are permitted? Are they vetted by an MSP/IT consultant?
- Who are the identified people to authorize use of an AI tool?
- When is it permitted and with what human oversight?
  - Client communications - AI chatbots? Auto-reply emails?
  - CE materials use? Blogs or publications?
- Consider ethical issues, not just legal ones
- Data Protection:
  - make clear that NPI, PII, and confidential info should not be put into a public AI system
  - only use approved, company-purchased solutions that are private use only

Audit Trail Documentation

Maintain detailed records of AI tool usage for compliance reviews and quality assurance purposes.

Remember: AI is a powerful tool, but in title and banking, accuracy and confidentiality are non-negotiable. Every AI application must undergo rigorous vetting and continuous monitoring.

Simple Day-to-Day Safeguards

Multi-Factor Authentication

Implement MFA on all systems handling sensitive data. Use authenticator apps rather than SMS when possible for enhanced security.

Phishing Simulations

Conduct monthly staff phishing tests using AI-generated scenarios to keep awareness high and identify training needs.

Password Management

Deploy enterprise password managers with automatic rotation policies and password complexity and uniqueness requirements. Eliminate duplicate passwords.

Zero Trust Verification Mindset

Question and verify every unusual request, regardless of apparent source. When in doubt, use alternative communication channels to confirm.

AI as a Defensive Tool

While AI enables new threats, it also provides powerful defensive capabilities. Smart implementation can significantly enhance your security posture.

Fraud Detection Algorithms

AI systems analyze transaction patterns to identify anomalies and flag potentially fraudulent activities in real-time.

Transaction Monitoring

AI-powered surveillance systems track wire transfer patterns and automatically flag suspicious routing or timing anomalies.

Voice Analysis Technology

Advanced audio processing can detect deepfake voices and voice cloning attempts during phone verifications.

Document Authentication

Machine learning models can detect forged documents and AI-generated content with increasing accuracy.

Case Study: Voice Clone Heist

What Happened

A sophisticated fraud ring targeted a major title company. They used publicly available audio from the company's marketing videos to create a voice clone of the senior closing officer.

The Attack

The fraudsters called buyers 24 hours before closing, perfectly mimicking the officer's voice and mannerisms. They provided "updated" wire instructions due to a "bank routing issue," directing funds to an account in the Cayman Islands.

The Damage

Diverted funds across three transactions before the scheme was discovered. Recovery efforts failed due to rapid international transfers. Resulting in over $2 million in losses.

The Lesson: Voice verification alone is no longer sufficient. This company now requires encrypted email confirmation and dual-person verification for any wire instruction changes.

What Companies Can Do NOW

Establish & Train on AI Use Policy

Create comprehensive guidelines covering AI tool usage, data handling, and approval processes. Include clear consequences for policy violations. Train your team multiple times and with varying methods.

Verify Vendor Security

Audit all technology vendors for AI-related security measures. Ensure contracts include specific AI fraud protection clauses and liability terms.

AI-Awareness Training

Conduct immediate staff education sessions focusing on AI-enhanced threats. Include practical exercises using real-world scenarios.

Layered Prevention Tools

Implement multiple security layers: advanced email filtering, voice authentication for approvals of changes/access, biometric verification for approvals of changes/access, and anomaly detection systems.

Strategic Partnerships

Collaborate with brokerages, banks, underwriters, and local government to develop joint defense strategies, share threat intelligence, and coordinate incident response plans.

Key Takeaways

AI Magnifies Everything

Artificial intelligence amplifies both fraud risks and defensive capabilities in title and banking transactions.

Human + AI = Double Risk

The combination of human vulnerability and AI capabilities creates unprecedented opportunity and danger in our industry.

Prevention Requires All Three

Effective protection demands coordinated process improvements, advanced technology deployment, and strong security culture.

> "Trust but verify—every transaction, every time."

Questions & Open Discussion

Share Your Experiences

Have you encountered AI-related fraud attempts in your transactions? What red flags have you noticed?

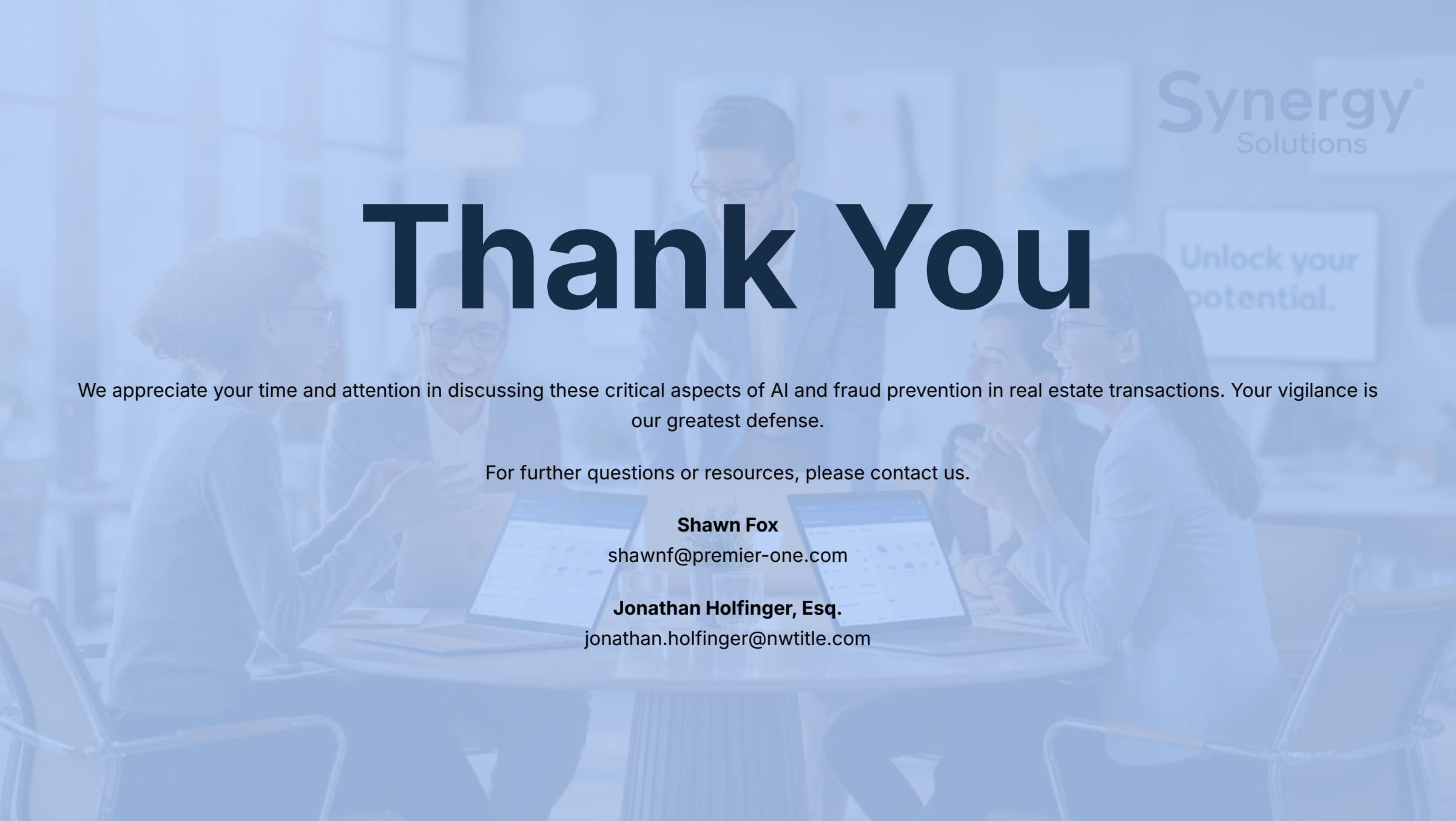
Defense Strategies

What security measures has your company implemented? Which approaches have been most effective?

Industry Collaboration

How can we better share threat intelligence and coordinate defenses across the title and lending community?

Your insights and experiences help strengthen our entire industry's defense against AI-enhanced fraud. Let's discuss practical solutions and lessons learned from real-world incidents.



Thank You

We appreciate your time and attention in discussing these critical aspects of AI and fraud prevention in real estate transactions. Your vigilance is our greatest defense.

For further questions or resources, please contact us.

Shawn Fox
shawnf@premier-one.com

Jonathan Holfinger, Esq.
jonathan.holfinger@nwtitle.com