velera

Risk Mitigation in the AI-Verse

2026 Fraud Trends Report

1

When Scams Went Industrial

1. **Social Engineering and Scam Manipulation Accelerated**
   Key Takeaways: Traditional fraud controls increasingly being bypassed with consumer engaged persuaded fraud. Next frontier will entail FI ability to not only **detect** suspicious transactions but also **manipulated intent**.

2. **Identity Became the Battleground**
   Key Takeaways: Fraud continues to move upstream into ID and access points across the full member lifecycle. The most effective defense for FI's in 2026 is an **AI-powered, multi-layered, optichannel, zero-trust strategy**. Transition to real-time behavioral biometrics, adaptive MFA, and cross-institutional consortium data.

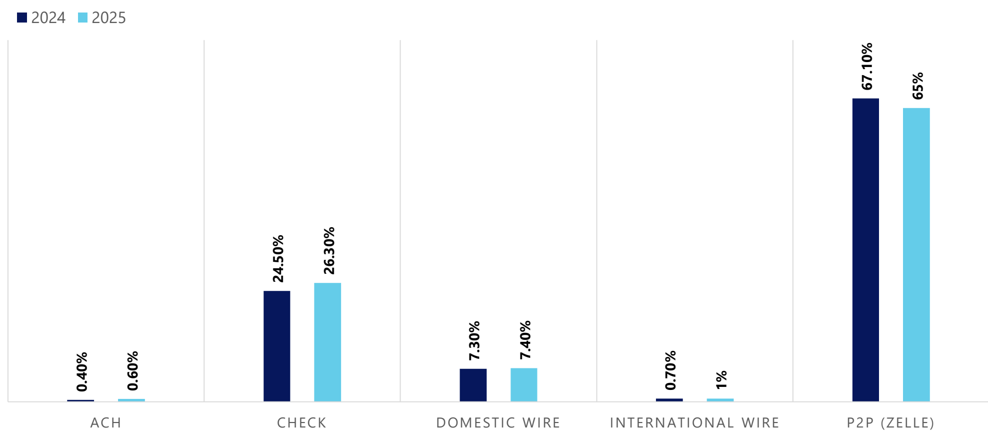
3. **Check, Debit, and Traditional Payment Fraud Continues**
   Key Takeaways: Dual reality: legacy fraud methods remain active while digital and AI-enabled fraud are accelerating. Check fraud surged proving that institutions still need **modernization across traditional fraud controls** and **payment rails**.

2

2

2024 – 2025 YOY U.S. Fraud Volume Share Growth

Checks and P2P payment rails see the most significant impact of fraud volume



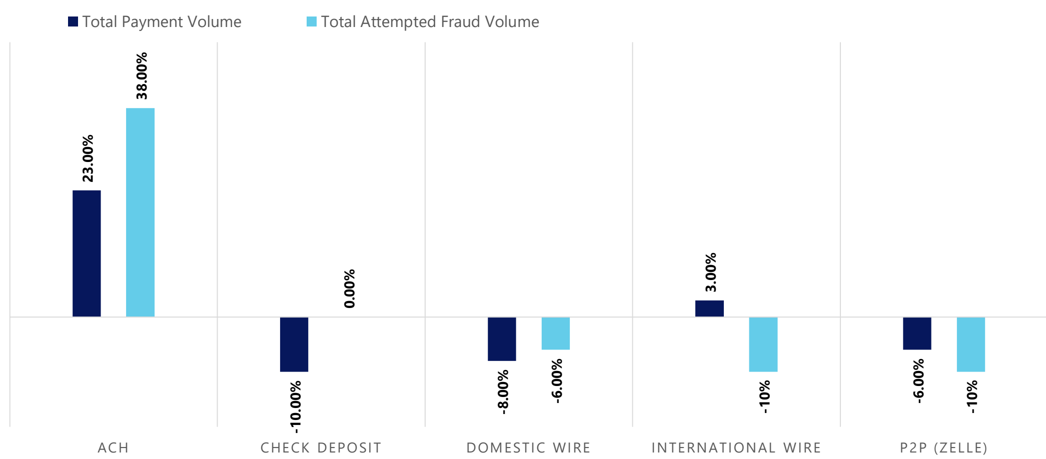
3

Source: Nice Actimize

3

2024 – 2025 YOY Fraud Volume Growth vs. Payments Volume

*Fraud pressure is **not** uniformly scaling with payment growth but concentrating in specific rails, thus prompting the need for rail-specific risk controls rather than uniform response models.*



4

Source: Nice Actimize

4

velera

Does payments innovation come at the cost of fraud and risk?

5

velera

The AI-Verse: Reshaping the Future of Payments in 2026 & Beyond

The AI-Verse is an expanding ecosystem of generative AI, predictive AI, agentic AI, machine learning models, data platforms, and intelligent digital assistants that are reshaping how businesses and consumers interact with technology and financial services.

6

The Scampocalypse Evolution…

Consumer engagement through deceptive practices, commonly known as scams extend beyond financial loss, funding serious crimes like trafficking while harming victims' mental health and credit. They also erode trust in credit unions, reducing engagement and adoption.

Psychological Manipulation

Consumers will experience increased threats targeted at emotional distress, using such tactics as arrests, physical harm, and extortion.

Hyper-Personalization

AI can easily sift through old and new data breaches to build consumer profiles. This will allow the events to be more real and specialized to increase success rates.

Leverage High-Tech Lives

Scams will branch outside of text, voice and email. We will see scams taking place through home devices, videos and agentic agents.

7

7

The Evolution of the Fraud Universe

Protecting Transactions | **Protecting Identities** | **Protecting Trust**

Fraud 1.0
The Transaction-Verse
Era: ~1980s-2000s
Counterfeit Cards, Account takeover, Unauthorized transactions

Fraud 2.0
The Digital-Verse
Era: ~2005-2020
Synthetic identities, New account fraud, Credential compromise

Fraud 3.0
The AI-Verse
Era: 2020s+
Scams, Deepfakes, AI-enabled deception, consumer engaged persuaded fraud

8

8

Artificial Intelligence: In the Hands of the Criminals

In 2026 and beyond, AI will continue to power increasingly personalized, convincing, and scalable fraud scams targeting credit union members. Cyber and fraud attacks will continue to scale by leveraging advanced models.

$20-40B

Global Annual Impact Due to Synthetic IDs

Fraudulent identity creation has become industrialized, driven by open-source AI models that allow criminals to quickly generate convincing fake identities. In some cases, false IDs directly inserted into detection systems, making it harder for organizations to spot false identities.

8M in 2025

Deepfake Volume Increasing

Deepfake incidents will become more bold and direct. They will be leveraged in anything from scams to synthetic ids to employment. Validating IDs through normal documentation will not be sufficient.

40%

Scam Velocity Increase

Agentic AI has accelerated scam creation velocity by 40%, enabling mass personalized attacks at scale. Agentic AI does not rest and is executed on mass scale. Increasing reach and believability.

Agentic Commerce

$3–$5 Trillion in projected global B2C transactions managed by AI agents by 2030

Advanced Fraud & Security Threats

1. **Agent Hijacking & Bot Takeover**
   Criminals compromise AI agents and stored credentials to execute unauthorized transactions
2. **Malicious Merchant Manipulation**
   Fake "AI-friendly" storefronts harvest payment data from automated purchasing agents
3. **"Low and Slow" Fraud**
   Manipulated agents execute clean-looking transactions that evade traditional anomaly-based detection systems
4. **Deepfakes & Impersonation**
   Automated social engineering using voice clones and brand impersonation to bypass biometric security

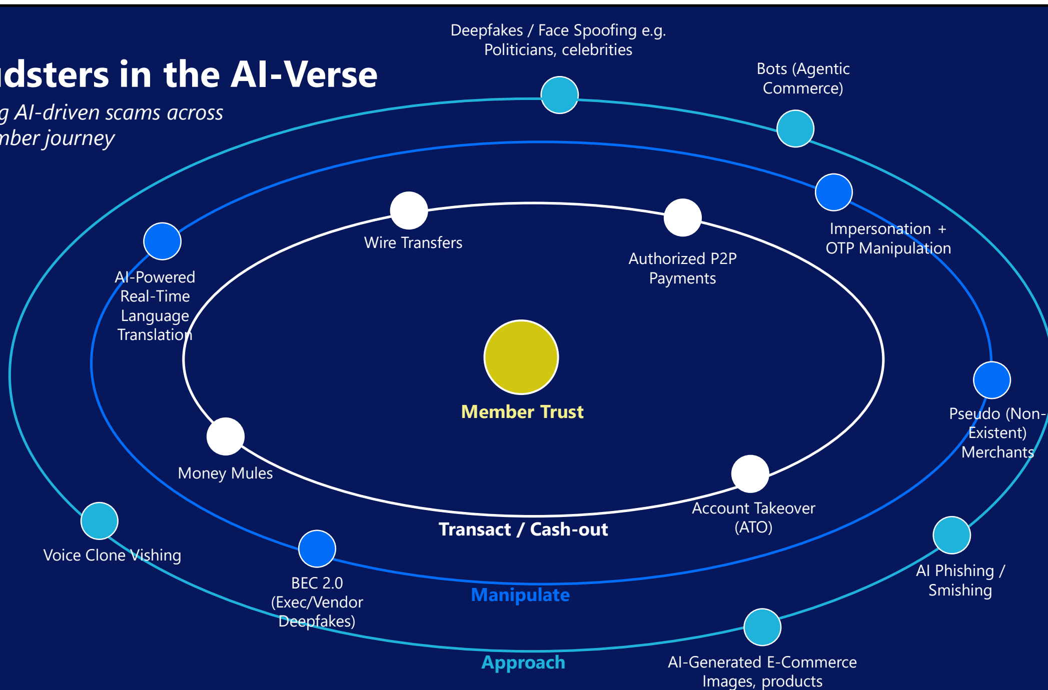
Liability Chaos

1. **First-Party Fraud Claims**
   "My AI agent did it" claims create highly complex liability frameworks for financial institutions with no clear precedent
2. **Unclear Authorization**
   Broad AI permissions and Regulation E gaps may leave banks bearing the cost of refunds when agents make mistakes
3. **Dispute Volume Surge**
   High-volume automated purchasing by AI agents may overwhelm banks with unprecedented transaction dispute volumes

Agentic commerce is shifting from passive browsing to autonomous AI-driven purchasing, creating new attack surfaces and complexities for credit unions that have potential to exasperate already disruptive issues.

Fraudsters in the AI-Verse

Mapping AI-driven scams across the member journey



11

Card-Not-Present Fraud Journey: Social Engineering Attack

1. **TARGET** — Identify a vulnerable member using breached data, social signals, or public information.
2. **IMPERSONATE** — Pose as a trusted institution, merchant, or contact to make the message feel legitimate.
3. **CAPTURE** — Manipulate the member into sharing card details, credentials, codes, or account information.
4. **EXPLOIT** — Use the stolen data to attempt unauthorized digital purchases or card-not-present transactions.
5. **MONETIZE** — Convert fraud into value through purchases, resale, mule networks, or cash-out activity.

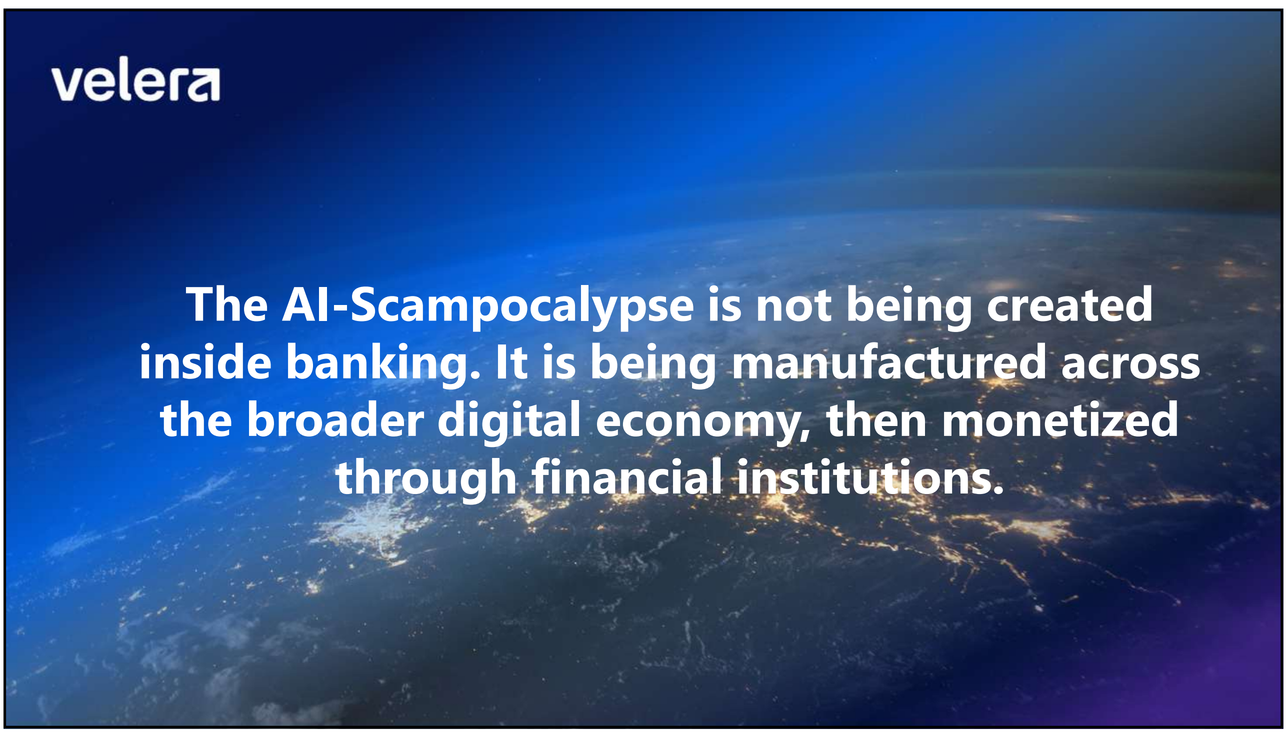
12

12

Counterfeit ID & Impersonation Fraud: Shared Branch

1. **COMPROMISE** — Capture real member identity data through breach exposure, phishing, smishing, or other social engineering.
2. **COUNTERFEIT** — Pair stolen member data with a fabricated or altered ID designed to survive visual inspection.
3. **RECRUIT** — Use a mule or runner who can present the ID, follow a script, and answer basic branch questions.
4. **ATTEMPT** — Enter a Shared Branch location and request a high-risk withdrawal, cashier's check, or similar cash-out transaction.
5. **CASH OUT** — If successful, move funds quickly; if challenged, abandon the attempt and reuse tactics elsewhere.

13



14

Meta Case Study: Corporate Greed Over Consumer Security

- Reuters reported that Meta internally projected about **10% of its 2024 revenue, roughly $16 billion**, would come from **ads for scams and banned goods**
- Platforms showed users an **estimated 15 billion "higher risk" scam ads per day**
- Meta's systems only ban advertisers when **fraud prediction reached** at **least 95%** certainty, while suspected scammers beneath that threshold could be charged higher ad rates instead

15

velera

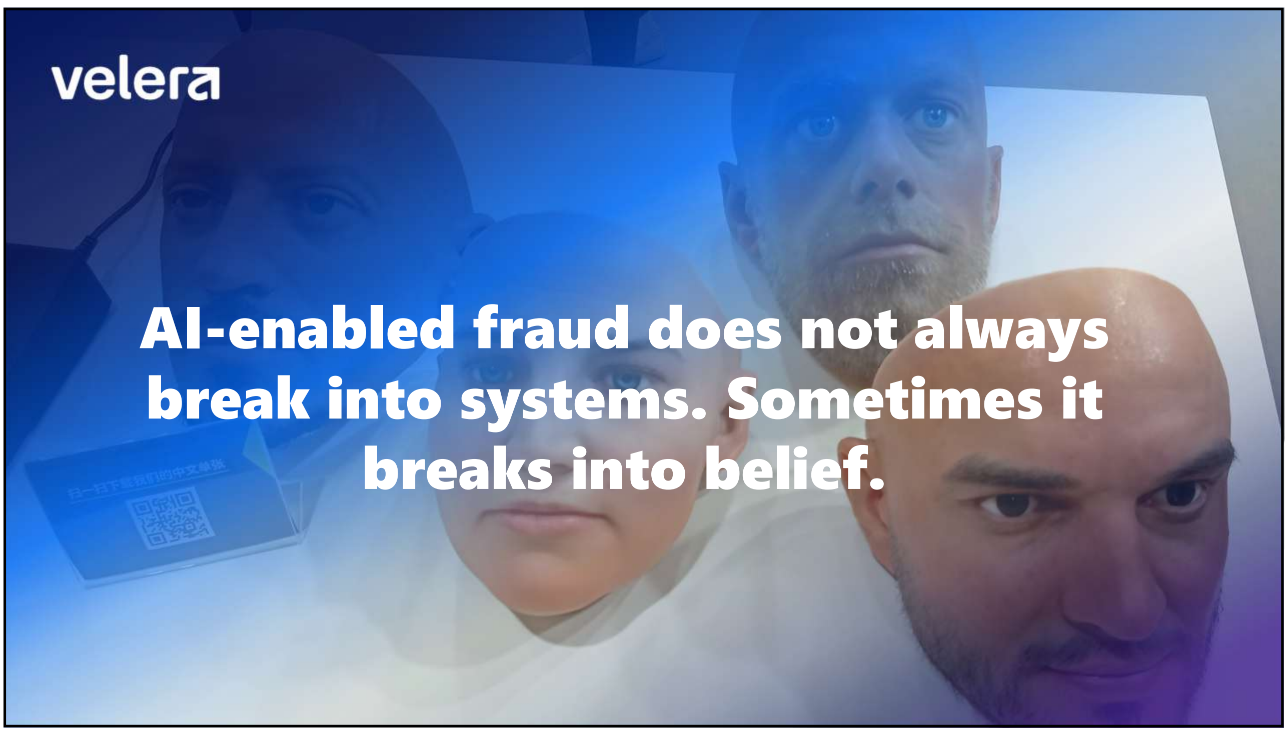
Credit unions are expected to protect members after the scam reaches the payment stage, while corporations like Meta financially benefit.

16

Arup Case Study: $25 Million Deepfake Video Call That Was Not a System Breach

- Early in 2024, an employee at global engineering firm Arup was deceived into **transferring $25 million** after what appeared to be a video call with senior management
- No company systems were compromised and no data was affected

17



18

Listen to these calls, can you spot the difference?

Voice Recording #1

Voice Recording #2

19

19

Listen to these calls, can you spot the difference?

Deepfake
~~Voice~~ Recording #1

Voice Recording #2

20

20

21

Main Challenges That Still Lie Ahead

Priority Misalignment — Corporations don't invest in stopping scams when they are not bearing the weight of absorbing the costs of fraud loss.

Global Consortium Dependencies — **69% of global stakeholders** believe the absence of harmonized AI standards is a major risk to global AI adoption and governance.

Lack of Investment — Companies worldwide are losing significant revenue to fraud—yet still under-investing. In fact, **only 3 investigators per 1,000 employees are staffed** in sectors outside of banking.

AI Investment Lag — Despite AI-driven identity attacks skyrocketing, only **22% of financial institutions** have deployed **AI-based fraud detection systems.** The pace of AI Scam innovation outpaces current ID and prevention infrastructure.

22

22

Regulatory and Government Barriers

1. Scam Liability Rules Still Fragmented
2. "All-Green" Fraud Regulation Lag
3. Real-time Payments are Outpacing Real-time Consumer Protections
4. No Singular AI Fraud Governance Standard Across U.S. Regulators
5. Third-Party AI Provider Oversight Gaps
6. Explainability and Model Variation Requirements Slowing Down Defensive AI Deployment
7. State AI Laws Creating Patchwork of Compliance Obligations

Strategic Priorities for 2027 and Beyond

The key areas aligning payments innovation with fraud readiness

Consumer Engaged Fraud Protection

Identifying and preventing social engineering, payment scams, and self-directed fraud (misuse) among members

Modernize ID & Authentication

Identity should be treated as a continuous control layer across the full member lifecycle

Fighting AI with AI

Leveraging artificial intelligence to detect and counter AI-powered fraud techniques at scale and increase operational impact

Opti-Channel Fraud Intelligence

Orchestrated, real-time event fraud intelligence and signaling will be critical for prevention against emerging complex multi-channel fraud threats.

Fighting AI Scams with an AI-Enabled Risk Mitigation Ecosystem

An ecosystem built to protect credit unions in the AI-Verse.

CURRENT AND FUTURE AI CAPABILITIES

TODAY + FUTURE

Voice & Contact Center Protection

- Passive caller risk assessments
- Conversational Authentication
- Synthetic / deepfake voice detection

POC / EVALUATION

Digital Scam Detection

- Identifying risk before victim engages
- Suspicious content risk detection scoring
- Earlier intervention before payment authorization

POC / EVALUATION

Identity & Counterparty Trust

- Recipient / counterparty verification before payment
- Trust check before funds move

PROSPECTIVE

Payment Moment Intervention

- Additional pre-payment decisioning
- Stronger protection at authorization

ATMOS RISK ECOSYSTEM Strategic orchestration layer connecting fraud detection, prevention, and member protection across card, digital, payments, contact center, and service channels.

Detect risk earlier. Verify trust faster. Protect members before scammers succeed.


Scan&Score™

27


velera
The AI-Verse Needs More Than AI Detection. It also needs orchestration. Atmos Risk is the intelligence layer powering the next generation of member protection.

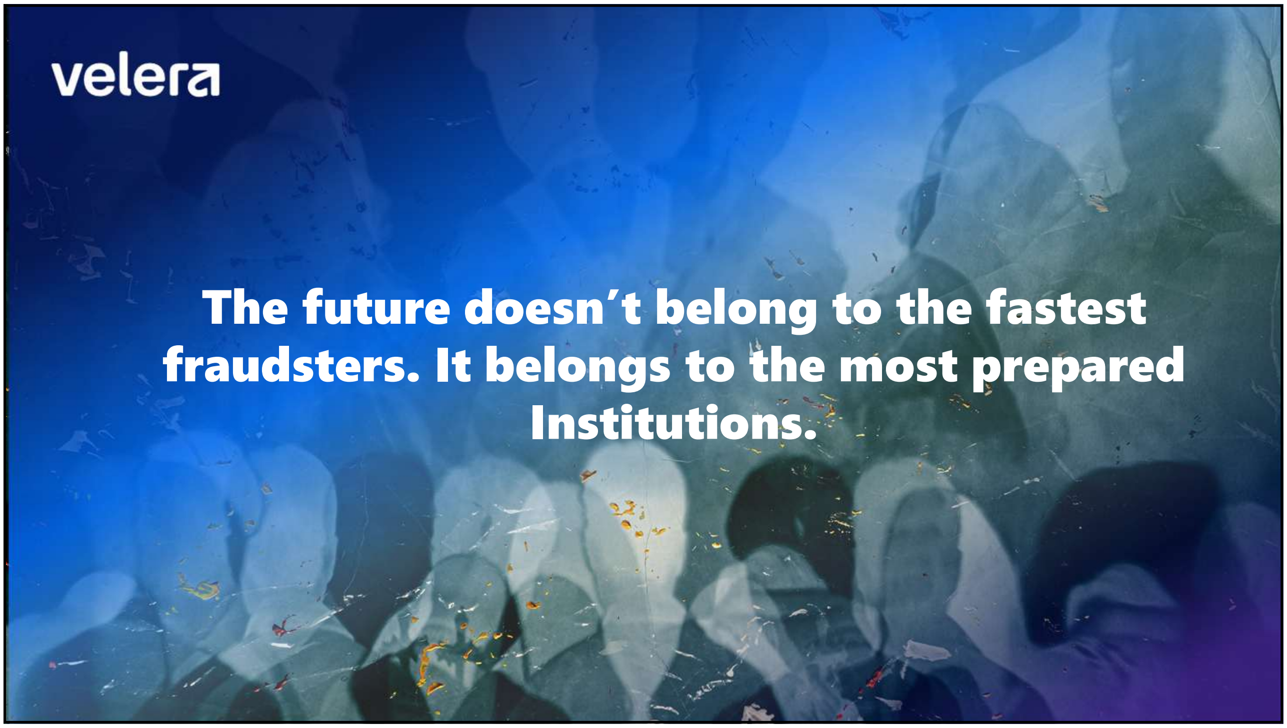
28


The Atmos Risk Ecosystem
Unifying data, decisioning, and protection across the member journey; transforming isolated tools into a connected defense ecosystem.
velera
Service and Intelligence
Atmos Risk Ecosystem
ethoca
VISA
LexisNexis
BioCatch
FICO
NICE Actimize
FEATURE SPACE
Risk Orchestration
Socure
ALLOY
BROADCOM
Casap
Scamnetic
©Velera. All rights reserved worldwide.

29


Digital Service Tools
Lexis Nexis / Fico Data
Digital Channels
Contact Center
Digital Payments
Member Service Data
Shared Branch
Data Analytics
Outside Data
Payment Networks
Networks
Card Processing
Authentication / Authorization
AI
Atmos Risk Ecosystem
Atmos Risk isn't defined by today's threats; it's powered by our ability to evolve faster than tomorrow's.

30


velera
The future doesn’t belong to the fastest fraudsters. It belongs to the most prepared Institutions.

31

velera

32