Deloitte.

Trust Under Pressure:

Balancing Fraud Prevention and Friction

January 28, 2026

Agenda

- CEFLI Administrative Reminders
- Presentation
- Questions
- CEFLI Closing Reminders

Thank You, CEFLI Premier Partners

Thank You, CEFLI Affiliate Members

Gold

Deloitte. faegre drinker

Silver

ankura

Bronze

Bell Analytics berwyngroup Evadata

Guidehouse MAYNARDNEXSEN

troutman pepper locke Wolters Kluwer

CEFLI Administrative Reminders

- The Presentation Deck: The presentation deck is available now: https://cefli.org/webinars/

- Post-Event Communication: We will email the following information to you in the next few days:
  - A link to the recording
  - A copy of the slides
  - A Certificate of Attendance template

- Questions Welcomed! Please use the **Chat** function and send messages to "Everyone." We will try to announce questions after each subsection of content.

Antitrust Reminder

The Compliance and Ethics Forum for Life Insurers (CEFLI) is committed to adhering strictly to the letter and spirit of the antitrust laws. Meetings conducted under CEFLI's auspices are designed solely to provide a forum for the expression of various points of view on topics described in the programs or agendas for such meetings.

Under no circumstances shall CEFLI meetings be used as a means for competing companies or firms to reach any understanding – expressed or implied -- which restricts competition or in any way impairs the ability of members to exercise independent business judgment regarding matters affecting competition. Accordingly, appropriate objection will be made to any presentation or colloquy that presents a risk from the standpoint of the antitrust laws.

The Presenters

Deloitte.

Alex Bolante
Managing Director, Deloitte
abolante@deloitte.com

Justin Fawley
Managing Director, Deloitte
jfawley@deloitte.com

Craig Friedman
Managing Director, Deloitte
crfriedman@deloitte.com

Deloitte.

Trust Under Pressure:

Balancing Fraud Prevention and Friction

January 28, 2026

Evolving trends in identity and ATO fraud

New and emerging digital fraud schemes have challenged the market with sophisticated attacks, forcing organizations to evaluate their existing fraud detection and prevention capabilities and controls.

5 minutes

Between each **deepfake fraud** attempt in onboarding flows in 2024[1]

4,151%

Growth of **phishing emails** after the **introduction of ChatGPT**[5]

1.1 million

Identity theft reports filed to the FTC in 2024[3]

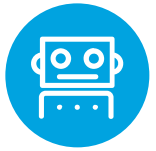
62%

of organizations experienced **account takeovers** in 2024[6]

Advanced fraud technology platforms – AI-assisted tools can create fake drivers' licenses with photo and signature generation, decreasing the time, skill, and effort required by criminals to create high-quality false identities.[7]

Faster transactions are common attack vectors with low recovery – real-time payment (RTP) and account takeover (ATO) instant-loss risk grew 41% YoY in 2024 as fraudsters exploit faster payment rails.[4]

Proactive defense is paramount – Bad actors utilize agentic AI and AI tools to help develop increasingly advanced and convincing social engineering and phishing campaigns.[8]



Generative AI chatbots designed for cybercrime – unrestricted AI tools such as WormGPT, FraudGPT, and EvilGPT have sprung up on the dark web, designed to create phishing campaigns, malware, and more.[2]

Increasing speed of financial/reputational damage – sophisticated fraud schemes exacerbate a bad actor's ability to quickly cause damage by exploiting weak identity systems.

Managing talent and costs will be key, as risk of fraud expands - AI-savvy talent and fraud subject matter specialists will be crucial for adaptability and scalability.

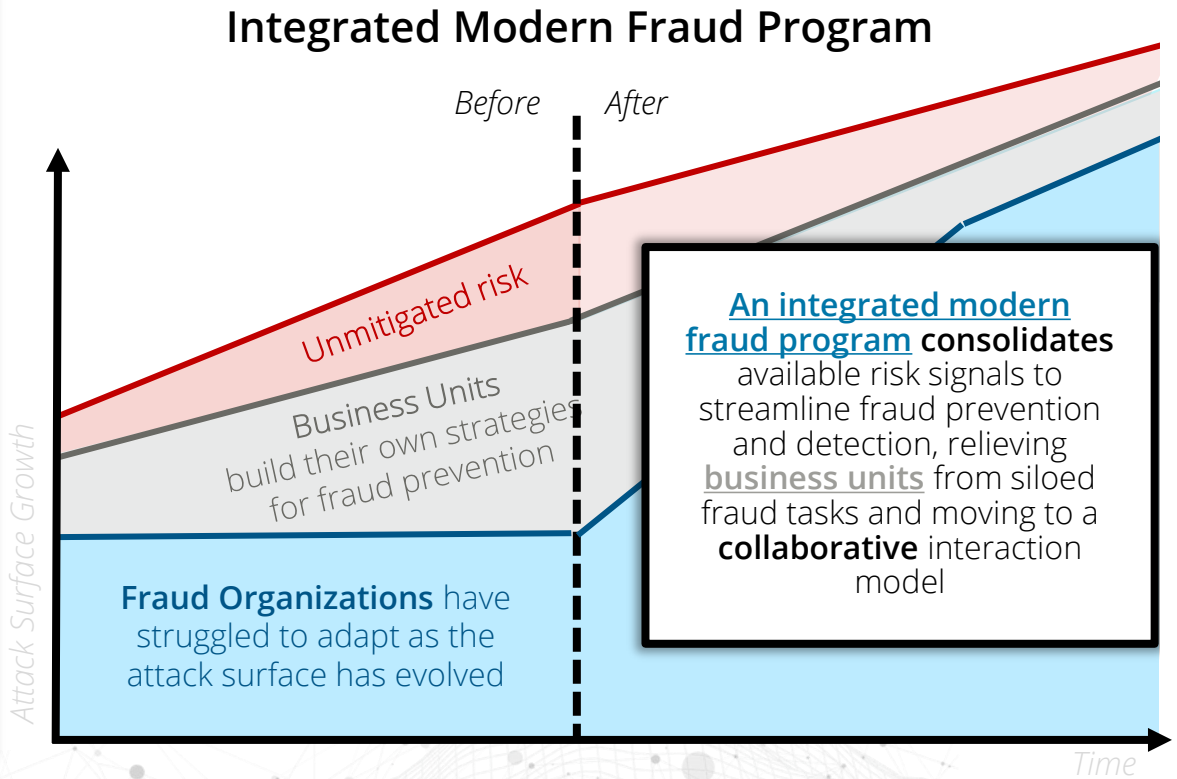
Sources: 1. Entrust 2. Abnormal 3. FTC 4. LexisNexis 5. Dashlane 6. Proofpoint 7. Resistant 8. IBM

Common challenges in anti-fraud programs

While organizations are striving to advance their anti-fraud capabilities to identify and mitigate sophisticated attacks from new and emerging threats, common challenges have become prominent that hinder their development and ability to minimize their exposure to fraud risks.

Many organizations today…

- x Have **siloed** fraud detection and prevention efforts, and siloed fraud mitigation signals
- x Rely on business units to **build their own strategies** for fraud prevention
- x Struggle to keep up with the **evolving attack surface** fueled by new types of threats (e.g., artificial intelligence, generative AI)
- x Respond by integrating multiple cyber and fraud tools that often create **redundancy and increase costs**

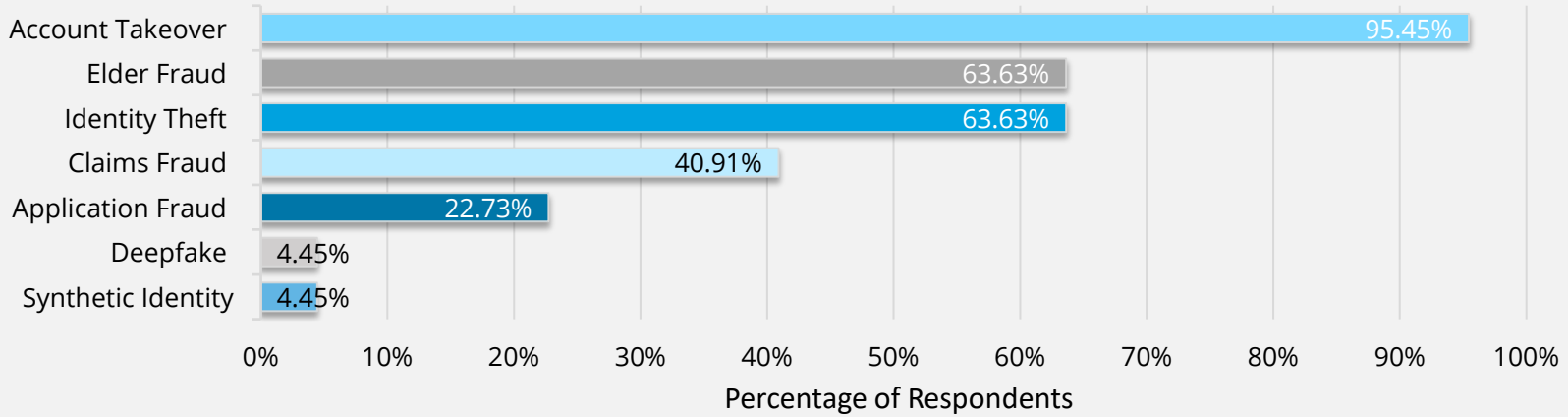


With an integrated modern fraud program, organizations can…

- ✓ **Centralize risk signal** aggregation, response, and strategy development
- ✓ **Standardize**, measure, and manage fraud prevention and detection operations
- ✓ **Eliminate redundancies** in technology, cutting costs, and leveraging appropriate tools and technologies
- ✓ Leverage AI and machine learning to adjust their fraud strategies based on **historical data**

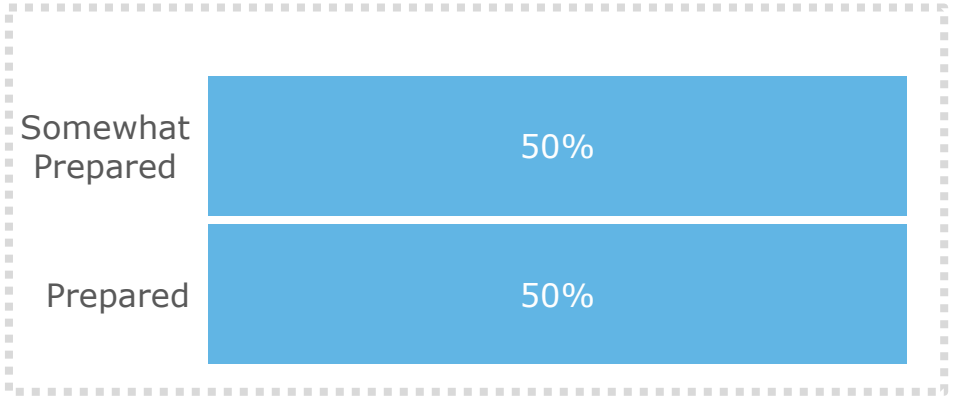
We asked, and your peers shared their top concerns…

Types of fraud of greatest concern to respondents



Readiness

All organizations reported being at least somewhat prepared for their fraud risk types of greatest concern



Types of fraud of greatest concern for firms somewhat prepared

- The fraud risk types of greatest concern to the 50% of the firms that reported being only somewhat prepared are similar to the types of greatest concern to all respondents
- **Less than 15% of firms indicated that they track adversarial cyber techniques** or map known cyber threats with detailed threat path documentation and visual maps. Such tracking is leading practice for combatting multiple types of cyber-related fraud risk types, including account takeover

*Agent / Sales Fraud was not available as a selection for the types of fraud of greatest concern

Stages of account takeover through the Call Center

Below are examples of the stages of account takeover in the Call Center, detailing how attackers progress from gathering information and gaining initial access to manipulating accounts, executing fraudulent activities, and ultimately monetizing through various scams.

Account Takeover – Call Center

Cyber — *Look Right* → ← *Look Left* — Fraud

Phase 1 – Reconnaissance	Phase 2 – Initial Access	Phase 3 – Positioning	Phase 4 – Execution	Phase 5 – Monetization
Dark web marketplace	Call center social engineering	Account linking	Submission of fictious claim	Electronic funds transfer
Elder abuse	Member impersonation	Add authorized user	Receive medical benefits	Automatic clearing house
Family fraud	Phone port-out	Add beneficiary	Receive medical services / products	Check
Identity theft	SIM swap	Change account details	Harvest data	Digital payments
Insider threat	Spoofed phone number	Change notification settings	Prescription fraud	
IVR processing		Collect personal information	Extend coverage/benefits to non-eligible individuals	
Mail theft		Create persistent access		
Malware infection		New payee		
Open-source intelligence		Request execution forms		
Third-party data breach				
Social engineering				

Standardizing identity verification across channels

Combating fraud and regulatory risk demands a layered verification strategy, that integrates technology, analytics, and regulatory checks for robust protection across all lines of business. These advanced techniques aim to intercept fraud before customer losses or regulatory failures occur, and that begins at identity verification.

Identity Verification Channels

Contact Center | Web | Mobile | Email | Chatbot

RESOLUTION

Distinguishing a person's identity in the context of the system.

VALIDATION

Collecting identity information from the user and confirming the accuracy of that information.

VERIFICATION

Verifying that the user is who they claimed to be (Government issued Photo ID & Biometric).

Identity Verification Capabilities

- Personal Identifiable Information (PII) Validation
- KYC / AML Checks
- Device Fingerprinting
- Phone Number Reputation Analysis
- Email Reputation Analysis
- Facial Liveness Detection

Risk Indicators

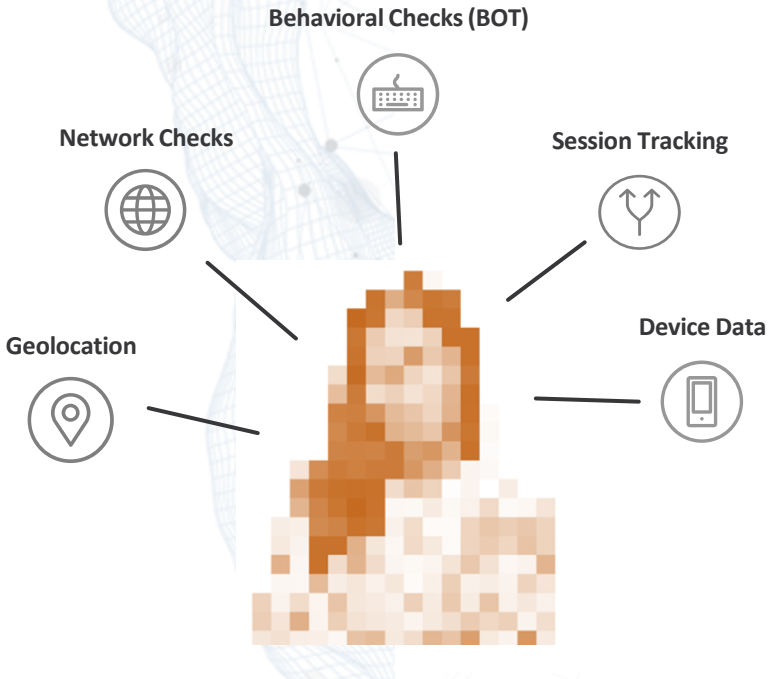
- Transaction Scores (behavior, inherence, possession, account, bot)
- Hardware / Network / Software attributes, Email / Phone number activity
- PII data for Sender and Receiver (traditional / non-traditional)
- Behavioral Patterns (incl. interaction, geo-location, velocity tracking, network security check)

EQUIFAX Accertify JUMIO experian 1KOSMOS BlockID Kount LexisNexis Prove onfido BioCatch SEON twilio ekata by neustar ID.me sardine IDEMIA Middesk ALLOY Socure

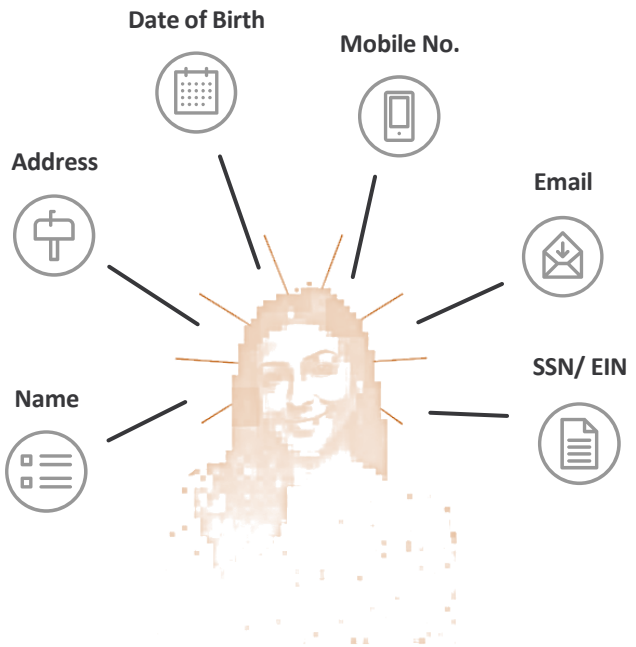
Building a 360° risk profile through identity verification

By leveraging modern identity verification tools and processes, insurers can create comprehensive risk profiles and confidently confirm that each user is who they claim to be, enabling more digital self-service with less friction, while effectively mitigating the risk of identity fraud.

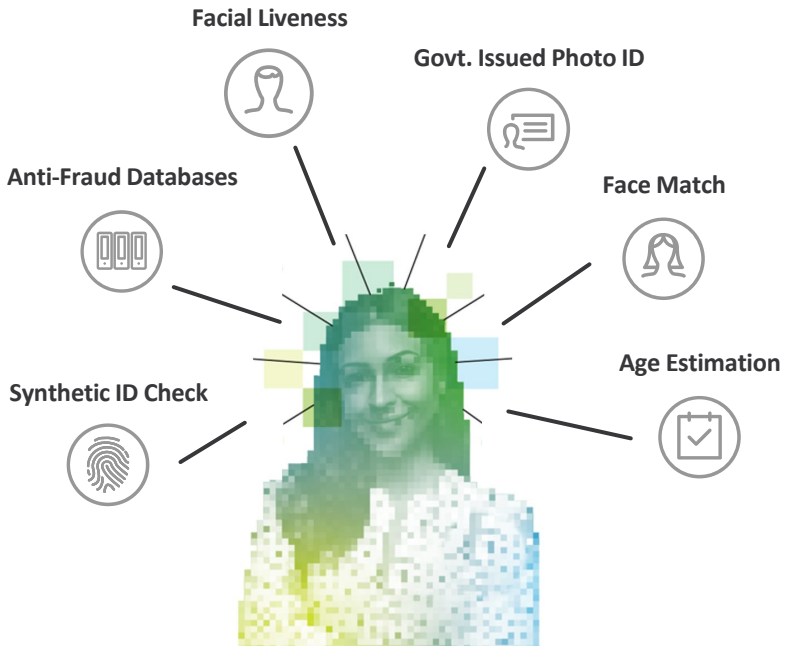
Probabilistic → **Deterministic**



RESOLUTION



VALIDATION
(Aggregators/ Consortium Data)



VERIFICATION
(Confirm the authenticity of identity documents and verify they belong to the identity of the individual)

Outcome: Risk-tiered verification reduces unnecessary step-ups for legitimate customers while tightening controls for high-risk sessions

Establishing and maintaining trust across the customer journey enables organizations to expand digital onboarding and servicing while delivering more personalized experiences. This is achieved by integrating reputational data, identifying links to known fraud risks, and applying these signals in transaction scoring.

Building an integrated & modern digital fraud program

We recognize that most organizations are looking to mature their fraud risk management programs to meet internal and client expectations. We have seen how leading organizations emphasize coordination between fraud and related teams, in strategy, people, process, and technology.

Many organizations are here today

AWARE

Aware of risks and over-rely on manual intervention by investigators for fraud prevention, investigations, and recalls

- Baseline capabilities **over-rely on investigators**
- **High friction experiences** for clients and agents
- Reactive implementation of detection capabilities **often using default settings**
- **Data is siloed** and distributed

REACTIVE

Reactive implementation of fraud technology and controls. Capabilities for real-time intervention are emerging but are not yet mature.

- New technology / changes to existing technology happen as a **reaction to fraud events**, no strategic direction yet
- Technology is organized to **evaluate risk at high-risk moments** of the customer journey
- **Formal fraud analytics group formed** to manage research and analysis of fraud events to customize rule-based detection
- **Centralized and standardized data** on past fraud events

PROACTIVE

Proactive with fraud detection, prevention, and control implementation. Balances fraud losses with client / agent experience accordingly.

- **Fraud capabilities are mature** and client and agent experiences are improved
- **Risk-based scoring is available** on-demand
- The client experience is **curated based on the risk** presented in the customer journey
- Strategic **objectives balance fraud losses with client and agent experience**
- **Fraud metrics have matured** and are aligned across systems, organizational teams, and fraud vectors inherent to the product mix

INTEGRATED

Integrated fraud controls across lines of businesses. Leverage AI/ML to improve controls, rules, and/or models based on historical data

- **360-degree risk view using active, passive and account level data**
- Fraud risk **strategic objectives are fully aligned** and integrated with other lines-of-business roadmaps
- **Fully integrated organizational performance monitoring program** (KPIs/LRIs) links impacts from one node to another
- Iterative feedback loop uses automated monitoring to evaluate fraud risk countermeasures and iteratively **adjusts models based on historical fraud data**
- Cross-lifecycle AI/ML **risk modeling supported by a centralized data solution** with risk indicators from across the customer experience

Where do organizations usually start

Enterprise Fraud Strategy

- Develop an enterprise strategy for fraud detection and prevention to identify and assess the **risk of Identity and other fraud types within all operations and systems of the organization, including impacts on agent / customer experience**
- **Define** a Fraud Organizational Structure
- **Establish** a cross-functional operations model with a RACI to clearly define roles and responsibilities
- **Design** an integrated solution architecture with technology components and systems to better **identify potential impacts when making future changes to tools and technology** within the organization

Fraud Risk Assessment

- **Conduct** a **fraud risk assessment** to evaluate and **identify gaps and vulnerabilities** within the existing *fraud detection and prevention tools and technology and fraud analytics and reporting capabilities.*
- Define recommendations that **enhance the end-to-end anti-fraud solution(s) and enhance the client and agent experience** (people, process, and technology).
- Develop a **high-level roadmap** for implementing enhanced fraud detection and prevention capabilities and controls, **including a robust Identity Verification capability**.

Phased Implementation Approach for Fraud Strategy Enhancements

- **Conduct** a **tool** and **technology evaluation** and procurement (centralize, decommission, or buy net-new)
- **Define** anti-fraud and agent / customer experience requirements and design controls surrounding fraud capabilities
- **Design** and implement fraud rules within a fraud rules engine to detect and respond to fraud
- **Outline** documentation to standardize and support process enhancements
- **Conduct** pilot tests to validate the effectiveness of new solutions
- **Implement** new solutions and provide continuous monitoring and improvement

Remaining Questions

Deloitte.

Deloitte.

CEFLI Thanks

Deloitte.

Alex Bolante
Managing Director, Deloitte
abolante@deloitte.com

Justin Fawley
Managing Director, Deloitte
jfawley@deloitte.com

Craig Friedman
Managing Director, Deloitte
crfriedman@deloitte.com

CEFLI Closing Reminders

- Survey: Please complete our 1-minute post event survey when you receive the email, shortly.

- Post Event Communication: The presentation deck, a link to the recording and a Certificate of Attendance form (for those who attended the live webinar) will be emailed within the next day or two.

- CLE/CE: CEFLI's materials are not filed for CLE or CE with any State Bar or other organizations. In the event you plan to self-submit for CE or CLE with the organizations you are involved with, the following slide may be helpful.

CLE/CE Information:

While CEFLI does not file its materials with any State Bar Associations, if you plan to self-submit for potential CLE consideration with a State Bar Association, the following may be helpful:

- CEFLI is the sponsor of its in-person and Educational Webinar events.
- CEFLI provides a Certificate of Attendance form only to individuals who attended a live webinar or an in-person event.
- CEFLI does not have a way of knowing how many attorneys attend a CEFLI webinar or event.
- CEFLI webinars (which are one hour in duration) do not have a timed agenda.
- Participants may ask questions of the speakers during webinar events by clicking on the chat feature in the Webex.
- CEFLI is not a marketing organization. It is a compliance and ethics organization whose mission is to support professionals by providing educational opportunities that address current compliance matters.

Thank You for Joining Us!

Deloitte.