NICE Actimize

White Paper

NICE Actimize Xceed AI FRAML

Designed for Frontier Financial Firms

NICE Actimize

Contents

What is a Frontier Financial Firm? 3

Key AI-Driven Capabilities 4

Why It Matters? 4

Strategic Implications 5

Why Xceed AI FRAML? 5

Xceed AI FRAML Solutions Map 6

Transforming Risk Management 6

How It Works 10

A Smarter Path to Frontier Financial Firm 11

What is a Frontier Financial Firm?

"An organization that combines financial crime human expertise with AI agents to improve efficiency, de-risk "frontier" customer segments and hyper scale financial crime and compliance operations without stretching human resources"

—Eric Tran-Le, Head of Actimize Premier, NICE Actimize

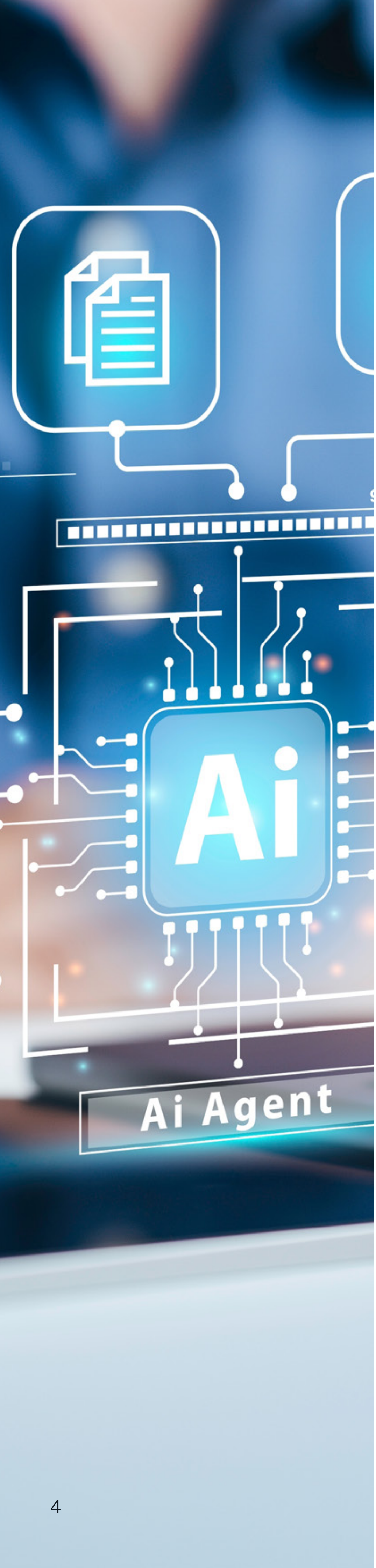
A Frontier Financial Firm is one that embeds AI agents – capable of reasoning, planning and acting – into its core financial crime workflows such as Alert-to-Case and Case-to-SAR.

These agents **initiate, decide, request** human approval and **execute** tasks across the end-to-end business flows.

Rather than relying on humans to handle routine tasks, the Frontier Financial Firm employs a **"crew of intelligent agents"** orchestrated by human oversight. This creates an environment where **intelligence is now a hyper-scalable, responsive utility, embedded** across every financial crime risk management process.

A Frontier Financial Firm:

- Treats **AI agents as co-workers**, not just tools, with **humans maintaining full oversight**
- Uses **real-time financial crime intelligence** to **prevent fraud before it happens**
- **Implements crews of AI agents** to **track money laundering at transaction speed**
- Shifts from traditional models to **agentic workflows with a human-in-the-loop** approach that scales without stretching resources



Key AI-Driven Capabilities

- **Autonomous Execution:** A crew of intelligent agents act without waiting for human prompts.
- **Contextual Reasoning:** AI agents interpret complex data-from regulatory changes to behavioral anomalies at the user, device and transaction level – and make decisions under human oversight.
- **Human Oversight:** Analysts shift from doing routine work that increases alert fatigue, to supervising, refining and auditing AI agent behavior.
- **Scalable Intelligence:** AI capacity scales with transaction volume and fraudster attack vectors, eliminating reliance on increased headcount or offshore resources.

Why It Matters?

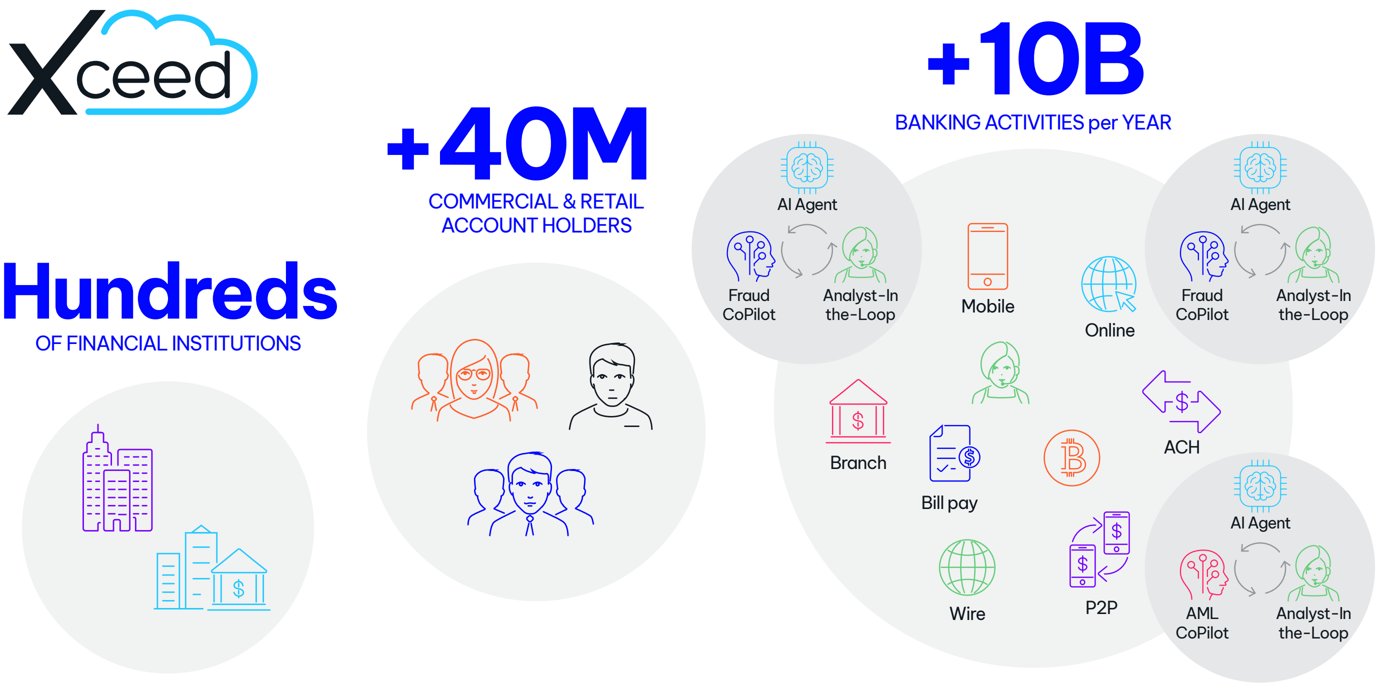
- **Speed:** In the era of digital payments, a new account can be opened in 10 minutes. Within 30 minutes, a significant wire transaction can be initiated at the originator bank and laundered to a mule-account at the receiving bank, all in real-time. This speed and scale makes real-time detection and intervention within fraud and compliance programs essential.
- **Precision:** The high volume of false positives, especially apparent in conventional rule-based tools for both fraud and AML, contributes to alert fatigue and increases the risk of missed fraud and compliance breaches. Reducing false positives in fraud and AML risk scoring by over 60% is required if financial firms don't have a high analyst staff churn.
- **Adaptability:** AI agents learn from feedback via a closed-loop process with human analysts to auto-calibrate their thresholds, adjusting to new regulations and changing payment network operating rules such as NACHA 2026.
- **Cost Efficiency:** Automated agents permit leaner operations with higher throughput and fewer manual bottlenecks.

Strategic Implications

- **Agentic Risk Management:** Imagine a crew of AI agents working 24x7/365 to fight financial crime in real-time, collaborating seamlessly with human analysts. This enables financial firms to de-risk the "frontier" and grow into high-risk customer segments that conventional banks' risk governance models typically avoid.
- **Agentic Compliance:** Autonomous AI agents are able to screen and monitor content for regulatory violations across respective state-jurisdictions. They also interpret changes at the state-level and issue updated KYC forms specific to each jurisdiction.
- **Agentic Retention:** AI agents personalize user onboarding and their ongoing experience based on behavioral signals from customer information, devices and transaction patterns.

Why Xceed AI FRAML?

The Xceed customer base currently has over 400 financial institutions, neo banks, fintechs and BaaS providers, monitoring more than 10 billion banking activities per year.

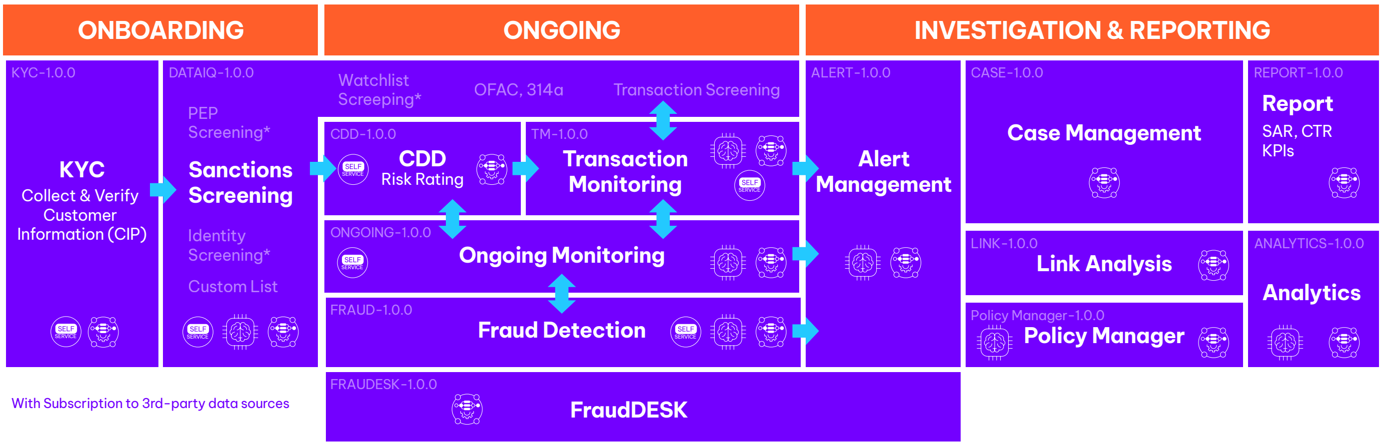


Xceed helps its clients save millions in fraud losses daily, while enabling the seamless filing of hundreds of SARs and CTRs to regulatory authorities.

Xceed AI FRAML Solutions Map

This solutions map is the blueprint for building an **agentic financial institution**—where AI agents collaborate with human teams to deliver scalable, adaptive and secure financial services.

Real-Time Fraud Prevention and AML Compliance Solutions Map



Transforming Risk Management

Empowering Financial Institutions with End-to-End Risk Intelligence

Our comprehensive solutions map guides your organization through the transformation to proactive, real time risk management—integrating advanced analytics, AI agents and unified workflows to deliver continuous fraud prevention and AML compliance.

Onboarding: Build Trust from the Start

Our onboarding process begins with a flexible KYC questionnaire, enabling tailored KYC/KYB for each industry and customer type. It includes advanced fuzzy logic matching to effectively filter watchlists. Sanctions screening is powered by automatic refreshes from the opensanctions.org list, with the option to integrate third-party sanctions lists. Regulatory list updates for 314a are supported, along with the ability to incorporate 314b integration.

- **Flexible KYC**
  Seamless customer identity verification tailored to your risk appetite
- **Watchlist Screening**
  Real-time checks against PEPs, OFAC and adverse media
- **Customer Risk Rating**
  Intelligent scoring to assess and segment risk profiles from day one

Ongoing Monitoring: Stay Ahead of Emerging Threats

Unified Fraud and AML (FRAML) risk monitoring delivers continuous customer risk ratings, integrated with CDD/EDD, and includes unique real-time inline OFAC screening.

Comprehensive Transaction Monitoring: The platform supports scenarios with easy-to-configure, low code rules and policies for rapid deployment. It delivers real-time digital banking fraud prevention through purpose-built AI behavioral analytics for both online and mobile retail and business channels. The system enables real-time intervention across major digital banking platforms, with options to integrate device behavioral fingerprint analytics for enhanced precision. It also provides comprehensive, real-time fraud prevention across digital and payment channels, including Check Fraud, Check Image Analytics, Wire, ACH ODFI, ACH RDFI, P2P Zelle, TCH RTP and FedNOW.

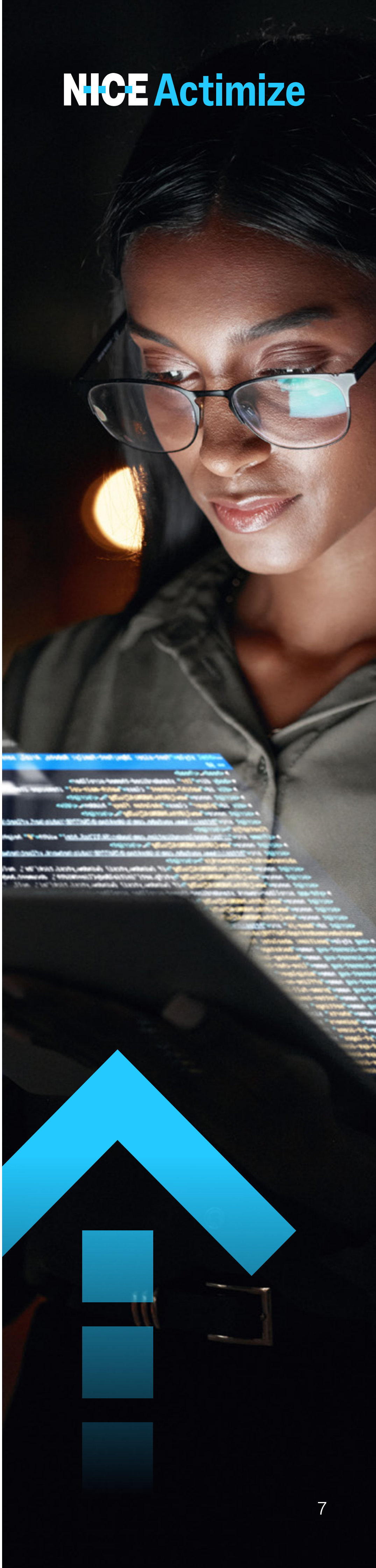
- **Sanctions Screening**
  Inline OFAC checks for real-time compliance
- **Custom Transaction Risk Monitoring**
  Monitor transactions with tailored rules and thresholds
- **Open Sanctions Integration**
  Leverage third-party data for enhanced fraud detection across retail and business banking
- **314a/314b Compliance**
  Strengthen payment fraud defenses across ACH, wire, check and card networks

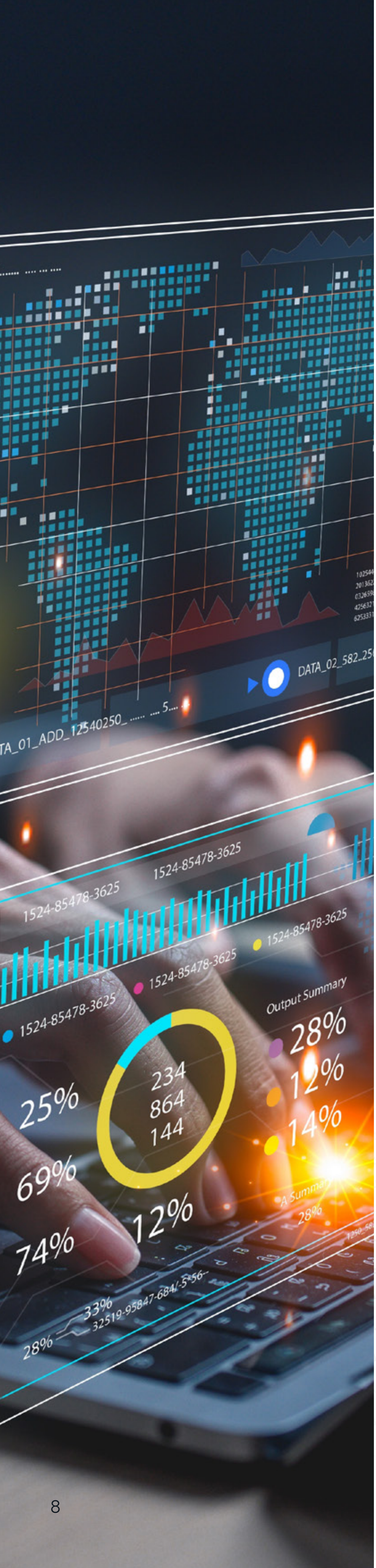
---

Smarter, Faster, Unified Decisioning

The solution's modern UI is designed to be insightful-at-any-scale and enable follow-the-money at transaction speed. It features a powerful FRAML alert workbench and case management system, supported by AI agents that generate case summaries and SAR narratives. Filing and managing SARs and CTRs is streamlined, including automated CTR aggregation for regulatory compliance.

- **Cross-Channel Visual Analytics**
  - Interactive map visualizations
  - Link analysis for networked risk
  - Alert and case management
  - Workflow and policy orchestration
- **Unified Risk Scoring**
  Centralized alerting and filtering for consistent decision-making
- **Quality Control and Regulatory Filings**
  Ensure accuracy and audit-readiness across all compliance outputs





From Insight to Action with Analytics

Access advanced analytics tools with over 20 out-of-the-box reports, along with the flexibility to create custom reports and dashboards. Our analytics are supercharged with AI Agents Smart Segmentation and Model Validation Readiness Report, as well as Data Intake Audit Reporting.

- **Regulatory, Audit Reporting**
  Comprehensive, automated reporting for internal and external stakeholders
- **Advanced Analytics**
  - Descriptive: Understand what happened
  - Predictive: Anticipate future risks
  - Prescriptive: Recommend optimal actions
- **Smart Segmentation**
  AI-driven entity grouping and dynamic alert calibration
- **Model Validation Ready**
  Built-in support for third-party validation and model governance

Infrastructure and Intelligence

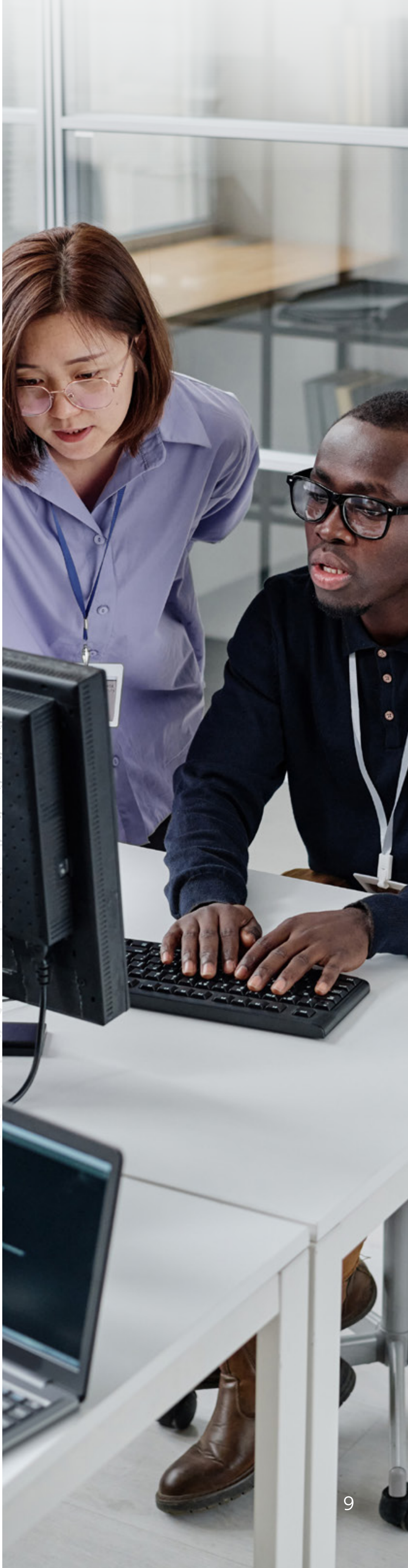
Xceed is a highly scalable native cloud platform built on a modern technology stack, including NoSQL, MongoDB and Graph Database. It supports elastic scaling and offers extensive cloud storage expansion. The platform is powered by an ensemble of battle-tested AI models deployed across hundreds of financial institutions. These models are augmented by secure AI agents operating with human-in-the-loop oversight, enabling Fraud and AML analyst teams to combat financial crime efficiently with a single source of truth and collaborative investigation.

Xceed AI FRAML supports over 65 payment processors connectors and integrates with all major core connectors to accelerate deployment and time-to-value.

- **Unified Alert and Case Management**
  Centralized "Evidence Lake" for a single source of truth
- **Risk Controls**
  High availability, disaster recovery (DR) and SOC2 compliance
- **FraudDESK and AMLDesk with AI Agents**
  Augment human expertise with intelligent automation
- **Connectors and APIs**
  Seamless integration with your existing ecosystem

Trusted Network Risk Xchange

The **Xceed Trusted Network Risk Xchange** is a **secure multi-party risk exchange** framework designed to enable collaborative financial crime investigations while preserving data privacy. It leverages **Secure Multi-Party Computation (MPC)** to allow multiple institutions—such as banks, regulators and financial service providers—to share and analyze sensitive risk intelligence without exposing underlying data.



How It Works

Risk Monitoring At-Transactions Speed
As instant payments become pervasive across both retail and business banking, it is essential for Frontier Financial Institutions to observe user and device digital behavior, as well as transactions patterns, in real time. The ability to infer risk at the moment these events occur is critical for institutions looking to embrace digital payments, virtual currencies or partnerships with fintechs.

Screening-In-Real-time
From account opening during onboarding to continuous CDD and transaction monitoring, the solution allows institutions to screen individual or business entities in real-time. This includes identifying sanctions exposure and detecting risky transactions that may indicate fraud or trigger the need for SAR filings.

Act-in-Real-time
Detect fraud and/or money laundering events "as-they-come" and intervene with "Friction Right Policy" in real-time. AI agents operating 24x7x365 can interdict and hold suspicious activity for review by human analysts during business banking hours. This continuous collaboration defines the workforce 2.0 model of a Frontier Financial Institution.

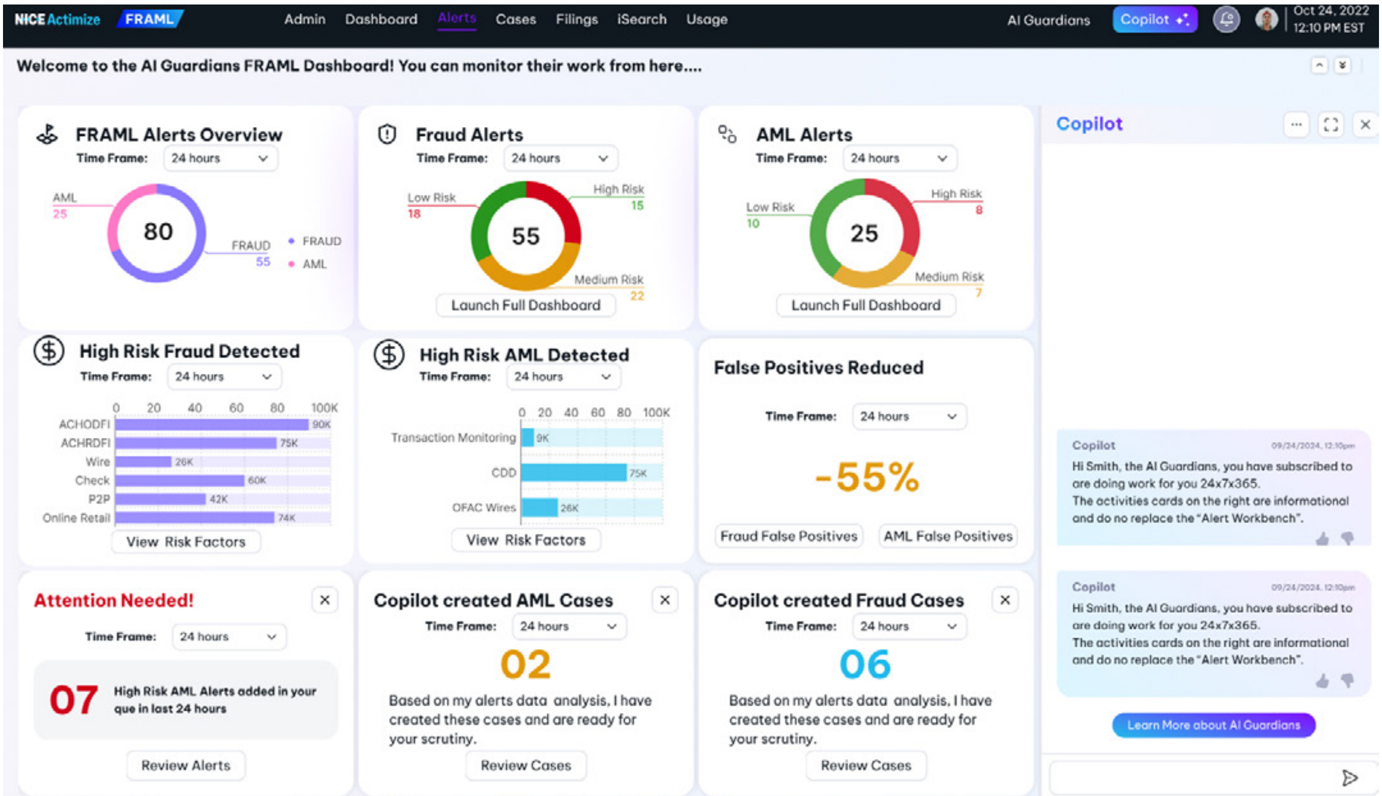
Secure Multi-Party Computation (MPC)
MPC enables multiple parties to jointly compute risk models or investigate suspicious activities without revealing their private data to each other. This cryptographic technique ensures that data remains encrypted and confidential throughout the process, even during analysis.

Privacy-Preserving Collaboration
Institutions can collaborate on fraud detection and AML investigations across organizational boundaries. Sensitive customer or transaction data is never exposed, ensuring compliance with GDPR, SOC2 and other privacy regulations

Real-Time Risk Intelligence Sharing
Participants in the network can exchange risk signals, alerts and assessments in real time with each other. This creates a network effect, where each additional participant strengthens collective intelligence and improves detection capabilities.

AI-powered agents and desks (e.g., FraudDESK, AMLDESK)
AI-powered agents and desks assist in orchestrating investigations across institutions. These agents can triage alerts, correlate cross-entity risks and recommend actions while maintaining strict data boundaries. Data is maintained in the country of residence, avoiding offshoring risks as key activities are performed in a fully SOC2, secure cloud environment.

Copilot and Multi-Agents AI Risk Monitoring



A Smarter Path to Frontier Financial Firm

In an era of accelerating risk and regulatory complexity, financial institutions must evolve beyond traditional compliance. Xceed AI FRAML offers a strategic blueprint for building a real-time, agentic risk management ecosystem—where AI agents and human expertise work in harmony to detect threats, ensure compliance and deliver trust at scale.

By embracing unified data, intelligent automation and adaptive analytics, your organization can become a Frontier Financial Institution—one that's not only resilient, but ready to lead in the future of finance.

→ Accelerate Your FRAML Strategy Today

NICE Actimize

Know more. Risk less.

info@niceactimize.com
niceactimize.com/blog
@NICE_actimize
/company/actimize
NICEactimize

About NICE Actimize

As a global leader in artificial intelligence, platform services and cloud solutions, NICE Actimize excels in preventing fraud, detecting financial crime and supporting regulatory compliance. Over 1,000 organizations across more than 70 countries trust NICE Actimize to protect their institutions and safeguard assets throughout the entire customer lifecycle. With NICE Actimize, customers gain deeper insights and mitigate risks. Learn more at **www.niceactimize.com**.