

June 2025



Leading 50™

Financial Crime and Compliance (FCC) Technology Providers 2025



Like F1 cars, financial institutions need precision technology to outpace financial crime

In the fast-paced world of financial services, the battle against financial crime unfolds like a thrilling Formula 1 race, where financial institutions, including banks, FinTech firms, asset managers, payment processors, insurance companies, and brokerage firms, compete as elite racing teams. They strive relentlessly to secure pole position in regulatory compliance, customer trust, and operational efficiency. The track they navigate is fraught with perilous challenges posed by sophisticated financial criminals engaged in money laundering, fraud, terrorist financing, and sanctions violations, constantly adapting tactics and exploiting digital vulnerabilities.

Legacy compliance systems, reminiscent of outdated racing vehicles, struggle to manage the demanding conditions of this complex racecourse. Key challenges include customer lifecycle inefficiencies, such as cumbersome onboarding and periodic due diligence processes; limitations in screening and monitoring, leading to delayed and inaccurate transaction checks; inadequacies in fraud detection methods, resulting in ineffective fraud prevention; heightened risks of regulatory noncompliance, increasing exposure to penalties and sanctions; and operational and reputational vulnerabilities due to inflexibility in adapting quickly to emerging threats.

Enter the FCC technology providers – expert engineers dedicated to equipping racing teams with advanced performance enhancements. These providers design innovative solutions to automate and streamline compliance operations, significantly reducing manual interventions and human errors. They deploy sophisticated AI systems that proactively identify suspicious patterns and predict potential threats, enhancing predictive agility and responsiveness.

ML algorithms refine transaction monitoring processes by continuously learning from historical data to accurately pinpoint anomalies and reduce false positives. Real-time analytics offer strategic insights, enabling rapid decision-making and dynamic risk mitigation in volatile compliance scenarios. By integrating seamlessly with institutions' existing infrastructure, FCC technology providers facilitate agile adaptations to regulatory changes, ensuring continuous compliance and operational resilience.

As regulatory complexities intensify and financial crime threats evolve rapidly, collaboration between financial institutions and FCC technology providers has become more important than ever. Historically, institutions have struggled with internal capability gaps, resource limitations, and the accelerated pace of technology advances, making it difficult to independently manage increasingly sophisticated financial crimes. This dynamic partnership ensures institutions stay ahead of competitors and confidently cross the finish line ahead of financial criminals, reinforcing trust and security across the global financial ecosystem.

Yet, a vital question remains: Can legacy compliance systems keep pace with today's escalating demands for robust regulatory adherence, operational agility, and growth, or will they fall behind like outdated racing cars struggling to compete? The industry stands at the brink of a transformative era, akin to a pivotal racing moment where precision, speed, and adaptability become indispensable. Modern, intelligent compliance platforms are no longer optional but essential, offering cutting-edge capabilities required to dominate the challenging regulatory track. Institutions must now decide whether to continue making incremental upgrades to legacy systems or fully embrace next-generation FCC solutions designed to confidently accelerate them into the future.

This report explores leading FCC technology providers, their key offerings, and the important trends shaping the industry's modernization journey.

Contents

- 05 Background, research methodology, and scope of research
- 08 Everest Group Leading 50™ Financial Crime and Compliance Technology Providers
- 14 Evolving trends and key drivers transforming FCC
- 17 Geographical distribution of Leading 50™ FCC providers
- 18 Compliance technology deal insights
- 20 Everest Group recognitions for key FCC technology providers
- 23 Transforming FCC technology through industry cloud partnerships, driving innovation, agility, and scalability
- 24 Leveraging generative AI in FCC technology solutions
- 26 Key investors shaping the FCC landscape
- 27 The role of System Integrators (SIs) and advisory firms in FCC technology adoption
- 28 Implications for FCC technology providers
- 29 Building a resilient FCC strategy: the TRUST framework for enterprises

WHAT

is the Everest Group Leading 50™ Financial Crime and Compliance (FCC) Technology Providers research?

The Everest Group Leading 50™ Financial Crime and Compliance (FCC) Technology Providers is a global ranking of the leading technology providers specializing in solutions that combat financial crime and ensure regulatory compliance across the financial services industry. The list is based on multiple objective parameters, including:

Scale and growth momentum: evaluates providers' revenue generated specifically from FCC technology solutions, along with indicators of business growth such as market expansion, client traction, and external investment momentum

Value-chain coverage: evaluates providers' solution breadth across the FCC value-chain functions comprising Know Your Customer (KYC), Anti-money Laundering (AML), fraud and chargeback, business intelligence and reporting, and horizontal capabilities across AI, ML, automation, platforms, and analytics

Innovation and investment: analyzes providers' innovation capabilities, focusing on cloud-readiness, strategic partnerships, horizontal and vertical AI and ML solutions

Client geographic coverage: assesses providers' global reach across regions such as North America (NA), the UK, Continental Europe (CE), Middle East and Africa (MEA), and Asia Pacific (APAC), and client mix by buyer types such as banks, capital markets, hi-tech and entertainment, and payment enterprises

In addition to this evaluation, Everest Group recognizes select FCC providers in most actively sought-after technology segments for enterprises. Recognition is based on publicly available data, investor announcements, and provider press releases and inputs, ensuring a comprehensive and objective evaluation. We have categorized these recognitions into eight areas:

- Digital identity solutions
- Modernizing transaction monitoring systems
- Trade-finance compliance
- Unified fraud and AML systems
- Crypto and blockchain compliance
- Transaction and payment screening solutions
- AI/ML in compliance
- Risk intelligence in FCC

Note to banks and enterprises: This list is intended to serve as a starting point to build your own list of potential technology suppliers in specific sub-segments. It is important to note that the ranking is not an assessment of these firms' capabilities, but rather an ordered list based on revenue, off-the-shelf coverage, and recent investments to bolster their coverage; for details, we have provided information on how the list is constructed on the next page. For a more comprehensive understanding of their capabilities and a holistic analysis of these providers, please contact our analyst team and refer to specific [Everest Group PEAK Matrix assessment reports](#).

WHY

the Everest Group Leading 50™ Financial Crime and Compliance (FCC) Technology Providers research?

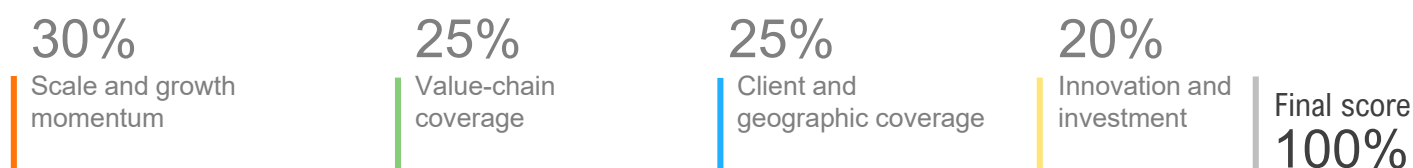
This report provides an objective and detailed analysis of the FCC technology landscape, helping financial institutions identify leading providers and evaluate their functional strengths. It serves as a valuable benchmarking resource for technology providers and offers insights for institutions seeking innovative FCC solutions. In addition, this report helps System Integrator (SI) service providers by providing guidance on industry-specific partnerships to build more robust value propositions for enterprises. Everest Group ranks the providers as leading performers, which is not a comparative capability analysis but a factual representation of these providers' business performance, geographical reach, and innovation focus.

HOW

is the Everest Group Leading 50™ Financial Crime and Compliance (FCC) Technology Providers determined?

The analysis began with over 200 FCC technology providers and following a comprehensive evaluation, we shortlisted the Leading 50 Providers:

- **Qualification criteria:** companies with dedicated FCC technology platforms/solutions to serve enterprises with a special focus on financial institutions
- **Rank determination:** technology providers ranked based on a weighted composite score across four key parameters – scale and growth momentum, value-chain coverage, client and geographic coverage, and innovation and investment; the respective weights across these four parameters are presented below:



KEY

information sources for this report

We used multiple information sources in our analysis:

- **Proprietary data:** information sourced directly from technology providers, coupled with Everest Group's proprietary analysis and database of FCC technology providers
- **Publicly available data:** reported revenue and coverage based on public sources such as listed firms' annual filings and/or providers' press releases; in cases where providers did not disclose information publicly, we relied on publicly available data from external sources

Scope of the research

FCC value-chain scope

KYC	AML	Fraud management and chargeback	Business intelligence and reporting
-----	-----	---------------------------------	-------------------------------------

Everest Group's view of the FCC value chain

[NOT EXHAUSTIVE]



KYC



AML


**Fraud
management
and chargeback**

**Business
intelligence
and reporting**

Onboarding / Trigger-based refresh

Enhanced Due Diligence (EDD)

Monitoring

Reporting

Document management	Sanctions list screening	Suspicious Activity Monitoring (SAM)	Suspicious Activity Report (SAR) / Unusual Activity Report (UAR)	Check tampering	Internal audits
Onboarding platform	Watch list screening	Transaction lookback and cash flow monitoring	Currency Transaction Report (CTR)	Anti-bribery and corruption	Network analysis
Data profiling	Politically Exposed Person (PEP) screening	Alert and case management	Terrorist property/financing reporting	Fraud detection and recovery management	Navigation and link analysis
Customer Identification Program (CIP)	Adverse media screening	Ongoing screening	314a and 314b data requests/sharing	Identity theft detection	GRC control checks
General profile and negative news search	Office of Foreign Assets Control (OFAC) screening	Suspicious Designated Nationalist (SDN) screening	Subpoena support	Payment screening	Risk assessment and mitigation
Customer refresh	External data checks	AML monitoring for Money Service Businesses (MSB)		Chargeback data and transaction management	
Customer risk assessment	Data stream validation/notification	Trade-based money laundering		Dispute management	
Quality assessment	Entity resolution	Customer risk scoring		Model validation and refinement	
Behavioral analysis				Blockchain and analytics	

Platforms (including customer lifecycle management)

Analytics | AI | Automation

Geography scope



Everest Group Leading 50™ Financial Crime and Compliance Technology Providers 2025 (page 1 of 2)

Rank	Technology Provider	HQ	Final score
1	LexisNexis Risk Solutions	US	90.30
2	NICE Actimize	US	88.54
3	Quantexa	UK	74.94
4	Fenergo	Ireland	73.66
5	WorkFusion	US	73.18
6	Oracle Financial Crime and Compliance Management	US	70.84
7	LSEG Risk Intelligence	UK	69.01
8	SymphonyAI	US	64.16
9	GBG	UK	62.68
10	Tookitaki	Singapore	62.43
11	Signzy	India	61.66
12	Moody's	US	61.54
13	ComplyAdvantage	UK	61.49
14	Jumio	US	60.29
15	Napier AI	UK	59.68
16	Featurespace*	UK	58.14
17	Feedzai	Portugal	55.68
18	ThetaRay	Israel	55.43
19	Nasdaq Verafin	Canada	55.26
20	Lucinity	Iceland	55.01
21	Onfido	UK	53.76
22	Dow Jones Risk & Compliance	US	52.01
23	Unit21	US	51.38
24	Trulioo	Canada	51.24
25	Appian	US	50.88

*Note: Featurespace, following its acquisition by Visa in December 2024, is now a Visa solution

Everest Group Leading 50™ Financial Crime and Compliance Technology Providers 2025 (page 2 of 2)

Rank	Technology Provider	HQ	Final score
26	Incode	US	48.99
27	BigId	US	48.88
28	Bureau	US	48.68
29	Cleareye.ai	US	48.58
30	Eastnets	UAE	47.66
31	Socure	US	47.24
32	Sumsub	Cyprus	46.99
33	Mitek Systems	US	46.98
34	Kharon	US	46.58
35	Elliptic	UK	46.46
36	Xapien	UK	46.39
37	IMTF	Switzerland	45.76
38	Fincom.co	Israel	44.61
39	Flagright	Germany	44.34
40	Forter	US	43.96
41	SmartKYC	UK	43.93
42	Encompass	UK	43.68
43	Rzolut	Singapore	43.48
44	Facctum	UK	43.11
45	Hawk	Germany	42.61
46	AP Solutions IO	France	41.78
47	Fraud Finder	UK	41.48
48	Alertspeed	US	40.46
49	Salv	Estonia	40.13
50	Acuminor	Sweden	40.06

Coverage across key geographies and buyer type (page 1 of 2)

Rank	Technology Provider	Client geography coverage						Buyer type				
		NA	LATAM	UK	CE	APAC	MEA	Banks	Payment	Capital markets	Hi-tech and entertainment	Others
1	LexisNexis Risk Solutions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	NICE Actimize	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Quantexa	✓		✓	✓	✓	✓	✓		✓		✓
4	Fenergo	✓		✓	✓	✓	✓	✓	✓	✓		✓
5	WorkFusion	✓		✓	✓	✓	✓	✓	✓	✓	✓	
6	Oracle Financial Crime and Compliance Management	✓	✓	✓	✓	✓	✓	✓	✓			✓
7	LSEG Risk Intelligence	✓		✓	✓	✓	✓	✓	✓	✓		✓
8	SymphonyAI	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
9	GBG	✓		✓	✓	✓		✓	✓	✓	✓	✓
10	Tookitaki	✓	✓			✓	✓	✓	✓	✓		✓
11	Signzy	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓
12	Moody's	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
13	ComplyAdvantage	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
14	Jumio	✓	✓		✓		✓	✓	✓	✓	✓	✓
15	Napier AI	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
16	Featurespace*	✓	✓	✓	✓	✓	✓	✓	✓		✓	
17	Feedzai	✓		✓	✓	✓		✓	✓	✓		✓
18	ThetaRay	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
19	Nasdaq Verafin	✓		✓				✓	✓			✓
20	Lucinity	✓		✓	✓	✓		✓	✓	✓		
21	Onfido	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
22	Dow Jones Risk & Compliance	✓	✓	✓	✓	✓	✓	✓	✓			✓
23	Unit21	✓				✓		✓	✓	✓	✓	✓
24	Trulioo	✓			✓	✓		✓	✓	✓	✓	✓
25	Appian	✓		✓	✓	✓		✓	✓	✓		✓

*Note: Featurespace, following its acquisition by Visa in December 2024, is now a Visa solution

Coverage across key geographies and buyer type (page 2 of 2)

Rank	Technology Provider	Client geography coverage						Buyer type				
		NA	LATAM	UK	CE	APAC	MEA	Banks	Payment	Capital markets	Hi-tech and entertainment	Others
26	Incode	✓			✓	✓		✓	✓	✓	✓	✓
27	BigId	✓		✓	✓			✓	✓	✓	✓	✓
28	Bureau	✓				✓	✓	✓	✓	✓	✓	✓
29	Cleareye.ai	✓		✓	✓	✓	✓	✓				✓
30	Eastnets	✓		✓	✓	✓	✓	✓	✓	✓		✓
31	Socure	✓						✓	✓	✓	✓	✓
32	Sumsub	✓		✓	✓	✓		✓	✓	✓	✓	
33	Mitek Systems	✓		✓	✓			✓	✓	✓	✓	
34	Kharon	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
35	Elliptic	✓	✓	✓		✓		✓	✓			✓
36	Xapien	✓		✓	✓	✓	✓			✓	✓	✓
37	IMTF				✓	✓	✓	✓	✓	✓		✓
38	Fincom.co	✓		✓	✓		✓	✓	✓	✓	✓	✓
39	Flagright	✓		✓	✓	✓	✓	✓	✓	✓		
40	Forter	✓		✓	✓	✓			✓		✓	
41	SmartKYC	✓	✓	✓	✓	✓	✓	✓		✓		✓
42	Encompass	✓		✓	✓	✓		✓	✓	✓		✓
43	Rzolut	✓		✓		✓	✓	✓	✓	✓	✓	✓
44	Facctum			✓	✓		✓	✓	✓	✓	✓	✓
45	Hawk	✓		✓	✓	✓	✓	✓	✓			✓
46	AP Solutions IO			✓	✓		✓	✓	✓	✓		✓
47	Fraud Finder	✓		✓	✓			✓	✓			✓
48	Alertspeed	✓		✓	✓		✓	✓	✓	✓	✓	
49	Salv			✓	✓			✓	✓	✓	✓	
50	Acuminor	✓		✓	✓	✓	✓	✓	✓	✓		✓

Coverage across key LoBs (page 1 of 2)

Rank	Technology Provider	KYC					AML			Fraud and chargeback		BI and reporting	
		EDD	Perpetual KYC	Digital onboarding	Entity resolution	KYB	Name/Watchlist screening	Payment screening	Transaction monitoring	Fraud	Chargeback	Regulatory reporting	Risk assessment and threat mitigation
1	LexisNexis Risk Solutions	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓
2	NICE Actimize	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
3	Quantexa	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓
4	Fenergo	✓	✓	✓		✓	✓	✓	✓			✓	✓
5	WorkFusion	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
6	Oracle Financial Crime and Compliance Management	✓		✓		✓	✓	✓	✓	✓			✓
7	LSEG Risk Intelligence	✓	✓	✓		✓	✓	✓	✓	✓			✓
8	SymphonyAI	✓	✓				✓	✓	✓	✓		✓	✓
9	GBG	✓		✓	✓	✓	✓	✓	✓	✓		✓	✓
10	Tookitaki	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
11	Signzy	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
12	Moody's	✓		✓	✓	✓	✓					✓	✓
13	ComplyAdvantage	✓	✓				✓	✓	✓			✓	✓
14	Jumio	✓		✓			✓	✓	✓	✓		✓	✓
15	Napier AI	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
16	Featurespace*							✓		✓		✓	✓
17	Feedzai						✓	✓	✓	✓		✓	✓
18	ThetaRay						✓	✓	✓				✓
19	Nasdaq Verafin	✓			✓	✓	✓	✓	✓	✓		✓	✓
20	Lucinity	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓
21	Onfido	✓		✓			✓						✓
22	Dow Jones Risk & Compliance	✓				✓	✓	✓					✓
23	Unit21	✓				✓	✓	✓	✓	✓		✓	✓
24	Trulioo	✓		✓		✓	✓						✓
25	Appian	✓		✓			✓		✓				✓

*Note: Featurespace, following its acquisition by Visa in December 2024, is now a Visa solution

Coverage across key LoBs (page 2 of 2)

Rank	Technology Provider	KYC					AML			Fraud and chargeback		BI and reporting	
		EDD	Perpetual KYC	Digital onboarding	Entity resolution	KYB	Name/Watchlist screening	Payment screening	Transaction monitoring	Fraud	Chargeback	Regulatory reporting	Risk assessment and threat mitigation
26	Incode	✓		✓		✓	✓			✓			✓
27	BigId				✓								✓
28	Bureau	✓	✓	✓	✓	✓	✓		✓	✓			✓
29	Cleareye.ai	✓				✓	✓		✓	✓		✓	✓
30	Eastnets	✓			✓		✓	✓	✓	✓		✓	✓
31	Socure	✓		✓	✓	✓	✓						
32	Sumsub	✓		✓		✓	✓			✓			✓
33	Mitek Systems	✓		✓		✓	✓			✓			✓
34	Kharon	✓	✓		✓	✓	✓	✓	✓			✓	✓
35	Elliptic	✓			✓		✓	✓	✓				✓
36	Xapien	✓	✓	✓	✓	✓	✓						✓
37	IMTF	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
38	Fincom.co	✓	✓		✓	✓	✓	✓		✓		✓	
39	Flagright	✓	✓				✓	✓	✓	✓		✓	✓
40	Forter				✓					✓	✓		
41	SmartKYC	✓	✓	✓	✓	✓	✓						
42	Encompass	✓	✓	✓	✓	✓	✓						✓
43	Rzolut	✓	✓	✓	✓	✓	✓						✓
44	Facctum	✓				✓	✓	✓	✓				✓
45	Hawk	✓			✓		✓	✓	✓	✓			✓
46	AP Solutions IO	✓	✓			✓	✓	✓	✓	✓			✓
47	Fraud Finder			✓		✓	✓			✓			
48	Alertspeed	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
49	Salv	✓					✓	✓	✓	✓			✓
50	Acuminor	✓	✓			✓			✓	✓			✓

Evolving trends and key drivers transforming FCC

The FCC landscape is undergoing significant transformation, as customer expectations for seamless, secure, and frictionless experiences intensify, driven by the rise of digital channels, faster transactions, and real-time financial services. This shift is further compounded by rapidly evolving financial crime threats and increasingly stringent regulatory requirements. Financial institutions today navigate an increasingly intricate web of global regulations, facing unprecedented scrutiny by regulators intent on enforcing compliance through record-breaking fines. High-profile cases such as the substantial fines against major global banks for AML violations and failure to detect fraud have vividly underscored institutions' reputational, financial, and operational risks. Coupled with the rapid digitization of financial services, increased adoption of digital payments, and the relentless sophistication of financial criminals, these challenges highlight an urgent need for enhanced vigilance and proactive risk management.

As financial crime tactics continue to evolve, the need for compliance modernization through holistic, end-to-end FCC solutions is becoming more pressing. Regulators worldwide are becoming more demanding, pushing institutions to demonstrate greater transparency, adaptability, and proactive compliance capabilities. Modernizing FCC technology through integrated platforms – spanning screening, monitoring, fraud prevention, and reporting – not only mitigates regulatory risks but also streamlines operations, reduces false positives, and enhances customer experience by accelerating onboarding and due diligence procedures. Financial institutions must prioritize investment in intelligent compliance solutions, seamless system integrations, and data-driven risk management to navigate the complexities of modern financial crime. Several key factors are accelerating the transformation of FCC operations:



The shift toward proactive risk management: Financial institutions are moving from reactive compliance models to proactive financial crime prevention. AI-driven risk assessment, predictive analytics, and real-time transaction monitoring are enabling financial institutions to detect and prevent fraudulent activities before they escalate, reducing both financial losses and regulatory scrutiny. AI and ML are increasingly vital in combating financial crime, dramatically improving the efficacy of detection and prevention capabilities.



Increasing regulatory complexity and global coordination: Regulators worldwide are tightening financial crime regulations, requiring institutions to comply with multiple jurisdictional mandates. The introduction of stricter AML, KYC, and other compliance measures is driving financial institutions to adopt automated, scalable compliance solutions. This regulatory complexity and convergence underscore the criticality of adopting flexible, integrated, and agile compliance platforms capable of scaling globally while effectively addressing local regulatory nuances.



Increasing sophistication and scale of financial crimes: Financial criminals continuously adapt their techniques, exploiting vulnerabilities within legacy systems and digital channels. Criminals increasingly use highly sophisticated and coordinated methods, ranging from synthetic identity fraud, advanced phishing attacks, cyber-enabled money laundering schemes, to sophisticated sanctions evasion tactics facilitated by emerging payment methods. Given the scale, speed, and complexity of modern financial crimes, traditional detection methods are insufficient. To effectively counter these sophisticated threats, institutions are adopting advanced threat intelligence platforms, network analytics, and dynamic behavioral analytics to swiftly detect anomalies, track transaction flows, and disrupt illicit activities at scale.



Expansion of digital identity verification and biometrics: Traditional document-based KYC processes are being replaced by biometric authentication, digital ID verification, and decentralized identity solutions. These advances improve customer onboarding efficiency and enhance fraud detection by leveraging facial recognition, fingerprint scans, and real-time identity validation.



Convergence of Fraud and Anti-money Laundering (FRAML): The increasing complexity of financial crimes has accelerated the shift toward integrated FRAML solutions, offering a unified view of customer behavior and risk. FRAML leverages advanced analytics and ML to identify correlations between fraudulent activities and money laundering patterns, significantly improving detection accuracy. By consolidating alerts and streamlining workflows, institutions reduce operational redundancies and enhance responsiveness. As regulators advocate integrated approaches, FRAML has become essential for institutions aiming to effectively detect, disrupt, and mitigate complex financial crimes.



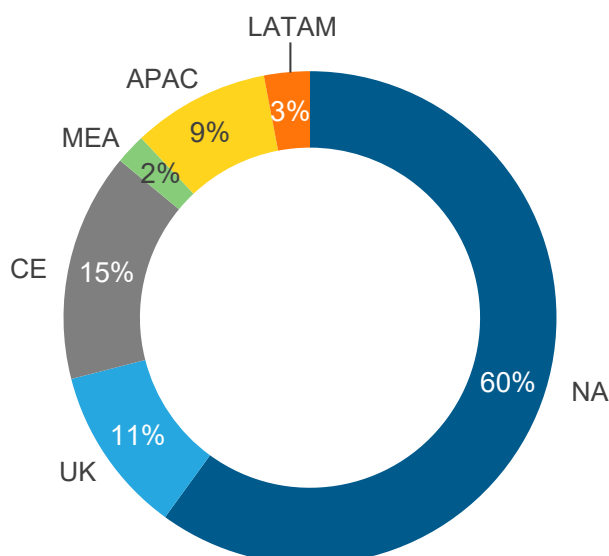
Demand for scalable frameworks and accelerated ecosystem innovation: As financial institutions scale operations and expand their digital presence, there is a growing demand for flexible frameworks that can evolve alongside the business. Institutions increasingly seek modular platforms, pre-integrated ecosystems, and low-/no-code capabilities that reduce time-to-market and simplify solution deployment. This faster ecosystem evolution, supported by API-first architectures and cloud-native foundations, enables quicker onboarding of niche providers, co-innovation with partners, and more agile responses to shifting regulatory and criminal threats.

The rapid evolution of financial crime tactics and compliance requirements is pushing financial institutions to modernize their risk management strategies. As threats become more sophisticated and regulatory expectations increase, the ability to leverage AI, ML, real-time analytics, and cloud-based compliance solutions will be key to ensuring resilience against financial crime. Financial institutions that proactively embrace these advances will not only enhance compliance efficiency but also gain a strategic advantage in an increasingly complex regulatory landscape.

FCC technology

2024; percentage of total market size by geography

100% = US\$20-25 billion



Key market points for each region:

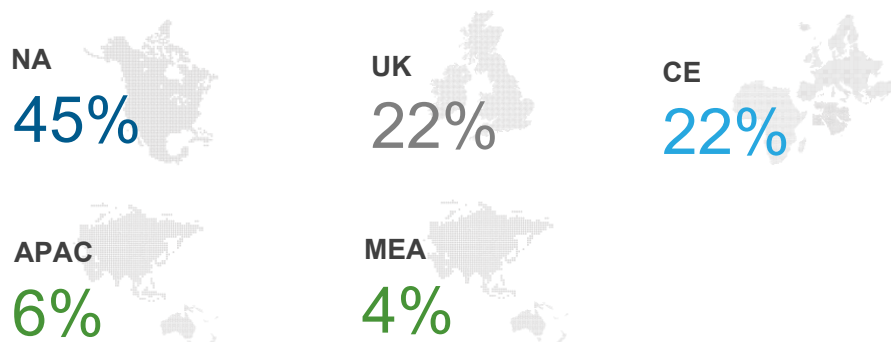
- **NA:** The region's leadership is driven by stringent regulatory requirements, such as the Bank Secrecy Act (BSA), USA PATRIOT Act, and evolving AML frameworks. Large financial institutions and regulatory bodies demand advanced AI-driven transaction monitoring, KYC, and fraud detection solutions. The high adoption of cloud-based, API-driven compliance solutions and a strong presence of global tech leaders contribute to the region's dominance in FCC technology innovation
- **UK:** The UK is a key hub for FCC technology, benefiting from its role as a global financial center. The regulatory landscape, shaped by the Financial Conduct Authority (FCA) and alignment with European Anti-money Laundering Directives (AMLD), has led to significant investments in digital KYC, perpetual compliance monitoring, and transaction screening solutions. Brexit has further intensified compliance needs, with UK firms ensuring regulatory equivalence with EU and global standards. FinTechs and RegTechs in the UK are leading the innovation in AI-powered fraud prevention and digital identity verification
- **CE:** The region is experiencing steady growth in FCC technology adoption, driven by increasing regulatory pressures from the European Commission's AMLD regulations and the establishment of the EU-wide Anti-money Laundering Authority (AMLA). The demand for compliance automation, digital onboarding, and AI-based risk assessments is rising, particularly among banks operating across multiple jurisdictions. Countries such as Germany, France, and the Netherlands are key hubs for RegTech firms, offering advanced compliance and fraud mitigation solutions

- **APAC:** This region remains a developing market for FCC technology, with regional variations in regulatory maturity. The growing presence of international financial hubs such as Singapore, Hong Kong, and Australia is driving the adoption of digital AML, transaction monitoring, and fraud detection solutions. Governments across APAC are enhancing regulatory frameworks to combat cross-border financial crime, leading to increased investment in AI-driven compliance automation
- **MEA:** The region represents a nascent yet growing market for FCC technology. Regulatory modernization efforts, such as the UAE's Financial Action Task Force (FATF) compliance push and Saudi Arabia's Vision 2030 financial reforms, are prompting financial institutions to adopt enhanced compliance solutions. The rise of digital payments and mobile banking in Africa, coupled with the increasing threat of financial fraud, is driving the demand for AML, fraud detection, and biometric KYC solutions. However, cost constraints and infrastructural challenges slow widespread adoption

Geographical distribution of Leading 50™ FCC providers

The global FCC market exhibits a diverse geographical distribution, with FCC providers spread across multiple regions. As regulatory requirements intensify worldwide, enterprises are investing heavily in compliance solutions to mitigate risks and ensure adherence to evolving standards. In this section, we explore the geographical distribution of the leading 50 FCC providers, their headquarters, and the factors influencing market growth. This overview highlights key trends shaping the industry and the dynamics driving adoption in different parts of the world.

Everest Group Leading 50™ FCC Technology Providers by headquarters¹



¹ Distribution by geography is based on the location of the headquarters
Source: Everest Group 2025

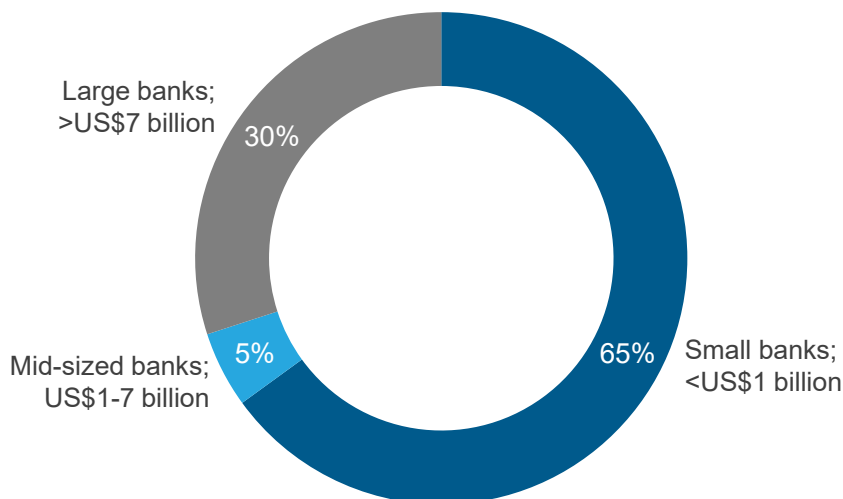
Compliance technology deal insights

Deal distribution by buyer size highlights the dominant role of small banks (less than US\$1 billion in revenue), which account for the largest share at 65%. This suggests that smaller financial institutions are actively investing in FCC solutions, likely driven by increasing regulatory scrutiny and the need to enhance operational resilience. Large banks (more than US\$7 billion in revenue) represent 30% of deals, reflecting their ongoing commitment to strengthening compliance frameworks, often through sophisticated, customized solutions. Mid-sized banks (US\$1-7 billion in revenue) constitute only 5% of deals, indicating either a more cautious investment approach or reliance on existing compliance infrastructure. This distribution underscores how compliance investments are vital across all bank sizes, with smaller banks prioritizing accessible and scalable solutions, while larger institutions continue to enhance their robust compliance ecosystems.

FCC deals by buyer size (revenue)

2022-24; 60+ deals

100% = US\$20-25 billion



Our analysis of recent public FCC technology deals over the past two years has uncovered the following key trends:



AI and ML lead the compliance innovation: AI and ML are central to financial crime prevention, improved fraud detection, anomaly detection, and transaction monitoring. Many providers leverage AI for AML operations, risk assessment, and sanctions screening, enabling financial institutions to respond swiftly to threats. AI-powered self-learning algorithms are improving compliance effectiveness while reducing false positives.



Accelerated adoption of real-time monitoring and sanctions screening:

There is a marked uptick in demand for real-time fraud and AML transaction monitoring, with financial institutions prioritizing instant detection and automated resolution. Notably, recent deals reflect increased investment in real-time sanctions screening to meet tightening global regulatory expectations and reduce the risk of compliance breaches.



Growing focus on digital identity verification and KYC compliance: With the rise in digital banking and remote onboarding, financial institutions demand robust identity verification solutions. Various companies are leading investments in AI-driven KYC, biometric authentication, and document verification. Perpetual KYC and real-time onboarding solutions are becoming the new standard in compliance and fraud prevention.



Expansion of FCC technology in global markets: FCC is a global challenge, with providers expanding into new regions through partnerships. Institutions in different parts of the world are seeking region-specific compliance solutions to address local regulatory requirements while ensuring global financial integrity. As compliance regulations continue to evolve, financial institutions are turning to technology providers that can offer tailored solutions for specific markets.

Everest Group recognitions for key FCC technology providers (page 1 of 3)

1

Digital identity solutions

This category explores providers delivering comprehensive digital identity solutions that enhance security protocols and compliance measures within financial ecosystems. It emphasizes the vital role of secure digital identities in mitigating identity theft and fraud, especially in an era of increasing digital transactions. Innovations in this space streamline identity verification processes and integrate with broader financial crime prevention frameworks, thereby reinforcing trust and security across financial platforms.

2

Modernizing transaction monitoring systems

This category highlights providers with a strong focus on enhancing AML transaction monitoring using AI and ML. These providers apply advanced models to detect complex typologies, improve alert precision, and reduce false positives. As financial crime grows in scale and sophistication, AI-/ML-led transaction monitoring has become a key differentiator for compliance effectiveness and efficiency.

3

Trade-finance compliance

Focuses on technology providers offering specialized solutions that strengthen defenses against trade-based money laundering. This segment is significant due to the complexity and volume of global trade, which presents unique challenges and vulnerabilities in financial security. Providers enhance transaction monitoring and use complex data analysis to mitigate risks, thus ensuring compliance with international trade regulations and AML laws.

Note: The logos are arranged in alphabetical order for each recognition category.

Everest Group recognitions for key FCC technology providers (page 2 of 3)

4

Unified fraud and AML systems

Recognizes providers that integrate fraud detection and AML processes into a single streamlined system. This recognition is important as it underscores the synergy between fraud and AML processes, which enhances the overall effectiveness of financial crime prevention. Combined data insights and predictive analytics significantly elevate institutional risk management strategies and operational efficiency.

5

Crypto and blockchain compliance

Details how technology providers serve cryptocurrency firms by offering regulatory compliance solutions tailored to the unique challenges of digital currency transactions. This category highlights the increasing importance of establishing robust compliance frameworks as cryptocurrencies become mainstream, ensuring that blockchain transactions are secure, transparent, and in line with financial regulations to prevent money laundering and fraud.

6

AI/ML in compliance

Depicts providers that are leading AI/ML integration into financial crime technology systems. This category is important as AI/ML technologies transform the landscape of financial crime detection by predicting and adapting to evolving fraud patterns with unprecedented accuracy and speed. It covers the implementation of AI-driven models that enhance the ability of financial institutions to address potential threats and adapt to dynamic regulatory demands preemptively.

Note: The logos are arranged in alphabetical order for each recognition category.

Everest Group recognitions for key FCC technology providers (page 3 of 3)

7

Transaction and payment screening solutions

This category highlights the importance of technology solutions that screen payments and transactions for financial crimes. Using advanced algorithms and ML, these systems detect signs of illicit activities efficiently, ensuring compliance with regulatory standards. They minimize false positives and maintain transaction integrity, enhancing both security and operational efficiency for financial institutions.



8

Risk intelligence in FCC

This category recognizes providers that deliver actionable risk insights to enhance FCC programs. Their solutions help institutions proactively identify and assess external risks – such as sanctions evasion, illicit networks, geopolitical exposures, typology shifts, and credit risks – through proprietary data intelligence. By embedding risk intelligence into workflows, they enable smarter detection, decision-making, and response.



Note: The logos are arranged in alphabetical order for each recognition category.

Transforming FCC technology through industry cloud partnerships, driving innovation, agility, and scalability

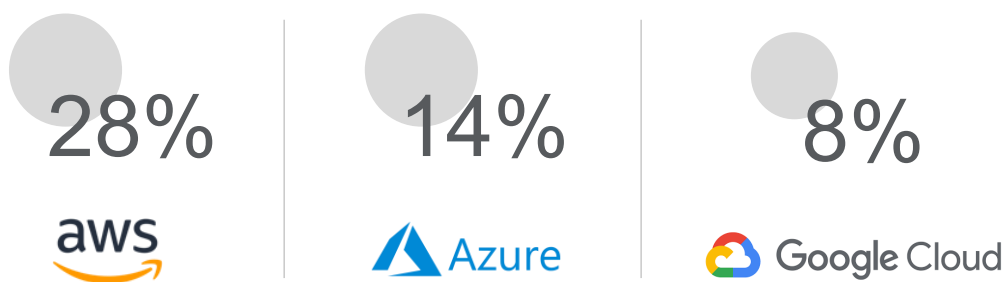
Industry cloud partnerships have emerged as a key enabler for FCC technology, leveraging the capabilities of hyperscalers such as Amazon Web Services (AWS), Microsoft Azure, and Google Cloud Platform (GCP). These collaborations facilitate the rapid deployment of cloud-based compliance solutions, offering financial institutions scalable and efficient tools to combat financial crime.

A key benefit of industry cloud-powered compliance solutions is their ability to deliver real-time monitoring, advanced analytics, and AI-driven risk detection. Cloud infrastructure allows compliance providers to integrate and analyze vast amounts of transactional data, improving fraud detection and AML capabilities. Additionally, industry clouds enhance regulatory compliance by providing secure, globally accessible environments.

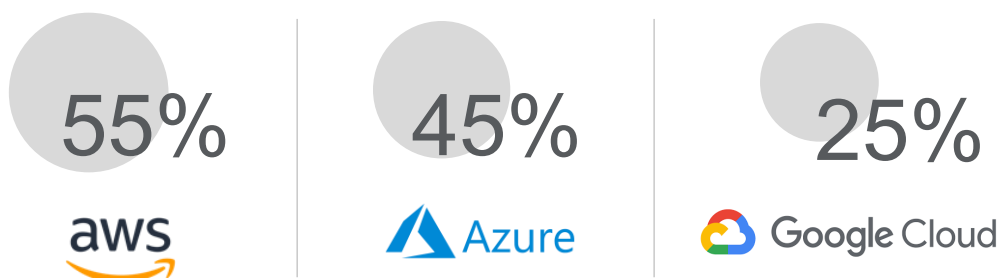
As financial crime threats grow in complexity, financial institutions are increasingly turning to cloud-based compliance solutions to stay ahead. The scalability, agility, and security of industry cloud platforms will continue to drive the adoption of FCC technology, reinforcing the industry's shift toward cloud-native, AI-powered risk management solutions.

Presence of the Leading 50™ FCC providers in hyperscalers' industry cloud offerings

Leading 50™ FCC providers are partnering with cloud hyperscalers to join their industry cloud journeys. AWS dominates the scale of partnerships with the Leading 50™ providers.



Leading 20 FCC providers see a high adoption of cloud partnerships.



Leveraging generative AI in FCC technology solutions

Generative AI has the potential to transform FCC operations, enabling institutions to proactively address complex regulatory challenges, automate intricate processes, and significantly enhance decision-making capabilities. Financial institutions and compliance technology providers are increasingly adopting generative AI to innovate and optimize their FCC solutions, driving substantial operational efficiencies and accuracy improvements.

While generative AI adoption remains in its early stages, with limited implementations, initial deployments have focused on enhancing fraud detection, streamlining regulatory reporting, and automating case management. However, concerns around data security, explainability, and regulatory compliance have led to cautious experimentation rather than full-scale adoption.

Use case split by value chain³

The highest number of generative AI applications' use cases developed by technology providers were observed in AML and fraud management.

01		Chargeback 1-3%
02		Screening 17-20%
03		KYC 21-24%
04		Fraud management 27-30%
05		AML monitoring and reporting 27-30%

³ Based on a sample of 50 use cases collected from technology providers

Note: One generative AI application may represent multiple use cases across the value chain

Top use cases for generative AI in FCC

1

Automated case narratives and reporting

Generative AI streamlines the creation of compliance investigation reports, transaction summaries, and Suspicious Activity Reports (SARs) by converting structured and semi-structured data into regulator-ready narratives.

Key benefit: This automation reduces manual workload, minimizes errors, and accelerates submission timelines. By ensuring consistency and standardization, it enhances compliance with regulatory requirements.

2

Real-time alert summarization

Generative AI-driven solutions generate concise, real-time summaries of compliance alerts, enabling analysts to quickly understand and prioritize flagged transactions. By distilling complex alert data into digestible insights, compliance teams can assess risks more efficiently and take immediate action.

Key benefit: This enhances response times, optimizes resource allocation, and improves investigative efficiency. Faster risk assessment reduces exposure to compliance threats and enhances overall security.

3

Enhanced adverse media monitoring

Generative AI-powered adverse media monitoring rapidly analyzes vast amounts of global news, social media, and online content to detect negative information about customers or counterparties.

Key benefit: By proactively identifying compliance risks, these systems enable institutions to escalate issues early and implement mitigation strategies. Real-time monitoring ensures financial organizations stay ahead of emerging threats, maintaining strong risk oversight in dynamic regulatory environments.

4

Entity resolution and data matching

Generative AI automates entity resolution by accurately matching and verifying financial, personal, and transactional data from multiple sources. AI-driven pattern recognition improves the correlation and consolidation of records, strengthening customer due diligence and KYC compliance.

Key benefit: This reduces errors, enhances regulatory adherence, and streamlines onboarding processes. Faster and more accurate data matching improves operational efficiency and risk management.

5

Investigator and compliance officer copilots

AI-powered compliance copilots assist investigators by providing real-time insights, generating case summaries, and visualizing transaction flows. These intelligent assistants recommend investigative steps, assist in risk assessments, and enhance decision-making.

Key benefit: By reducing manual workload and accelerating analysis, compliance teams can achieve faster resolutions. This significantly improves investigative outcomes, operational productivity, and overall compliance effectiveness.

Key investors shaping the FCC landscape

Investment in FCC technology is rapidly growing as financial institutions and regulators prioritize more effective risk management and fraud prevention strategies. Unlike traditional banking technology investments, funding in FCC is being driven by the increasing complexity of financial crimes, the rise of digital fraud, and the need for real-time compliance with evolving regulations.

Funding is primarily allocated to enhancing AI-driven fraud detection, automating regulatory compliance processes, and expanding cloud-based compliance platforms. As financial institutions increasingly shift toward real-time transaction monitoring and predictive risk analytics, investment is fueling the development of next-generation solutions capable of identifying and mitigating financial crime more effectively.

One key area attracting investment is the automation of regulatory reporting and case management. With compliance teams struggling to manage large volumes of alerts and regulatory requirements, funding is flowing into platforms that streamline compliance workflows, reduce manual efforts, and enhance the accuracy of risk assessments. Another major trend is the rise of cross-border compliance solutions, as financial crime is no longer confined to specific jurisdictions. Investors are backing platforms that offer global compliance coverage, integrating multi-regional regulatory frameworks and enabling financial institutions to track and report suspicious transactions across borders efficiently. As cyber threats and financial crime tactics continue to evolve, the demand for proactive threat intelligence is rising. Investors are increasingly supporting companies that specialize in cyber-enabled financial crime prevention, including solutions that detect synthetic identity fraud, deepfake scams, and AI-generated financial fraud schemes.

With regulators tightening enforcement and penalties for noncompliance growing steeper, the FCC sector is expected to remain a high-growth investment opportunity.

Key investors

[NOT EXHAUSTIVE]



JPMORGAN CHASE & CO.

TIGERGLOBAL



WARBURG PINCUS

Key recipients in 2024-25



SAY RI



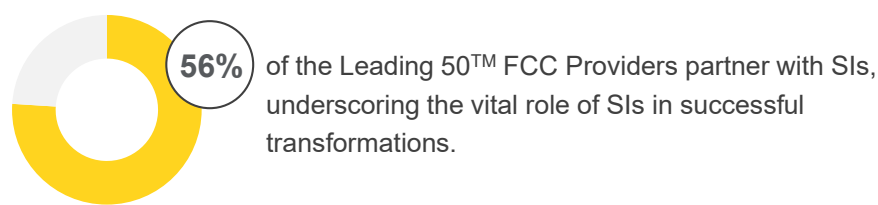
quantexa



The role of SIs and advisory firms in FCC

SIs and advisory firms play pivotal roles in assisting financial institutions to navigate the complexities of FCC. They act as expert partners that design and implement sophisticated FCC solutions, ensuring that platforms work seamlessly within a bank’s or financial institution’s infrastructure.

The role of SIs and advisory firms in FCC continues to evolve in response to emerging financial crime threats and rapid technology advances. SIs serve as the bridge between financial institutions, regulatory bodies, and technology providers, orchestrating end-to-end compliance transformations. By integrating advanced analytics, AI-driven monitoring, and cloud-based compliance platforms, they help organizations modernize their risk management strategies while minimizing operational disruptions.



The proportion of SIs and advisory firms that partner with Everest Group’s Leading 50™ Financial Crime and Compliance (FCC) Technology Providers⁴ is depicted below:

[NOT EXHAUSTIVE]

<10%	10-20%	>20%
Coforge DXC TECHNOLOGY FIS HCLTech LTIMindtree Mphasis The Next Applied NTT DATA WNS Tech Mahindra	Capgemini cognizant IBM Infosys KPMG pwc tcs TATA CONSULTANCY SERVICES wipro	accenture Deloitte. EY

⁴ Based on press releases, provider inputs, and official recognition on partner pages or websites as of March 2025
Source: Everest Group 2025

Meanwhile, advisory firms contribute deep regulatory insights and management consulting expertise that complement SIs' technical implementations. These firms provide strategic oversight, policy advisory, and change management services, ensuring that the financial institutions' compliance transformations are aligned with global compliance standards and are strategically positioned for future scalability and adaptability.

Together, SIs and advisory firms enable financial institutions to navigate complex regulatory landscapes by embedding automated compliance processes that reduce manual oversight and improve reporting accuracy. They offer strategic guidance on optimizing compliance frameworks, streamlining investigation workflows, and improving risk-based decision-making. As the financial crime landscape evolves, the integrated roles of SIs and advisory firms are expected to grow, with increased emphasis on AI-driven compliance, cloud-based risk management, and the integration of data analytics for real-time fraud detection.

Implications for FCC technology providers



Accelerate platform innovation and agility

FCC technology providers must continuously innovate and enhance platform agility to address evolving regulatory complexities and sophisticated criminal behaviors. Emphasizing cloud-native solutions, microservices architectures, and flexible integration capabilities will ensure rapid adaptation to shifting regulatory landscapes and client requirements.



Enhance AI/ML capabilities and explainability

Providers must invest significantly in advanced analytics, AI, and ML solutions, prioritizing model transparency and regulatory explainability. Building solutions that include Explainable AI (XAI), clear audit trails, bias mitigation strategies, and transparent decision-making frameworks will ensure regulatory acceptance and client trust.



Expand integrated FRAML offerings

To address the convergence of fraud prevention and AML activities, providers must develop integrated FRAML solutions that unify data sources, detection mechanisms, and investigative workflows.



Invest in advanced digital identity and verification solutions

Providers must strengthen their capabilities in digital identity verification, biometrics, and decentralized identity management. Solutions that enhance customer onboarding experiences, streamline identity authentication, and proactively mitigate identity-related fraud risks will be increasingly demanded by financial institutions.



Prioritize ecosystem partnerships and collaboration

FCC technology providers must pursue strategic partnerships and ecosystem collaboration with complementary technology firms, hyperscalers, data providers, and SIs. Building and nurturing these collaborations will help providers deliver comprehensive, integrated solutions, expanding market reach and accelerating deployment timelines, ultimately driving greater adoption among financial institutions.

Building a resilient FCC strategy: the TRUST framework for enterprises

FCC's transformation is driven by five key pillars, encapsulated in the TRUST framework: Threat prevention and mitigation, Regulatory adaptability, Unified risk intelligence, Seamless automation, and Technology-driven compliance. These elements highlight both the current shift and the path forward for financial institutions as they strive to meet growing compliance demands while strengthening risk resilience.

T Threat prevention and mitigation

Enterprises must move beyond compliance as a regulatory obligation and focus on proactive risk mitigation. AI-driven behavioral analytics, real-time fraud detection, and advanced network analysis identify suspicious patterns before fraud occurs. Cross-channel risk assessment, deep learning fraud models, and dynamic transaction screening are essential to combat emerging threats such as synthetic identity fraud, money mule activity, and deepfake-enabled scams.

R Regulatory adaptability

With rapidly evolving AML directives and financial crime laws, enterprises need automated compliance systems that dynamically update to new regulations. Traditional rule-based models are insufficient – financial institutions must adopt AI-driven compliance tools that continuously align with global mandates, support perpetual KYC, and automate SAR to ensure seamless regulatory adherence.

U Unified risk intelligence

Financial institutions operate in a highly interconnected ecosystem where risks stem from multiple sources. Enterprises need centralized risk intelligence platforms that consolidate customer data, transaction insights, and external risk feeds into a single compliance ecosystem. This eliminates silos, enhances risk profiling, and allows proactive detection of hidden financial crime networks.

S Seamless automation

Reducing compliance bottlenecks and operational costs requires low-code/no-code automation for KYC, AML screening, and case management. AI-powered automation improves risk assessment, due diligence, and fraud investigations, ensuring faster regulatory reporting. Perpetual KYC, automated alert prioritization, and case workflow enhancements enable institutions to focus resources on high-risk investigations.

T Technology- driven compliance

Enterprises must shift from reactive to proactive financial crime management by leveraging AI, ML, and advanced analytics. Cloud-native, API-driven compliance solutions enable real-time risk assessment and fraud detection while reducing false positives. Integrating AI-powered transaction monitoring, name screening, and anomaly detection enhances accuracy, improves investigative workflows, and strengthens compliance efficiency.

Stay connected

Dallas (Headquarters)
info@everestgrp.com
+1-214-451-3000

Bangalore
india@everestgrp.com
+91-80-61463500

Delhi
india@everestgrp.com
+91-124-496-1000

London
unitedkingdom@everestgrp.com
+44-207-129-1318

Toronto
canada@everestgrp.com
+1-214-451-3000

Website
everestgrp.com

Blog
everestgrp.com/blog

Follow us on



www.everestgrp.com

Everest Group is a leading research firm helping business leaders make confident decisions. We guide clients through today's market challenges and strengthen their strategies by applying contextualized problem-solving to their unique situations. This drives maximized operational and financial performance and transformative experiences. Our deep expertise and tenacious research focused on technology, business processes, and engineering through the lenses of talent, sustainability, and sourcing delivers precise and action-oriented guidance. Find further details and in-depth content at www.everestgrp.com.

Notice and Disclaimers

Important information. Please read this notice carefully and in its entirety. By accessing Everest Group materials, products or services, you agree to Everest Group's Terms of Use.

Everest Group's Terms of Use, available at www.everestgrp.com/terms-of-use, is hereby incorporated by reference as if fully reproduced herein. Parts of the Terms of Use are shown below for convenience only. Please refer to the link above for the full and official version of the Terms of Use.

Everest Group is not registered as an investment adviser or research analyst with the U.S. Securities and Exchange Commission, the Financial Industry Regulation Authority (FINRA), or any state or foreign (non-U.S.) securities regulatory authority. For the avoidance of doubt, Everest Group is not providing any advice concerning securities as defined by the law or any regulatory entity or an analysis of equity securities as defined by the law or any regulatory entity. All properties, assets, materials, products and/or services (including in relation to gen AI) of Everest Group are provided or made available for access on the basis such is for informational purposes only and provided "AS IS" without any warranty of any kind, whether express, implied, or otherwise, including warranties of completeness, accuracy, reliability, noninfringement, adequacy, merchantability or fitness for a particular purpose. All implied warranties are disclaimed to the extent permitted by law. You understand and expressly agree that you assume the entire risk as to your use and any reliance upon such.

Everest Group is not a legal, tax, financial, or investment adviser, and nothing provided by Everest Group is legal, tax, financial, or investment advice. Nothing Everest Group provides is an offer to sell or a solicitation

of an offer to purchase any securities or instruments from any entity. Nothing from Everest Group may be used or relied upon in evaluating the merits of any investment. Do not base any investment decisions, in whole or part, on anything provided by Everest Group.

Everest Group materials, products and/or services represent research opinions or viewpoints, not representations or statements of fact. Accessing, using, or receiving a grant of access to Everest Group materials, products and/or services does not constitute any recommendation by Everest Group to (1) take any action or refrain from taking any action or (2) enter into a particular transaction. Nothing from Everest Group will be relied upon or interpreted as a promise or representation as to past, present, or future performance of a business or a market. The information contained in any Everest Group material, product and/or service is as of the date prepared and Everest Group has no duty or obligation to update or revise the information or documentation.

Everest Group collects data and information from sources it, in its sole discretion, considers reliable. Everest Group may have obtained data or information that appears in its materials, products and/or services from the parties mentioned therein, public sources, or third-party sources, including data and information related to financials, estimates, and/or forecasts. Everest Group is not a certified public accounting firm or an accredited auditor and has not audited financials. Everest Group assumes no responsibility for independently verifying such information.

Companies mentioned in Everest Group materials, products and/or services may be customers of Everest Group or have interacted with Everest Group in some other way, including, without limitation, participating in Everest Group research activities.