

April 2026



Everest Group®

Top 50™

Financial Crime and Compliance (FCC) Technology Providers 2026

This document has been licensed to WorkFusion, a UiPath Company

Everest Group®

FINANCIAL CRIME AND
COMPLIANCE (FCC)
TECHNOLOGY PROVIDERS

**TOP
50™**
2026

Rebuilding the FCC stack for always-on channels, real-time controls, and accountable AI

The Financial Crime and Compliance (FCC) landscape is entering a new operating era. Faster payments, embedded finance, and always-on digital channels have compressed decision windows from hours to seconds, while the threat environment has expanded beyond traditional Anti-money Laundering (AML) into scams, mule networks, digital identity abuse, and increasingly complex cross-border typologies. At the same time, regulatory expectations continue to rise, demanding stronger governance, better evidence trails, and tighter control over third-party dependencies across the compliance stack.

This shift is forcing financial institutions to modernize beyond incremental upgrades. Legacy FCC environments, built as fragmented point solutions with batch-oriented checks, struggle to keep pace with real-time risk decisions, multi-entity customer structures, and rapidly evolving criminal behavior. The result is familiar: rising operational workload, uneven coverage across channels, inconsistent controls across geographies, and growing pressure to demonstrate explainability, auditability, and resilience under scrutiny.

FCC technology providers are responding by re-architecting solutions around end-to-end workflows and ecosystem integration. Platforms are moving closer to enterprise data estates and cloud environments, enabling faster analytics, more scalable monitoring, and tighter orchestration across onboarding, screening, transaction monitoring, investigations, and reporting. In parallel, automation is evolving from simple assistance to execution – where intelligent workflows and agentic capabilities can reduce manual effort while strengthening control consistency and governance.

As FCC programs transition to real-time and cross-channel controls, technology adoption is increasingly being shaped by three practical

constraints: speed (decisioning in always-on channels), defensibility (clear reasoning and audit trails), and deployability (secure, resilient implementation across jurisdictions and operating models). This is accelerating the demand for modular platforms that can interoperate with enterprise data, integrate with core banking and payment rails, and support rapid configuration as typologies and regulatory priorities evolve.

Across the provider landscape, differentiation is shifting from “feature depth in one module” to “operational performance across the value chain.” Institutions are prioritizing solutions that can reduce latency, improve detection fidelity, and streamline investigations at scale, while lowering false positives and ensuring consistent controls across lines of business. This is also pushing vendors toward ecosystem-led delivery: deeper hyperscaler alignment, stronger SI/advisory partnerships, and pre-integrated capabilities that shorten time to value.

A second inflection point is the emergence of agentic approaches in compliance operations. While earlier waves of AI focused on scoring, detection, and summarization, the next wave is oriented toward controlled execution, triaging alerts, assembling evidence, and coordinating actions across tools with human oversight. This does not replace the need for strong governance; rather, it raises the bar for accountability, authorization, traceability, and reversibility in how compliance work is performed.

This report explores the Top 50 FCC technology providers; their positioning across the FCC value chain; the key shifts shaping adoption across market demand, regional priorities, and ecosystem partnerships; and the move toward more automated, orchestrated, and resilient FCC operating models.

Contents

- 04 Background, research methodology, and scope of research
- 05 Everest Group Top 50™ FCC Technology Providers 2026
- 12 Evolving trends and key drivers transforming FCC
- 16 Geographical distribution of Top 50™ FCC providers
- 17 Deal themes shaping FCC buying behavior
- 18 Everest Group recognitions for key FCC technology providers
- 22 Transforming FCC technology through industry cloud partnerships, driving innovation, agility, and scalability
- 24 Leveraging agentic AI in FCC technology solutions
- 26 The role of System Integrators (SIs) and advisory firms in FCC technology adoption
- 27 Implications for FCC technology providers
- 28 Building a resilient FCC strategy: the TRUST+ framework for enterprises
- 30 Special mentions

Everest Group’s scope of research for Top 50™ FCC Technology Providers 2026

This research evaluates leading FCC technology providers supporting financial institutions. The assessment spans the end-to-end FCC value chain, including KYC and digital identity, sanctions and screening, AML screening and transaction monitoring, regulatory reporting, fraud management, trade-finance compliance, and crypto compliance. It covers both enterprise-wide FCC platforms and specialist providers addressing specific risk domains, such as entity resolution, adverse media, network analytics, Suspicious Activity Reporting (SAR) automation, fraud detection, and Trade-based Money Laundering (TBML) monitoring. The study examines providers across major global markets and evaluates their functional depth, platform capabilities, AI and analytics enablement, workflow orchestration, data strategy, deployment models, and geographic presence to identify the Top 50 FCC technology providers shaping the global compliance landscape.

FCC technology value chain

[NOT EXHAUSTIVE]

		AML				
KYC	Sanctions and screening	Screening and monitoring	Reporting	Fraud management	Trade-finance compliance	Crypto/Digital-asset compliance
Digital identity verification	Sanctions list screening	Client lifecycle risk and screening	Alert management and prioritization	Transaction fraud detection	Trade document and transaction screening	Blockchain transaction monitoring
Customer Due Diligence (CDD) and risk scoring	Watchlist / (Politically Exposed Person) PEP / Adverse media screening	Transaction monitoring	Regulatory reporting (e.g., SAR/STR/CTR/LCTR filing)	Identity theft and account takeover detection	TBML typology and pattern detection	Wallet address screening
Enhanced Due Diligence (EDD)	Dynamic/Fuzzy matching and false-positive reduction	Ongoing surveillance	Case escalation and workflow automation	Mule account and fraud ring detection	Counterparty, vessel, and commodity due diligence	Virtual Asset Service Provider (VASP) due diligence and travel rule compliance
Perpetual KYC / ongoing refresh	Screening list management	Entity and network analytics		Payment fraud monitoring		
Customer lifecycle management and onboarding workflows	Risk intelligence data (e.g., PEP / sanction / adverse media, etc. lists)	CDD/EDD		Chargeback, dispute and recovery management		
		Platform and deployment model				
		Workflow and orchestration				
		Analytics and AI enablement				
		Risk intelligence and data strategy				
Geography scope						
North America	LATAM	UK	CE	APAC	MEA	

Everest Group Top 50™ FCC Technology Providers 2026 (page 1 of 2)

▲ Up ▼ Down ■ No change ● New to the list

Rank	Delta	Technology provider	HQ	Final score
1	■	LexisNexis Risk Solutions	North America	91.0
2	■	NICE Actimize	North America	89.0
3	■	Quantexa	UK&I	76.5
4	■	Fenergo	UK&I	76.0
5	■	WorkFusion, a UiPath Company	North America	74.0
6	▲	LSEG Risk Intelligence	UK&I	73.0
7	▲	Moody's	North America	69.3
8	▼	Oracle Financial Crime and Compliance Management	North America	69.1
9	▲	Tookitaki	APAC	69.0
10	▼	SymphonyAI	North America	68.9
11	▲	ThetaRay	MEA	68.8
12	▲	ComplyAdvantage	UK&I	68.7
13	▲	Napier AI	UK&I	68.6
14	■	Jumio	North America	68.5
15	▲	Feedzai	Europe	68.4
16	▼	GBG	UK&I	67.0
17	▼	Visa Protect	UK&I	65.7
18	▲	Onfido ¹	UK&I	65.6
19	▼	Signzy	APAC	65.0
20	▲	Sumsub	Europe	63.7
21	▼	Nasdaq Verafin	North America	63.7
22	●	Mozn	MEA	63.0
23	■	Unit21	North America	62.4
24	▼	Lucinity	Europe	62.3
25	▲	Eastnets	MEA	61.0








¹ Onfido is now an Entrust company

Everest Group Top 50™ FCC Technology Providers 2026 (page 2 of 2)

▲ Up ▼ Down ■ No change ● New to the list

Rank	Delta	Technology provider	HQ	Final score
26	●	26 Outseer	North America	60.5
27	▼	-3 Trulioo	North America	60.1
28	▼	-2 Incode	UK&I	59.8
29	▼	-7 Dow Jones Risk & Compliance	UK&I	58.0
30	▲	1 Socure	North America	57.7
31	▼	-3 Bureau	UK&I	57.0
32	▼	-3 Cleareye.ai	North America	56.8
33	▲	12 Hawk	North America	56.7
34	■	0 Kharon	APAC	56.5
35	▲	4 Flagright	North America	56.4
36	●	36 Bretton AI	MEA	56.3
37	●	37 IDfy	UK&I	56.2
38	●	38 Sigma360	UK&I	56.1
39	▼	-6 Mitek Systems	North America	55.7
40	▼	-5 Elliptic	Europe	55.6
41	●	41 Vouched	UK&I	55.5
42	▲	1 Rzolut	UK&I	55.5
43	▼	-1 Encompass	UK&I	55.0
44	■	0 Facctum	APAC	53.1
45	▼	-9 Xapien	Europe	51.3
46	●	46 Azentio	North America	50.9
47	●	47 Facephi	MEA	49.7
48	▼	-2 AP Solutions IO	North America	47.2
49	▼	-8 smartKYC	Europe	45.0
50	●	50 Discai	MEA	42.0

Top risers in the Top 50™ FCC Technology Providers 2026

Top risers	Positions climbed
 	1 → 12
	2 → 7
 	3 → 5
	4 → 4
	5 → 3

New entrants in the Top 50™ FCC Technology Providers 2026





 **Discai**





 **MOZN** ^{<AI>}







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	Payments	Capital markets	Hi-tech and entertainment	Others
1	LexisNexis Risk Solutions	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
2	NICE Actimize	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
3	Quantexa	✓		✓	✓	✓	✓	✓	✓		✓	✓
4	Fenergo	✓			✓	✓	✓	✓	✓	✓		✓
5	WorkFusion, a UiPath Company	✓		✓	✓	✓	✓	✓	✓	✓	✓	
6	LSEG Risk Intelligence	✓		✓	✓	✓	✓	✓	✓	✓		✓
7	Moody's	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓
8	Oracle Financial Crime and Compliance Management	✓	✓	✓	✓	✓	✓	✓	✓			✓
9	Tookitaki		✓			✓	✓	✓	✓			✓
10	SymphonyAI	✓		✓	✓	✓	✓	✓	✓	✓	✓	
11	ThetaRay	✓	✓	✓	✓		✓	✓	✓	✓		✓
12	ComplyAdvantage	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
13	Napier AI	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓
14	Jumio	✓	✓		✓		✓	✓	✓	✓	✓	✓
15	Feedzai	✓		✓	✓	✓		✓	✓	✓		✓
16	GBG	✓		✓	✓	✓		✓	✓	✓	✓	✓
17	Visa Protect	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
18	Onfido ¹	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
19	Signzy	✓	✓		✓	✓	✓	✓	✓		✓	✓
20	Sumsub	✓		✓	✓	✓	✓	✓	✓	✓	✓	
21	Nasdaq Verafin	✓		✓				✓	✓	✓		✓
22	Mozn	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
23	Unit21	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
24	Lucinity	✓		✓	✓	✓		✓	✓	✓		
25	Eastnets	✓		✓	✓	✓	✓	✓	✓	✓		✓

1 Onfido is now an Entrust company

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	Payments	Capital markets	Hi-tech and entertainment	Others
26	Outseer	✓	✓	✓	✓	✓	✓	✓	✓			✓
27	Trulioo	✓			✓	✓		✓	✓	✓	✓	✓
28	Incode	✓			✓	✓		✓	✓	✓	✓	✓
29	Dow Jones Risk & Compliance	✓			✓	✓	✓	✓	✓			✓
30	Socure	✓						✓	✓	✓	✓	✓
31	Bureau	✓			✓	✓	✓	✓	✓		✓	✓
32	Cleareye.ai	✓		✓	✓	✓	✓	✓				✓
33	Hawk	✓	✓	✓	✓	✓	✓	✓	✓			✓
34	Kharon	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
35	Flagright	✓	✓	✓	✓	✓	✓	✓	✓			✓
36	Bretton AI	✓		✓	✓		✓	✓	✓		✓	✓
37	IDfy					✓	✓	✓	✓	✓	✓	✓
38	Sigma360	✓	✓	✓		✓	✓	✓	✓	✓		✓
39	Mitek Systems	✓		✓	✓			✓	✓	✓	✓	
40	Elliptic	✓	✓	✓		✓		✓	✓	✓		✓
41	Vouched	✓	✓	✓	✓			✓	✓		✓	✓
42	Rzolut	✓		✓		✓	✓	✓	✓		✓	✓
43	Encompass	✓		✓	✓	✓		✓		✓		✓
44	Factum			✓	✓	✓	✓	✓	✓		✓	✓
45	Xapien	✓		✓	✓	✓	✓			✓	✓	✓
46	Azentio					✓	✓	✓	✓	✓		✓
47	Facephi	✓	✓		✓	✓	✓	✓	✓		✓	✓
48	AP Solutions IO			✓	✓		✓	✓	✓	✓		✓
49	smartKYC			✓	✓	✓		✓				✓
50	Discai				✓			✓				

Coverage across key LoBs (page 1 of 2)

Rank	Technology provider	KYC	Payment screening	Transaction monitoring	Fraud	Regulatory reporting	Risk assessment and threat mitigation
1	LexisNexis Risk Solutions	✓	✓	✓	✓	✓	✓
2	NICE Actimize	✓	✓	✓	✓	✓	✓
3	Quantexa	✓	✓	✓	✓	✓	✓
4	Fenergo	✓	✓	✓		✓	✓
5	WorkFusion, a UiPath Company	✓	✓	✓	✓	✓	✓
6	LSEG Risk Intelligence	✓	✓	✓	✓		✓
7	Moody's	✓				✓	✓
8	Oracle Financial Crime and Compliance Management	✓	✓	✓	✓		✓
9	Tookitaki		✓	✓	✓	✓	✓
10	SymphonyAI	✓	✓	✓	✓	✓	✓
11	ThetaRay	✓	✓	✓		✓	✓
12	ComplyAdvantage	✓	✓	✓		✓	✓
13	Napier AI		✓	✓		✓	✓
14	Jumio	✓	✓	✓	✓	✓	✓
15	Feedzai	✓	✓	✓	✓	✓	✓
16	GBG	✓	✓	✓	✓	✓	✓
17	Visa Protect		✓		✓	✓	✓
18	Onfido ¹	✓					✓
19	Signzy	✓		✓	✓		
20	Sumsb	✓		✓	✓		✓
21	Nasdaq Verafin	✓	✓	✓	✓	✓	✓
22	Mozn		✓	✓	✓	✓	✓
23	Unit21		✓	✓	✓	✓	✓
24	Lucinity	✓	✓	✓	✓	✓	✓
25	Eastnets	✓	✓	✓	✓	✓	✓

1 Onfido is now an Entrust company

Coverage across key LoBs (page 2 of 2)

Rank	Technology provider	KYC	Payment screening	Transaction monitoring	Fraud	Regulatory reporting	Risk assessment and threat mitigation
26	Outseer				✓		✓
27	Trulioo	✓			✓		✓
28	Incode	✓			✓		✓
29	Dow Jones Risk & Compliance	✓	✓				✓
30	Socure	✓			✓		✓
31	Bureau	✓		✓	✓		✓
32	Cleareye.ai	✓	✓	✓	✓	✓	✓
33	Hawk	✓	✓	✓	✓	✓	✓
34	Kharon	✓	✓			✓	✓
35	Flagright	✓	✓	✓	✓	✓	✓
36	Bretton AI	✓	✓	✓	✓		
37	IDfy	✓	✓	✓	✓	✓	✓
38	Sigma360	✓	✓	✓		✓	✓
39	Mitek Systems	✓			✓		✓
40	Elliptic	✓	✓	✓			✓
41	Vouched	✓		✓			✓
42	Rzolut	✓	✓	✓			✓
43	Encompass	✓					✓
44	Facctum	✓	✓	✓	✓		✓
45	Xapien	✓					✓
46	Azentio	✓		✓	✓	✓	
47	Facephi	✓			✓		✓
48	AP Solutions IO	✓	✓	✓	✓		✓
49	smartKYC	✓					✓
50	Discai			✓			✓

Evolving trends and key drivers transforming FCC

The FCC landscape is entering a new phase as financial institutions balance faster, always-on digital journeys with rising expectations for control effectiveness. Risk is no longer concentrated in a few traditional channels. It now surfaces across real-time payments, embedded finance ecosystems, digital onboarding, and token-adjacent rails, compressing the time available to detect and disrupt suspicious activity. At the same time, criminal tactics continue to industrialize, using scams, synthetic identities, and coordinated networks to move faster and blend across typologies.

In response, institutions are shifting from incremental upgrades to operating model and platform modernization. The focus is moving toward measurable outcomes, real-time readiness, and defensible decisioning. This shift is also reshaping technology expectations: platforms must support interoperability across controls, stronger governance for AI-driven decisions, and the ability to run across jurisdictions without creating excessive noise, friction, or investigator overload.

FCC technology market size

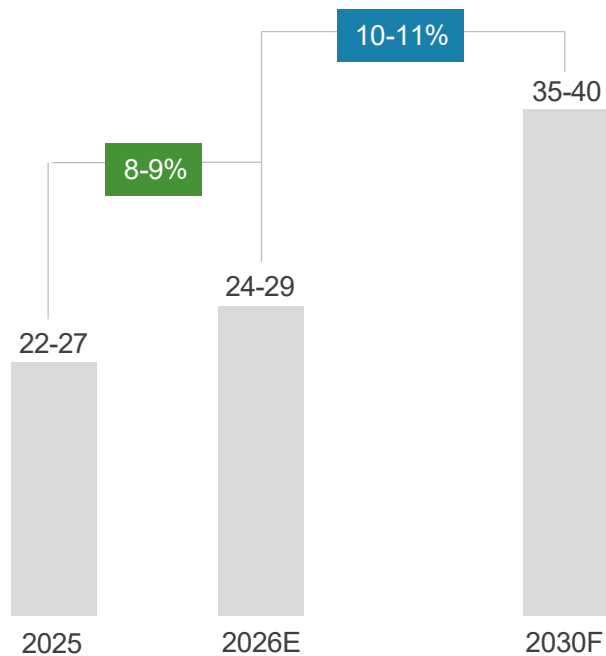
2025-30F; in US\$ billion

XX Growth rate

XX CAGR

E = Estimate

F = Forecast



Several shifts and factors are accelerating FCC transformation:



Regulatory and board-level pressure to demonstrate measurable FCC

program effectiveness: Institutions are moving away from adding point controls and looking at how consistently the program performs. The emphasis is shifting to decision quality, tuning discipline, model recalibration cadence, investigator consistency, and demonstrable reduction in exposure, rather than the volume of alerts or number of systems deployed.



Acceleration of real-time payments and digital onboarding pushing risk decisions earlier in the customer and transaction life cycle:

Risk decisions are moving upstream into onboarding, account lifecycle changes, and payments initiation. Continuous KYC/KYB refresh and earlier risk scoring are becoming critical as real-time rails reduce the opportunity for downstream clean-up. This shift is also tightening the link between identity, customer risk, and transaction behavior.



Rapid AI experimentation combined with tightening governance expectations reshaping FCC workflow design:

AI is evolving from insight generation to assisted execution across repeatable compliance tasks such as alert triage, contextual data gathering, case summarization, and report drafting. At the same time, governance expectations are rising. Institutions now require traceability, structured override logging, role-based guardrails, and audit-ready reasoning for every AI-supported action.



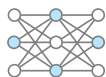
Growth of always-on digital channels increasing the demand for resilient, real-time-ready FCC platforms:

As payments and onboarding operate in real time, FCC systems can no longer remain latency-heavy, fragmented, or batch-bound. Institutions are increasingly prioritizing cloud-aligned, high-availability architectures, with scalable screening and monitoring layers that can operate continuously without creating customer friction or operational bottlenecks.



Operational inefficiencies and fragmented risk stacks driving the demand for unified data and case orchestration layers:

Many institutions are progressing toward architectures that unify data, signals, and cases across sanctions, AML, fraud, and emerging digital-asset risks. This does not always mean replacing every engine, but it does mean building a shared data model, common case record, and orchestration layer so teams can act on one consolidated view of customer and network risk.



Rising complexity in ownership structures and criminal networks increasing the demand for entity resolution and network transparency:

Financial crime is increasingly mediated through complex ownership structures, intermediaries, and partner ecosystems. This is driving deeper emphasis on beneficial ownership visibility, entity resolution, and network intelligence, especially where scam networks, mule activity, and cross-border structures blur accountability and increase hidden exposure.

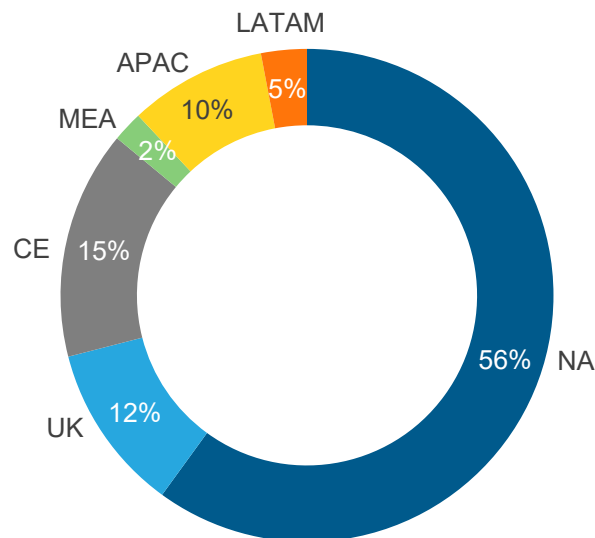
The evolution of threats, channels, and supervisory expectations is pushing FCC modernization beyond technology refresh into structural change. Institutions that invest in integrated decisioning, resilient platforms, and governed AI enablement will be better positioned to manage risk at scale while keeping customer journeys fast, frictionless, and defensible under scrutiny.

FCC technology market size by geography

FCC technology demand is being shaped by how quickly risk is shifting into real-time, digital-first journeys. As faster payments scale, onboarding becomes increasingly remote, and partner ecosystems widen exposure, institutions are investing in platforms that can operate at higher speeds with stronger governance. This is pushing modernization beyond point solutions toward resilient, interoperable stacks that support integrated decisioning across screening, monitoring, investigations, and reporting. The market size distribution below reflects where regulatory intensity, digital transaction scale, and maturity of FCC spend are currently most concentrated.

FCC technology market size by geography¹ 2025; percentage

100% = US\$22-27 billion



We discuss notable points for each region below.

- NA:** The region remains the largest and most mature FCC buying market, driven by a combination of high enforcement sensitivity, deep institutional spend, and growing pressure to manage fraud and AML together as real-time rails expand. Buyer conversations are increasingly anchored in effectiveness (tuning discipline, explainability, governance) and real-time readiness (low-latency screening, rapid interdiction, and scalable investigation throughput). There is also rising emphasis on integrating FCC controls into broader enterprise risk and data ecosystems rather than running them as isolated compliance stacks
- UK:** Buyers in the UK focus on fraud accountability, payment-journey protection, and sanctions responsiveness without adding friction for legitimate customers. Demand is rising for investigation productivity tooling (case summarization, triage support, workflow standardization) alongside stronger evidence trails and auditability. UK institutions also show strong preference for modular, API-aligned deployments that can be integrated quickly into existing digital channels and payment architectures

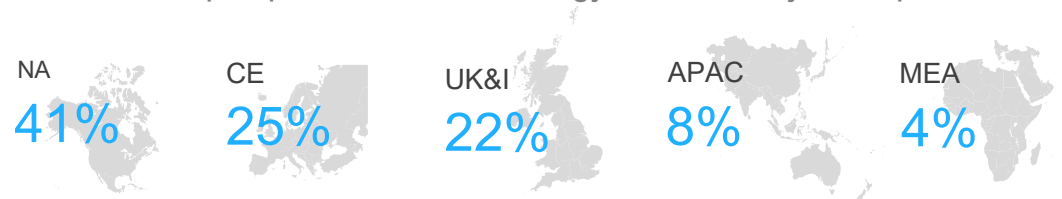
¹ Distribution by geography is based on the headquarters' location
Source: Everest Group 2026

- **CE:** The market is increasingly being shaped by the push toward standardization and supervisory consistency, which is nudging institutions toward scalable operating models across countries. Buyers are prioritizing platforms that can support multi-jurisdiction configurability, strong data lineage/traceability, and consistent governance alongside navigating stricter expectations around model oversight and operational resilience. There is also a clear tilt toward interoperable architectures, shared data models, orchestration layers, and unified customer risk views, especially for institutions operating across borders
- **APAC:** APAC demand is being pulled by high-velocity digital payments growth, persistent scam and mule-network exposure, and uneven regulatory maturity across markets. Consequently, buying patterns skew toward strong onboarding controls (eKYC/eIDV), behavioral monitoring, and network analytics that can surface coordinated activity early. Institutions also value solutions that are configurable and deployable in phases, because controls often need to be localized quickly as supervisory priorities shift from market to market
- **MEA:** MEA adoption is accelerating as regulatory modernization programs and national digital agendas increase expectations for stronger controls across banks, FinTechs, and cross-border corridors. Buyers in the region are balancing faster digitization with data residency and sovereignty requirements, creating the demand for flexible deployment models and cloud-aligned architectures that still satisfy local constraints. There is also increasing focus on ownership/UBO transparency, trade-linked risks, and maturing oversight of virtual asset exposure as more jurisdictions formalize expectations
- **LATAM:** LATAM's FCC demand is heavily shaped by high fraud pressure in digital channels and rapid customer growth across digital banks and payment ecosystems. Buyers tend to prioritize solutions that reduce noise; improve throughput, false-positive reduction, and case prioritization, and speed up onboarding controls, while remaining pragmatic on deployment speed and integration. There is also a consistent emphasis on controls that can keep pace with fast-moving payment ecosystems without slowing legitimate activity

Geographical distribution of Everest Group Top 50™ FCC Technology Providers

The Top 50™ FCC providers have a concentrated footprint in mature markets, reflecting where buyer spend, regulatory pressure, and product depth have historically been strongest. At the same time, the distribution shows how innovation and delivery capability are spreading across regions as providers expand go-to-market presence, establish local partnerships, and build configurable platforms that can serve multi-jurisdiction requirements at scale.

Everest Group Top 50™ FCC Technology Providers by headquarters



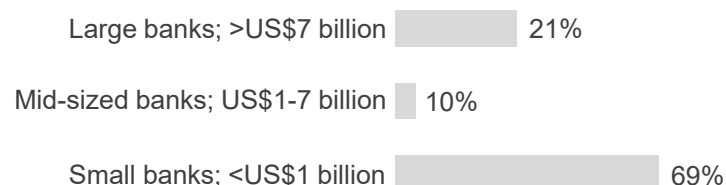
FCC technology deal insights

FCC technology revenue continues to be anchored by smaller banks (under US\$1 billion in annual revenue), which account for 69% of deal value. This underscores how compliance modernization is no longer concentrated among tier-1 institutions but is being driven by broad-based adoption across regional and community banks facing rising regulatory scrutiny, real-time payment risk, and fraud convergence pressures. These institutions are prioritizing modular, SaaS-led deployments that deliver faster time to value, improved alert quality, and workflow automation without large-scale core transformation.

Mid-sized banks (US\$1-7 billion) represent 10% of deal value, reflecting more targeted investments in transaction monitoring upgrades, sanctions optimization, and case management modernization as they scale digital channels and expand product footprints. Large banks (above US\$7 billion) contribute 21% of revenue, with spend concentrated in fewer, high-complexity programs such as unified risk fabrics, advanced analytics, AI governance, and resilience-driven platform modernization. While large institutions remain strategically important buyers, market momentum is increasingly shaped by scalable, standardized FCC deployments across the broader banking base.

FCC deals by buyer size (revenue)

2023-25; 100% = 70 deals*



* Based on publicly available deals

Deal themes shaping FCC buying behavior over the past 12-24 months

While the revenue mix shows adoption broadening beyond only the largest institutions, recent deal activity highlights how enterprises are modernizing FCC in practice. Buyers are no longer signing solely for “more monitoring;” they are investing in capabilities that move controls upstream, operate in real time, and embed compliance directly into the rails, ecosystems, and workflows where risk now originates and propagates. The themes below reflect the most consistent patterns observed across FCC deals signed in the past 12-24 months.



The pivot from KYC to automated KYB: Business onboarding is becoming the main battleground. Buyers are prioritizing automated business verification that can resolve legal entities, ownership structures, and UBO relationships quickly, especially for cross-border payments and platform-based commerce. The intent is to make business onboarding as scalable and low-friction as retail onboarding, without increasing manual due diligence load.



Compliance-by-design for sovereign digital rails (CBDCs and next-generation payment infrastructure): There is an uptick in FCC being embedded into the foundation of national-scale digital payment initiatives, not layered on later. This shifts the provider role from “bank vendor” to “infrastructure partner,” where fraud and compliance controls must work at scale, across participants, and under heightened scrutiny from the outset.



Fighting the “scam-demic” through network-level collaboration: A clear pattern is emerging around scam prevention that operates beyond a single institution. Buyers and networks are investing in capabilities that detect and disrupt scams across account-to-account flows, merchants, and multi-PSP ecosystems. The emphasis is on shared intelligence, faster interdiction, and coverage that reflects how scams bounce across banks and payment intermediaries.



Marketplace-led procurement and SaaS ecosystem integration: How FCC technology is bought is changing. Deal activity reflects cloud marketplace procurement and SaaS-first deployments, with buyers favoring solutions that can be switched on quickly, scale elastically, and integrate into existing cloud and data stacks. This also shows up as FCC being bundled more tightly into adjacent transformation programs (core, payments, digital onboarding), reducing procurement and implementation friction.



Specialized FCC for trade finance (verticalization): Trade finance continues to drive the demand for specialized solutions designed for trade-specific risk, including document-heavy workflows and complex counterparty structures. Rather than forcing TBML controls into general-purpose monitoring, institutions are layering trade-focused tooling alongside broader FCC platforms to address high-risk, high-complexity trade corridors more effectively.

Everest Group recognitions for key FCC technology providers (page 1 of 4)

1

Modernizing transaction monitoring for precision and scalability

This category highlights providers enhancing AML transaction monitoring through advanced analytics, graph intelligence, and hybrid detection architectures. Leading solutions improve alert precision, reduce operational noise, and support continuous tuning and model lifecycle discipline. As institutions prioritize measurable effectiveness over control proliferation, scalable and outcomes-driven monitoring has become central to FCC modernization. The leading providers in this category are:



2

Real-time screening and orchestration for payments and sanctions

This category recognizes providers delivering low-latency screening and orchestration capabilities suited for instant payment ecosystems and dynamic sanctions regimes. These solutions combine advanced matching, entity resolution, and configurable workflow controls to balance detection accuracy with operational efficiency. As payment speeds increase and sanctions obligations evolve, real-time readiness has become a core differentiator. The standout companies in this category are:



Everest Group recognitions for key FCC technology providers (page 2 of 4)

3

FRAML convergence and unified decisioning

This category evaluates providers integrating fraud detection and AML monitoring into unified platforms with shared data models and case workflows. By consolidating entity intelligence, behavioral signals, and transaction context, these systems enable cross-domain risk detection and reduce duplication across control environments. FRAML convergence reflects institutions' shift to unified risk fabrics rather than siloed stacks. The leading companies in this category are:



4

Advanced fraud prevention and behavioral analytics

This category highlights providers leveraging behavioral analytics, network intelligence, and anomaly detection to counter evolving fraud typologies, including scams, mule networks, and cross-channel manipulation. These solutions emphasize adaptive detection, customer behavior profiling, and dynamic risk scoring to reduce fraud losses while maintaining customer experience. We recognize the following companies in this category:



Everest Group recognitions for key FCC technology providers (page 3 of 4)

5

Network and consortium intelligence

This category recognizes providers embedding graph analytics and collaborative intelligence frameworks into FCC workflows. As financial crime increasingly operates through coordinated networks, leading solutions surface hidden relationships, ownership linkages, and cross-entity risk signals. Providers are also differentiated by their ability to integrate consortium or shared intelligence models while maintaining privacy and governance standards. The providers recognized in this category are:



6

Trade-finance compliance and TBML modernization

This category recognizes providers delivering specialized capabilities to detect and investigate trade-based money laundering risks. Leading solutions combine trade document analytics, counterparty intelligence, vessel and commodity monitoring, and typology libraries aligned to global regulatory frameworks. As trade flows grow in complexity, modernization beyond rules-based screening is increasingly critical. Providers recognized in this category are:



Everest Group recognitions for key FCC technology providers (page 4 of 4)

7

Crypto compliance and VASP risk management

This category evaluates providers supporting digital-asset compliance through integrated on- and off-chain risk intelligence. Solutions in this space link wallet analytics, sanctions screening, customer identity, and transaction monitoring into unified case workflows. As regulatory frameworks for virtual assets mature, integrated crypto compliance capabilities are becoming mainstream requirements. Standout providers in this category are:



8

Risk intelligence and typology innovation in FCC

This category highlights providers delivering actionable external intelligence across sanctions evasion, geopolitical exposure, illicit networks, and emerging typologies. By embedding curated intelligence into detection models and workflows, these solutions enable proactive risk identification and faster adaptation to evolving threats. Leading providers in this category are:



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

Industry cloud partnerships are becoming an enabler for FCC modernization as providers align with hyperscalers to deliver faster deployments, elastic scale, and stronger resilience. However, the partnership model itself is evolving. What began as “deploy on cloud” and “list on marketplace” is increasingly shifting to tighter integration with hyperscaler-native data, AI, and governance services, allowing compliance capabilities to operate closer to where enterprise data is created, enriched, and consumed.

These partnerships are also influencing how FCC is architected inside financial institutions. Rather than moving data into isolated FCC environments, institutions are increasingly embedding compliance logic into broader enterprise data layers. This reduces operational complexity and supports more consistent governance, security, and auditability. As adoption grows, hyperscalers are also playing a larger role in standardizing deployment patterns and simplifying procurement through marketplace-led buying and consumption-aligned commercial models.

The FCC technology ecosystem is entering a new phase of evolution, driven by hyperscaler expansion and AI-led workflow transformation. What was historically a marketplace of discrete compliance solutions is converging toward integrated, cloud-embedded architectures. The points below highlight the key shifts shaping this transition:



From marketplace-led distribution to data-fabric integration:

Compliance is moving closer to the enterprise data environment. Instead of relying on periodic extracts or slower handoffs, FCC workflows are increasingly being designed to operate within hyperscaler-native data fabrics, reducing latency and improving timeliness of detection and response.



Hyperscalers as primary providers of baseline compliance tasks:

Hyperscalers are starting to offer native services for select FCC needs, creating a co-opetition dynamic. Over time, this is likely to establish a layered model: hyperscaler-native “base compliance” capabilities for common tasks, complemented by specialist FCC platforms that provide differentiated analytics, workflow depth, and advanced automation.



An agentic orchestration layer becomes the connective tissue:

As agentic AI matures, the partnership focus is shifting to embedding AI-driven orchestration across compliance workflows. Investigators and operations teams will increasingly use cloud-native copilots to pull context across systems, coordinate decisions across multiple engines, and accelerate investigation documentation and reporting within a single guided workflow.



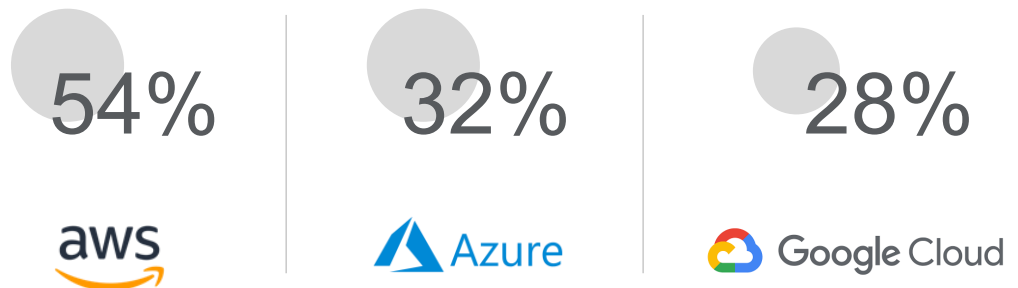
Digital sovereignty becomes a packaged deployment construct: Data residency and jurisdiction-specific expectations remain key barriers to scaling FCC on the cloud. Hyperscalers are responding with sovereignty-aligned deployment options, enabling institutions to run compliant configurations locally while maintaining standardized governance, security, and control frameworks across regions.



Outcome-aligned, “one-bill” procurement gains traction: Commercial models are also evolving. Rather than seeking separate infrastructure, software, and data contracts, institutions are increasingly looking for simplified, usage-based procurement through hyperscaler channels. Over time, this may shift buying toward an FCC-as-a-Utility model, in which cost aligns more directly with monitored volume, customers, and outcomes.

Presence of the Top 50™ FCC providers in hyperscalers’ industry cloud offerings

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



Leveraging agentic AI in FCC technology solutions

Agentic AI is emerging as the next step-change in FCC, shifting solutions from assistive intelligence (summarizing, drafting, and supporting human decisions) to execution-oriented intelligence that can carry out defined tasks across compliance workflows. Unlike earlier copilots that primarily helped investigators write faster or search better, agentic capabilities are positioned as digital workers that can triage alerts, assemble case context, recommend next actions, and progress low-risk outcomes with human oversight.

While adoption is still early and implementation patterns vary, the momentum is clear; most deployments are concentrating where FCC teams face the greatest operational pressure, high volumes, short response windows, and heavy manual effort. This is also increasing focus on control, institutions are asking not only “what can the agent do?” but “how is every step authorized, traceable, reversible, and auditable?” Consequently, agentic AI adoption is progressing alongside new emphasis on agent identity, governance, model assurance, and workflow guardrails that keep accountability with compliance teams.

Top use cases for agentic AI in FCC

Autonomous case investigations and narrative writing

Agentic AI can perform the legwork of investigations by gathering context across systems, summarizing transaction behavior, surfacing entity intelligence, and producing regulator-ready narratives for escalation and reporting.

Benefits: reduces investigation time and improves consistency by standardizing how evidence and rationale are compiled across cases.

Self-remediating alert triage and dispositioning

Agents act as a first-line layer that reviews low-risk alerts, resolves obvious false positives, and escalates only complex cases to investigators, while maintaining traceable decision paths and exception handling.

Benefits: cuts alert fatigue and improves investigator capacity by shifting effort away from repetitive reviews to higher-risk judgment work.

Cross-system enrichment and “next-best-action” guidance

Agents can automatically enrich alerts with customer context, counterparty risk signals, adverse information, and relationship patterns, then recommend prioritized investigative steps based on what similar cases required.

Benefits: improves decision quality and speed by ensuring investigators start with a complete, structured case context rather than assembling it manually.

End-to-end workflow orchestration across the FCC stack

Agentic AI is being embedded into orchestration layers to coordinate workflows across onboarding, screening, monitoring, investigations, and reporting, ensuring the right controls run in the right sequence with consistent handoffs.

Benefits: increases operational efficiency and reduces process breakpoints by turning fragmented tasks into a guided, governed execution flow.

Agent governance, model assurance, and “know your agent” controls

As agents take on operational responsibility, institutions are introducing controls to verify and govern agent actions, identity, authorization, traceability, reversibility, and audit evidence, along with stronger AI assurance and documentation.

Benefits: enables scaled adoption of agentic capabilities by making autonomous actions defensible under regulatory scrutiny and internal risk governance.

Inside the AI production stack: how FCC providers are operationalizing autonomy

Agentic AI is pushing FCC beyond assistive intelligence toward execution support across investigations, triage, and workflow automation. As adoption moves from pilots to production, enterprise scrutiny is shifting from what the model can do to how it runs in a controlled environment including deployment choices, guardrails for autonomous actions, and the ability to evidence outcomes for internal governance and regulatory review. In this context, differentiation is increasingly defined by the operating wrapper around agentic capability: the controls that manage when an agent can act, how decisions are reviewed or overridden, and what audit artifacts are generated.

The production readiness of AI-enabled FCC workflows should be viewed through three layers:

- Model layer: a hybrid of rules, Machine Learning (ML), graph analytics, and selective Large Language Model (LLM) usage aligned with specific tasks
- Control layer: workflow orchestration, human checkpoints, monitoring, and lifecycle discipline to keep autonomy bounded
- Evidence layer: traceability, rationales, and audit logs that make decisions explainable and review-ready

In practice, most implementations are hybrid by design. Deterministic components (rules, thresholds, workflow logic) continue to anchor consistency, while probabilistic techniques (ML, graph-based analytics, and LLM-driven reasoning) are applied where they add speed and context, such as in summarization, narrative drafting, enrichment, and guided next steps. This approach reflects a pragmatic balance: scaling throughput and responsiveness without weakening predictability in regulated FCC programs.

Explainability is also evolving from model-centric transparency to decision-centric defensibility. Beyond feature importance, providers are emphasizing end-to-end traceability linking outcomes to inputs, sources, decision paths, and reviewer actions so that cases can be reconstructed during assurance reviews. Alongside, deployment expectations are broadening, with many solutions supporting vendor-hosted, customer-hosted, or hybrid setups to align with data residency, sovereignty, and internal governance needs. Overall, production adoption is converging on the same requirement: agentic capability that can be deployed under enterprise constraints and operated with confidence.

The role of SIs and advisory firms in FCC

SIs and advisory firms are becoming more central to FCC modernization as institutions shift from incremental tool upgrades to end-to-end operating model change. The role is no longer limited to implementation support; SIs are increasingly shaping how FCC capabilities are stitched together across onboarding, screening, monitoring, investigations, and reporting, ensuring the stack works as one system rather than a collection of controls. This becomes critical as FCC programs expand across real-time rails, digital onboarding, and ecosystem-based delivery models, where integration quality and execution consistency matter as much as the underlying detection engines.

The nature of SI partnerships is also changing as cloud-native and AI-enabled architectures become the default travel direction. SIs are increasingly acting as last-mile ecosystem integrators, connecting hyperscaler-native data and AI services with specialist FCC platforms, and translating reference architectures into deployable, regulator-ready environments. Rather than bespoke builds, there is growing emphasis on reusable accelerators (templates, control libraries, data models, and investigation workflows) that allow institutions to scale across regions and business lines with lower friction.

The proportion of SIs and advisory firms that partner with Everest Group’s Top 50™ FCC Technology Providers¹ is depicted below:



[NOT EXHAUSTIVE]



¹ Based on press releases, provider inputs, and official recognition on partner pages or websites as of February 2026
Source: Everest Group 2026

Advisory firms are also evolving in parallel, with a stronger tilt toward governance and assurance as AI becomes more embedded in FCC workflows. As institutions experiment with more autonomous capabilities, demand is rising for support around decision accountability, how models behave, overrides are tracked, actions are justified, and outcomes are measured. This is pushing advisory work beyond policy design into model risk governance, control testing, and operating model redesign, especially where institutions must demonstrate defensible decisions under supervisory scrutiny.

Looking ahead, the next frontier is a shift from delivery milestones to managed outcomes. Institutions are increasingly pushing for measurable improvement, reduction in false positives, faster onboarding turnaround times, improved investigator productivity, and tighter real-time response, rather than go-live completion as the endpoint. This is likely to deepen co-investment models between SIs and FCC providers, including joint solution accelerators, packaged integration patterns, and domain-specific playbooks that can be rolled out repeatedly across clients.

We also expect SI and advisory roles to expand further as consortium-style approaches gain traction. As financial crime becomes more networked and cross-institutional, institutions will look for neutral orchestrators that can enable controlled data-sharing, privacy-preserving collaboration, and interoperability across tools and participants. In parallel, sovereign and in-country requirements are likely to increase the demand for local deployment expertise, positioning SIs as key partners not only for technology execution, but also for making global FCC transformations workable across regional regulatory realities.

Implications for FCC technology providers



Build compliance-grade agentic AI, not just AI features

Agentic AI is moving from nice-to-have productivity to operational execution (triage, remediation, investigation steps, and report drafting). Providers that win will package agents with clear boundaries: what the agent can do, when it must hand off, and how every action is logged and repayable for audit.



Treat explainability and governance as a license to operate

As AI governance hardens (especially in Europe), it will not be enough to say “we use AI.” Providers will need to bake in transparency: rationale, key drivers, model lineage, override logic, and evidence trails that work across models, rules, and human decisions, without creating extra investigator burden.



Focus on zero-data-movement and run where the bank’s data lives

Banks are pushing back on FCC stacks that require heavy ETL and parallel data stores. Providers now need native connectors and execution patterns that operate inside enterprise data platforms (lakehouse/fabric/warehouse), so detection and analytics happen with minimal latency and fewer security and data residency headaches.



Engineer for resilience, sovereignty, and regulated cloud by default

With operational resilience expectations rising and supervisory structures maturing, providers must make resilience and localization real product capabilities, not project customizations. Providers should think of regional deployment controls, in-country processing, strong third-party/ICT risk posture, and “prove-it” documentation that stands up in audits and regulator reviews.



Shift from selling modules to owning measurable outcomes

Enterprises are increasingly asking, “What changed after go-live?,” not “How many features did we buy?” Providers should be ready to contract and deliver around outcomes (false-positive reduction, analyst productivity, onboarding TAT improvements, scam loss reduction), supported by embedded benchmarking, continuous tuning, and operational playbooks, often jointly with SIs/advisors.

Building a resilient FCC strategy: the TRUST+ framework for enterprises

FCC is moving from periodic compliance checks to continuous, technology-driven risk execution. Instant payments, platform-based banking, and digitally enabled crime have compressed the window to detect and disrupt suspicious activity, while regulatory expectations increasingly emphasize demonstrable outcomes, transparency, and operational resilience. In this environment, enterprises need a closing lens that is familiar but future-proof. TRUST+ extends the TRUST framework by preserving its five pillars while raising the bar on speed, explainability, interoperability, and governed autonomy, the capabilities that will differentiate FCC programs as agentic workflows scale and compliance is always-on.

TRUST+ guides enterprises to build FCC programs that prevent threats earlier, adapt controls across jurisdictions, unify risk intelligence across silos, automate at scale with human oversight, and operationalize compliance on resilient cloud and data foundations. Ultimately, TRUST+ reframes FCC from a cost-of-compliance function into a strategic capability: protecting customers from scams, reducing operational drag, improving decision quality, and enabling faster innovation with confidence. We take a closer look below.



T Threat prevention and mitigation (from detection to disruption)

Move upstream and intervene earlier in the customer life cycle, onboarding, account changes, and payment initiation, so high-impact scams, mule networks, and synthetic identity risks are disrupted before they become downstream investigations. Pair behavioral analytics with network/context signals to improve precision as criminals adapt faster.



R Regulatory adaptability (from meeting rules to proving outcomes)

Design controls that can localize quickly across jurisdictions and evidence effectiveness on demand. The emphasis is shifting from “we have controls” to “our controls work,” making audit-ready traceability, policy-to-control mapping, and consistent decision rationale essential, especially where AI is involved.



U Unified risk intelligence (from silos to a single risk truth)

Converge fraud, AML, sanctions, and onboarding insights into a shared risk picture, at customer, entity, and network levels. Replace fragmented tooling with a unified risk fabric (shared data model, shared case record, orchestration across controls) so teams can act on one consolidated view of risk.



S Seamless automation (from workflow digitization to governed autonomy)

Automate the “heavy lifting” of FCC, triage, enrichment, investigation support, and narrative generation, while keeping clear human-in-the-loop checkpoints for material decisions. The goal is scalable productivity without sacrificing control: faster cycle times, lower false positives, and consistent investigator decisions.



T Technology-driven compliance (from platforms to real-time execution)

Modernize architecture to support real-time controls alongside instant rails, with cloud-native resilience and low-latency decisioning. Treat real-time and batch layers as complementary: real-time for interdiction, near-real-time/batch for deeper pattern discovery, back-testing, and continuous tuning.



The accelerator: speed, sovereignty, and accountable AI

While the TRUST pillars continue to anchor enterprise FCC strategy, their interpretation has evolved as compliance shifts from periodic control validation to continuous, real-time risk execution. The “+” reflects the set of capabilities that now sit on top of TRUST and determine whether an enterprise can operationalize those pillars at scale in day-to-day workflows. As payment and onboarding journeys become always-on and increasingly instantaneous, FCC programs must be engineered for real-time readiness rather than downstream remediation. Further, cloud adoption deepens across regulated environments, programs must be built with resilience and digital sovereignty as default design constraints, not deployment afterthoughts. Additionally, as automation moves from assistance to agent-led execution, institutions must embed accountable AI guardrails that keep autonomous actions authorized, explainable, traceable, and reversible. In effect, the “+” is what converts TRUST from a strategic blueprint into a modern operating mode, separating organizations that simply deploy contemporary FCC tools from those that consistently run a contemporary FCC program.

Special mentions

While the Everest Group FCC Technology Top 50™ recognizes providers with broad and established impact across the financial crime and compliance value chain, it is equally important to acknowledge a broader group of technology innovators shaping the market in meaningful ways. These special mention providers demonstrate strong capabilities in specific domains or emerging areas of FCC transformation, even if their overall coverage across the end-to-end value chain is more focused. Many of these firms are advancing niche capabilities, investing in differentiated intellectual property, or pioneering new approaches to areas such as AI-enabled investigations, digital identity defense, network intelligence, trade-based money laundering detection, crypto compliance, and upstream risk assessment. Through targeted innovation, ecosystem partnerships, and growing enterprise adoption, they are contributing to the evolution of more real-time, intelligence-led, and operationally efficient FCC programs. The companies below deserve a special mention.



Note: This is an indicative list of the technology providers with significant impact in the FCC technology space that were not included in our Top 50™ list

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



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.