Celent.

REGTECH SOLUTION BRIEF

Quantifying the Impact of AI-Driven Financial Crime Compliance

An Economic Study of Quantifind's Graphyte Platform in Action

Neil Katkov, PhD
February 2026

This is an authorized reprint of a Celent report. The reprint was prepared for Quantifind, but the analysis has not been changed. For more information about Celent, please see www.celent.com

A part of GlobalData

Contents

Economic Impact Summary **3**

The Cost of Inefficient Screening **5**

Why False Positives Are a Structural Problem 5

Changing the Economics of Screening 6

Who is Quantifind **7**

Company Overview 7

Quantifind's Graphyte Platform: Solution Overview 8

Quantifind Economic Impact Analysis **10**

AI-Driven Financial Crime Compliance: What It Means for Banks **12**

About Solution Briefs 12

Leveraging Celent's Expertise **13**

Support for Financial Institutions 13

Support for Vendors 13

Related Celent Research **14**

© CELENT

Economic Impact Summary

> Quantifind can unlock up to $177.9 million in annual KYC and sanctions cost efficiency for Tier 1 Banks.
>
> — Celent analysis

Financial crime compliance at banks is plagued by inefficiencies and high costs due to high false positive rates stemming from inadequate technology. To overcome these structural problems, innovative solutions are needed.

Quantifind addresses this need by providing AI-enabled screening and analytics to support know your customer (KYC), sanctions compliance, transaction intelligence, investigations, and third-party risk management. Quantifind's Graphyte platform has demonstrated success in improving accuracy, eliminating inefficiencies, and lowering costs in these essential financial crime compliance processes.

Quantifind has shared with Celent metrics on the Graphyte Platform's accuracy in several real-life client installations. Based on these metrics and Celent data on operational costs in financial crime compliance, Celent estimates that Tier 1 banks deploying Quantifind across KYC and sanctions screening alone could reduce annual alert-processing costs by up to $177.9 million, driven by substantially lower false positives and higher-confidence risk decisions. Tier 2 banks could achieve annual savings of approximately $42.5 million and Tier 3 banks could reduce costs by $3.4 million. Deploying Quantifind for additional use cases would generate more savings.

These savings stem from Quantifind's ability to autoclose or eliminate the majority of low-risk alerts generated by traditional screening systems, allowing compliance teams to focus analyst time on truly high-risk cases. In practice, these efficiencies are typically reinvested into higher-value compliance activities — such as complex investigations, regulatory change initiatives, and continuous monitoring — rather than simply reducing headcount.

Potential KYC and Sanctions cost savings across bank tiers

	Tier 1 Bank	Tier 2 Bank	Tier 3 Bank
KYC	$20.4M	$6.9M	$0.4M
Sanctions	$157.5M	$35.6M	$3.0M
Total	$177.9M	42.5M	$3.4M

This analysis offers a practical approach to quantify the economic value of higher-precision risk analytics in large banking environments. By improving screening accuracy while maintaining speed and scalability, Quantifind enables institutions to strengthen their control environment without increasing operational cost.

Looking ahead, Quantifind indicates that in 2026 it will expand Graphyte with agentic capabilities: AI agents that can automate discrete analyst tasks such as high-confidence entity resolution decisioning and post-screen validation, and provide interactive assistance (for example, explanation and structured summarization) to reduce follow-up research. If delivered with appropriate controls and auditability, these capabilities could further extend the efficiency gains described in this report by reducing manual effort beyond alert reduction alone.

In addition to economic benefits, Quantifind's platform can support compliance transformation by delivering insights at a scale and speed that supports continuous monitoring — the holy grail of "perpetual KYC." Moreover, Graphyte's low false positive rates make perpetual KYC a more attractive and realistic proposition, enabling banks to track their risk exposure as closely as possible.

The Cost of Inefficient Screening

Why This matters: Sanctions Screening Costs Scale with Transaction Volume Unless Alert Quality Improves.

Screening processes — for KYC, adverse media, sanctions, and other use cases — are critical components of financial crime compliance, designed to mitigate risks associated with financial crimes. The field is fraught with challenges, however, particularly due to the high false positive rates stemming from adverse media and sanctions screening. Traditional systems have struggled to deliver adequate performance in terms of both efficiency and accuracy, generating voluminous alerts — most of which prove to be false positives. This inefficiency necessitates the involvement of hundreds or even thousands of analysts at large financial institutions to process these alerts, placing a significant burden on compliance operations.

Why False Positives Are a Structural Problem

The high false positive rates — typically 95% or more of total alerts — of legacy systems are a serious structural problem for financial crime compliance, driving up costs and leading to relentless growth in analyst teams. The burden of resolving massive volumes of false positives can also pull resources away from mission critical high-risk investigation. These cost and organizational challenges apply across the financial crime compliance value chain, including KYC, sanctions, transaction monitoring, investigations, and third-party risk management.

Inadequate technology not only hampers operational efficiency but also drives regulatory risk. This has resulted in massive fines for the industry year in and year out, already topping the $1 billion mark by mid-2025. The growing digitization of financial services has further exposed the limitations of legacy technology in financial crime compliance, presenting financial institutions with the need to refresh, upgrade, and enhance their capabilities to support screening automation and increased volumes.

Why This Matters: Adverse Media Economics Have Historically Prevented Perpetual KYC

One of the most pressing challenges facing banks today is the struggle to achieve continuous monitoring (perpetual KYC) in order to track the bank's current risk exposure as closely as possible. The reliance on outdated technology has hindered the ability to implement continuous monitoring, which involves daily screening checks against adverse media and sanctions lists to identify changes in risk exposure.

False positives have been a significant barrier to banks implementing continuous monitoring. Quantifind asserts that it effectively resolves this issue through the greater precision of its adverse media screening analytics. Graphyte's low false positive rates make perpetual KYC a more attractive and realistic proposition for banks concerned about the costs, in terms of analyst time, of supporting a continuous monitoring operation. As importantly, the platform is able to deliver insights at a scale that supports continuous monitoring in large banking environments.

Changing the Economics of Screening

To address these pain points, innovative technology solutions are emerging in the market. New techniques for achieving more accurate name matching are bringing down false positive rates and increasing the ability to positively identify sanctioned entities. Advanced, AI-enabled adverse media search is particularly effective in identifying associates, predicate offenses, and other early warning risk signals involving not-yet-sanctioned entities.

Advanced risk analytics for sanctions and adverse media monitoring methods leverage several technologies to improve screening accuracy and efficiency:

- Artificial Intelligence (AI) and Natural Language Processing (NLP): These technologies support cognitive search capabilities, allowing for more nuanced understanding and analysis of data.
- Big Data Processing: This enables targeted screening against comprehensive sets of continuously refreshed data, ensuring that the most relevant information is considered.
- Intelligent Automation: By applying intelligent automation, the most pertinent highlights can be extracted for analyst review, streamlining the investigative process.
- Generative AI: Poised to drive the next generation of adverse media search, generative AI can significantly enhance screening accuracy while automating research tasks previously performed by human analysts.

Few vendors provide these advanced capabilities, but those that do can significantly enhance screening accuracy, automate research, and ultimately reduce costs. Quantifind is one such innovator that aims to enhance the KYC process through advanced analytics and automation.

Who is Quantifind

Screening processes for KYC, adverse media, and sanctions are essential for maintaining compliance and mitigating financial crime risks. However, the challenges posed by inadequate technology and high false positive rates necessitate innovative solutions. As financial institutions increasingly turn to advanced technologies, the potential for enhanced accuracy, efficiency, and regulatory compliance in screening processes becomes more attainable. By addressing these challenges head-on, banks can better navigate the evolving landscape of financial crime compliance and safeguard against the risks associated with financial crime.

Quantifind supports this evolution in financial crime compliance through its Graphyte Platform, which provides AI-enabled screening and analytics to support KYC, sanctions, transaction intelligence, investigations, and third-party risk management. The platform has demonstrated success in improving accuracy and eliminating inefficiencies in use cases across the financial crime compliance value chain.

The platform is also able to deliver insights at a scale that supports continuous monitoring of financial crime risk in large banking environments. The reticence to utilize adverse media screening due to high false positive rates is a significant barrier for many banks. Quantifind asserts that it effectively resolves this issue through the greater precision of its adverse media screening analytics. Graphyte's low false positive rates also make perpetual KYC a more attractive and realistic proposition for banks concerned about the costs, in terms of analyst time, of supporting a continuous monitoring operation.

Company Overview

Quantifind provides data analytics technology for risk detection and risk assessment in financial crime compliance to financial institutions as well as public sector agencies such as law enforcement and intelligence.

Quantifind was established in 2009 and is headquartered in Palo Alto, California, with additional teams in New York, Washington, D.C., and Boston. Quantifind has some 50 clients including a number of Tier 1 and 2 banks as well as government agencies.

Table 1: Quantifind Overview

Year Founded	2009
Headquarters	Palo Alto, California
Number of Employees	100
Revenues (USD)	Not disclosed
Financial Structure	Private with outside investors
VendorMatch Link	https://www.celent.com/en/directory/companies/quantifind

Source: Quantifind

Quantifind's Graphyte Platform: Solution Overview

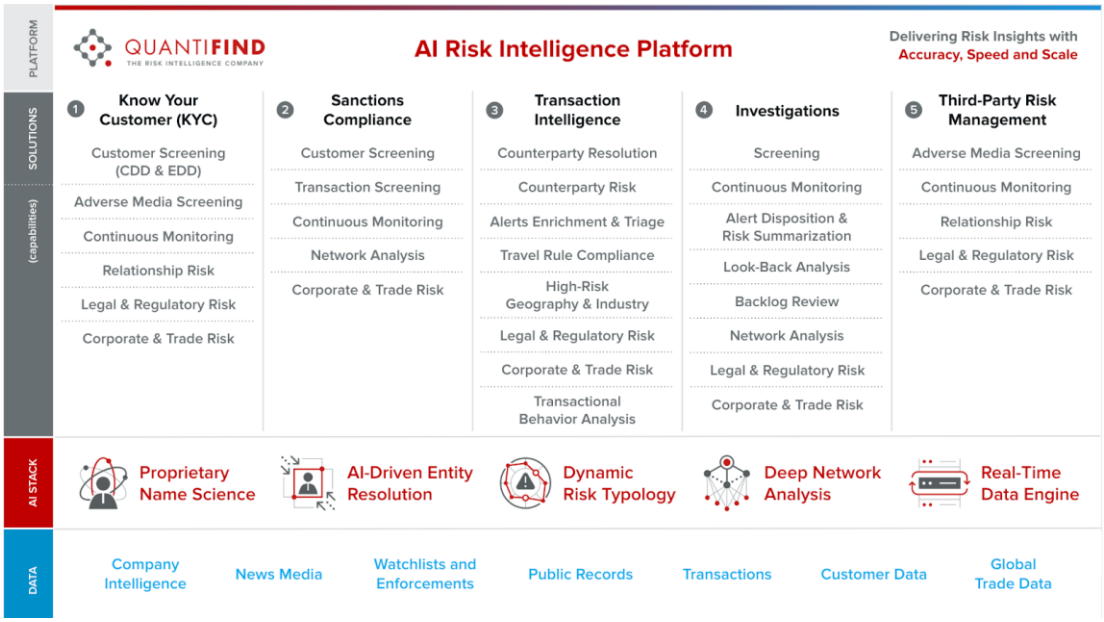
The Quantifind Graphyte Platform is a Software as a Service (SaaS) platform that addresses the challenges of financial crime compliance through innovative technology and advanced analytics. As financial institutions grapple with the overwhelming number of false positive alerts generated by traditional screening and decision analytics systems, Quantifind offers an alternative that significantly enhances the efficiency and effectiveness of compliance operations.

Quantifind provides AI-enabled screening and analytics to support KYC, sanctions compliance, transaction intelligence, investigations, and third-party risk management. Quantifind's capabilities focus on sanctions and PEPs screening and on risk analysis based on adverse media monitoring and other data. Quantifind's platform is used by clients to screen and risk assess new customers at onboarding and for periodic or event-driven monitoring (perpetual KYC); to support real time digital payments and other transactions; and for enhanced due diligence, investigations, third-party risk management, and other use cases in risk and compliance.

To support entity risk analysis, the Quantifind platform analyzes large amounts of textual data using AI, machine learning, and natural language processing (NLP) to understand the context of an entity within media articles or other records. The solution provides some 100 predictive risk factors designed to detect indicators of particular financial crime and other risk typologies in order to pinpoint the risk assessments.

Quantifind maintains its own dataset, which it pulls from public data sources using AI. The dataset is substantial, containing intelligence on 2 million PEPs, 25 million companies, and 1 billion media articles, according to the vendor.

Figure 1: Quantifind Risk Intelligence Platform



Source: Quantifind

Use case supported by Quantifind include:

- **Sanctions screening**. Quantifind supports sanctions screening by augmenting string-based name matching with additional features such as latent name features, location, and date of birth to contextualize the data elements in individual or legal entity searches. For example, surnames that are rare in a given jurisdiction would have a higher match likelihood than commonly occurring names. Quantifind calls its techniques "name science" and asserts that they can reduce false positives in sanctions screening by up to 98%. The solution also deploys entity resolution and deduplication techniques to further focus alerting, for example by applying deduplication to government releases on enforcement actions. Real time updates of sanctions activity further increase the accuracy of screening results.
- **Adverse media screening.** Quantifind's customer due diligence solution executes KYC checks including sanctions, PEPs, and adverse media screening to support account opening, customer review, and other stages in the customer lifecycle. Quantifind maintains its own proprietary database that houses some 1 billion articles. The platform aggregates data from diverse sources, including news articles, sanctions lists, politically exposed persons (PEPs), criminal records, leak data, and other sources to provide a holistic view of potential risks associated with each entity. Through AI-enabled analysis of this data, the solution can identify a wide range of risk types including money laundering, fraud, cybercrime, cryptocurrency-related risks, and legal proceedings.
- **Continuous monitoring.** Quantifind's solution can scan customers against its proprietary data — or third-party data sets — extract the relevant articles and deliver risk assessments within a second or two. The speed and scalability of Quantifind's solution is capable of supporting continuous adverse media monitoring for tens of millions of customers, providing effective support for perpetual KYC (pKYC).
- **Transaction intelligence.** Quantifind's platform can be deployed as an AI layer for transaction monitoring to enhance outcomes. Quantifind supports alert triage with entity resolution and alert enrichment; reduces false positives; and utilizes a range of techniques including anomaly detection and analysis of external data to surface risks.
- **Investigations**. Quantifind supports investigation by applying its entity resolution and name science techniques to reduce false positives and increase accuracy; and enrich alerts with intelligence from Quantifind's substantial adverse media dataset.
- **Third-Party Risk Management.** Quantifind leverages its data and analytics platform to support risk search and assessment for suppliers and other third parties.
- **Lookbacks.** Quantifind's speed and precision analytics can also support lookbacks and the clearing of backlogs. Quantifind has demonstrated that it can process large backlogs — that would take consultants weeks or months — in a matter of hours, in some cases eliminating the need for multi-million dollar consulting work.

Quantifind provides web-based alert management functionality which is adequate to cover the case management needs at midsize clients. Top tier clients are likely to use Quantifind to support L1 alert management and pipe results via APIs to third-party systems to support full case management requirements.

Quantifind Economic Impact Analysis

Quantifind has shared metrics on the Graphyte Platform's performance in several real-life client installations. Based on these metrics and Celent data on operational costs in financial crime compliance, Celent has estimated the potential savings from applying Quantifind to KYC and sanctions screening.

Our estimates quantify the efficiencies, in terms of analyst time spent on alerts, that are delivered by more precise screening outcomes. As part of this analysis, we considered the time required to resolve alerts, which vary significantly depending on the type of alert. For instance, sanctions alerts can be resolved in as little as five minutes, while adverse media alerts that uncover complex scenarios may take several hours to investigate.

Quantifind's analytics are highly accurate and, according to the vendor, can reduce false positives by 95% or more, depending on the use case and the client's risk tolerance. The economic analysis in this report is based on a somewhat more conservative autoclose rate of 80 - 90%.

Quantifind can reduce a Tier 1 bank's alert decisioning costs for sanctions screening by $157.5 million annually.

— Celent analysis

Sanctions Screening

Celent estimates that an average Tier 1 bank spends $175.0 million on manually decisioning sanctions alerts. According to Quantifind, the greater precision of its screening analytics can reduce alerts — or autoclose alerts generated by a third-party system — by 90% or more. This would reduce our Tier 1 bank's alert decisioning costs by $157.5 million annually. In other words, after inserting Quantifind into its sanctions screening process, alert processing costs could be reduced to $17.5 million or even less. For an average Tier 2 bank the cost savings would be $35.6 million, and Tier 3 banks could save $3.0 million annually.

KYC Screening

Celent estimates that a Tier 1 bank with 50 million customers and maintaining a 1/2/3 year review cycle for high, medium, and low risk customers spends $25.5 million annually on processing alerts generated by adverse media checks for these reviews. Quantifind asserts that its adverse media and sanctions analytics can reduce alerts by at least 80%. We therefore calculate that a Tier 1 bank using Quantifind would save $20.4 million annually for alert processing compared to legacy adverse media screening. The cost for alert processing after Quantifind would be reduced to $5.1 million. A Tier 2 bank with 12,000,000 customers and typically utilizing more manual processes would have a higher per-alert cost than a Tier 1 and spend $8.6 million on alert processing for customer review. Quantifind could potentially save this bank $6.9 million annually. A Tier 3 bank with 2 million customers would save $370,000 annually according to Celent analysis.

A Tier 1 bank using Quantifind would save $20.4 million annually for alert processing compared to legacy adverse media screening.

— Celent analysis

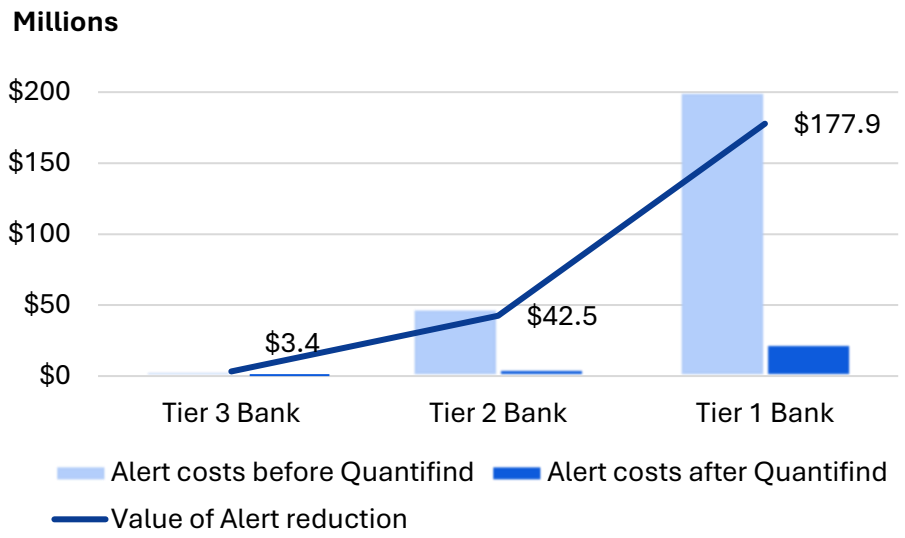
Table 2: KYC and Sanctions Alert Processing Costs Before and After Quantifind

	Tier 1 Bank		Tier 2 bank		Tier 3 Bank	
(1000s)	KYC	Sanctions	KYC	Sanctions	KYC	Sanctions
Annual alert processing costs	$25,500	$175,000	$8,600	$39,600	$460	$3,800
Alert reduction	- $20,400	- $157,500	- 6,900	- $35,600	- $370	- $3,000
Remaining alert processing costs	$5,100	$17,500	$1,700	$4,000	$90	$800

Note: Does not include savings from Quantifind transaction intelligence, investigations, or third-party risk management solutions.
Source: Celent estimates

Overall, according to our analysis, an average Tier 1 bank that exclusively relied on Quantifind across all customers and transactions could potentially reduce costs by $177.9 million, a Tier 2 Bank by $42.5 million, and a Tier 3 bank by $3.4 million on an annual basis across KYC and sanctions screening alone. Deploying Quantifind for additional use cases such as transaction intelligence, investigation, and lookbacks, would generate more savings.

Figure 2: Total KYC and Sanctions Alert Costs Before and After Quantifind



Note: Celent model assumes 80 – 90% alert autoclose.
Source: Celent estimates

These savings stem from Quantifind's ability to autoclose or eliminate the majority of low-risk alerts generated by traditional screening systems, allowing compliance teams to focus analyst time on truly high-risk cases. Nevertheless, these estimates are a reasonable way to highlight the potential value added from deploying an advanced risk analytics platform.

AI-Driven Financial Crime Compliance: What It Means for Banks

Financial crime compliance processes are increasingly challenged by high false positive rates, which burden financial institutions with inefficiencies and regulatory risk. Traditional anti-money laundering (AML) systems have proven inadequate, generating an overwhelming volume of alerts — most of which are false positives — that require extensive human resources to manage.

Quantifind has demonstrated that it can help financial institutions substantially reduce these pressures. By leveraging advanced analytics and AI-driven methodologies, Quantifind enhances screening accuracy, significantly reducing false positive rates and increasing accuracy. The platform's accuracy, speed, and scalability allow for continuous monitoring, even in large banking environments, enabling banks to conduct daily screening checks against adverse media and sanctions lists.

The economic benefits of implementing Quantifind can be substantial. Celent's analysis indicates that its precision analytics could reduce alert processing costs at a Tier 1 bank by a total $177.9 million across KYC and sanctions screening alone. Deploying Quantifind for additional use cases such as transaction intelligence, investigation, and lookbacks, would generate more savings.

Beyond these quantitative savings, Quantifind also addresses the qualitative challenges that have historically deterred banks from utilizing adverse media screening. By significantly lowering false positive rates, the platform fosters greater confidence in screening processes, enabling continuous monitoring and more frequent review cycles. This not only enhances compliance but also allows banks to allocate resources more effectively, ultimately leading to a more robust and efficient compliance framework.

Quantifind provides a compelling solution to the challenges of financial crime compliance, combining advanced technology with significant economic benefits. As financial institutions continue to navigate the complexities of AML regulations, the adoption of innovative solutions like Quantifind will be essential in achieving operational efficiency and regulatory compliance. This will ultimately help financial institutions to improve their processes, reduce regulatory risks, and enhance their overall compliance posture.

About Solution Briefs

A Solution Brief is a type of Celent Insight designed to provide research clients with timely updates on vendor/fintech solutions and strategies. Celent does not charge any fees to write a Solution Brief, and vendors do not have to be Celent research clients to be eligible for one. However, Celent analysts are selective and publish a limited number of notes throughout a year about briefings they found particularly interesting; the decision whether to write a note is at the Celent analyst's discretion. Vendors have the opportunity to check the draft before it's published to ensure we accurately represent the facts and don't disclose anything confidential, but otherwise do not have editorial control. Celent has not undertaken any additional due diligence beyond the briefing itself.

Leveraging Celent's Expertise

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

Support for Financial Institutions

Typical projects we support include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes and requirements. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short — term and long — term needs.

Support for Vendors

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials—including your website and any collateral.

Related Celent Research

Know Your Customer Systems: Identity Verification — Technology Capabilities Matrix and 2026 XCelent Awards
January 2026

Building Trust with Technology: Anti-Fraud Solutionscape and Technology Capabilities Matrix
September 2025

Trends in Fraud and AML Convergence at US Mid-Market Banks
April 2025

Dimensions: Risk IT Pressures & Priorities
March 2025

Top Tech Trends Previsory: Risk & Compliance, 2025 Edition
November 2024

So You Want to Buy an AML System: A Buyer's Guide to Financial Crime Compliance Technology
November 2024

Field Guide to GenAI Hyperscalers: Risk & Compliance Edition
September 2024

GenAI-oneers in Risk & Compliance: Cross-Sector Survey and Spotlights
July 2024

IT Spending on Risk Management in Banks: 2024 Edition
July 2024

IT and Operational Spending on Fraud: 2024 Edition
April 2024

IT and Operational Spending on Financial Crime Compliance: 2024 Edition
March 2024

Financial Crime Compliance Technology: Watchlist Screening Edition — 2024 XCelent Awards, Powered by VendorMatch
February 2024

Financial Crime Compliance Systems: AML Transaction Monitoring Edition — 2023 XCelent Awards, Powered by VendorMatch
July 2023

Inflexion Point in Financial Crime Compliance
April 2023

Maximizing the Value of Adverse Media Monitoring: Enabling a Dynamic Risk Assessment Framework for Anti-Money Laundering Compliance
September 2022

Copyright Notice

Copyright 2026 Celent, a division of GlobalData Plc. All rights reserved. This report may not be reproduced, copied or redistributed, in whole or in part, in any form or by any means, without the written permission of Celent, a part of GlobalData ("Celent") and Celent accepts no liability whatsoever for the actions of third parties in this respect. Celent and any third party content providers whose content is included in this report are the sole copyright owners of the content in this report. Any third party content in this report has been included by Celent with the permission of the relevant content owner. Any use of this report by any third party is strictly prohibited without a license expressly granted by Celent. Any use of third party content included in this report is strictly prohibited without the express permission of the relevant content owner This report is not intended for general circulation, nor is it to be used, reproduced, copied, quoted or distributed by third parties for any purpose other than those that may be set forth herein without the prior written permission of Celent. Neither all nor any part of the contents of this report, or any opinions expressed herein, shall be disseminated to the public through advertising media, public relations, news media, sales media, mail, direct transmittal, or any other public means of communications, without the prior written consent of Celent. Any violation of Celent's rights in this report will be enforced to the fullest extent of the law, including the pursuit of monetary damages and injunctive relief in the event of any breach of the foregoing restrictions.

This report is not a substitute for tailored professional advice on how a specific financial institution should execute its strategy. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisers. Celent has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been verified, and no warranty is given as to the accuracy of such information. Public information and industry and statistical data, are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information and have accepted the information without further verification.

Celent disclaims any responsibility to update the information or conclusions in this report. Celent accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

There are no third party beneficiaries with respect to this report, and we accept no liability to any third party. The opinions expressed herein are valid only for the purpose stated herein and as of the date of this report.

No responsibility is taken for changes in market conditions or laws or regulations and no obligation is assumed to revise this report to reflect changes, events or conditions, which occur subsequent to the date hereof.