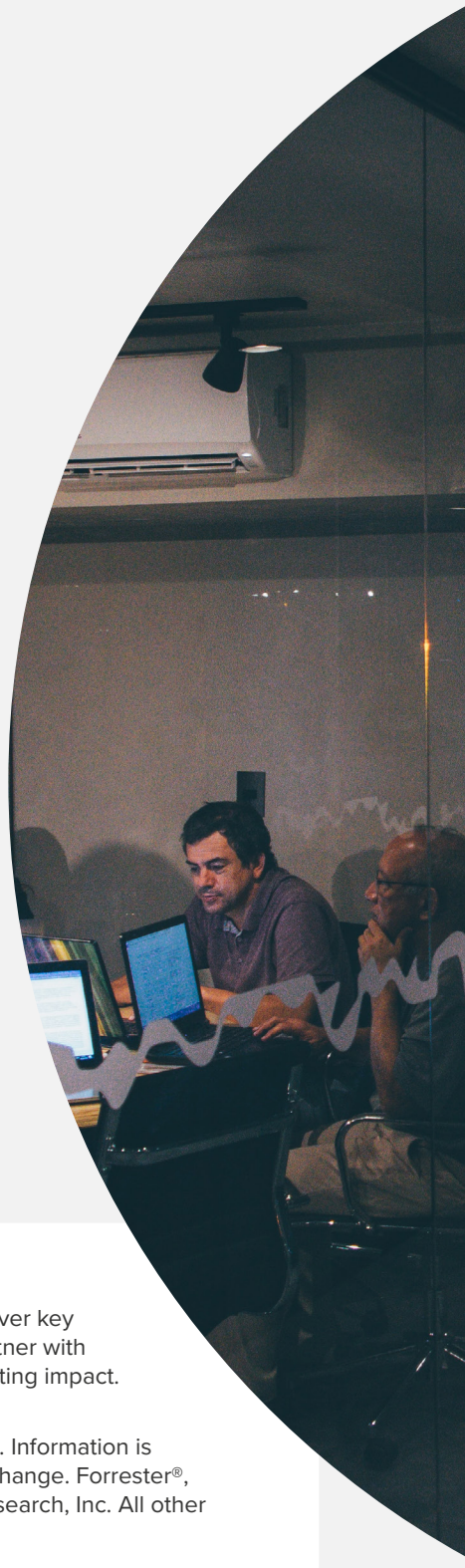
FORRESTER®

True Cost Of Financial Crime Compliance Study, 2023

A FORRESTER CONSULTING THOUGHT LEADERSHIP PAPER COMMISSIONED BY LEXISNEXIS® RISK SOLUTIONS, SEPTEMBER 2023

Table Of Contents



Project Team:

Antonie Bassi,
Market Impact Consultant

Emilie Beaud,
Associate Market Impact Consultant

Contributing Research:

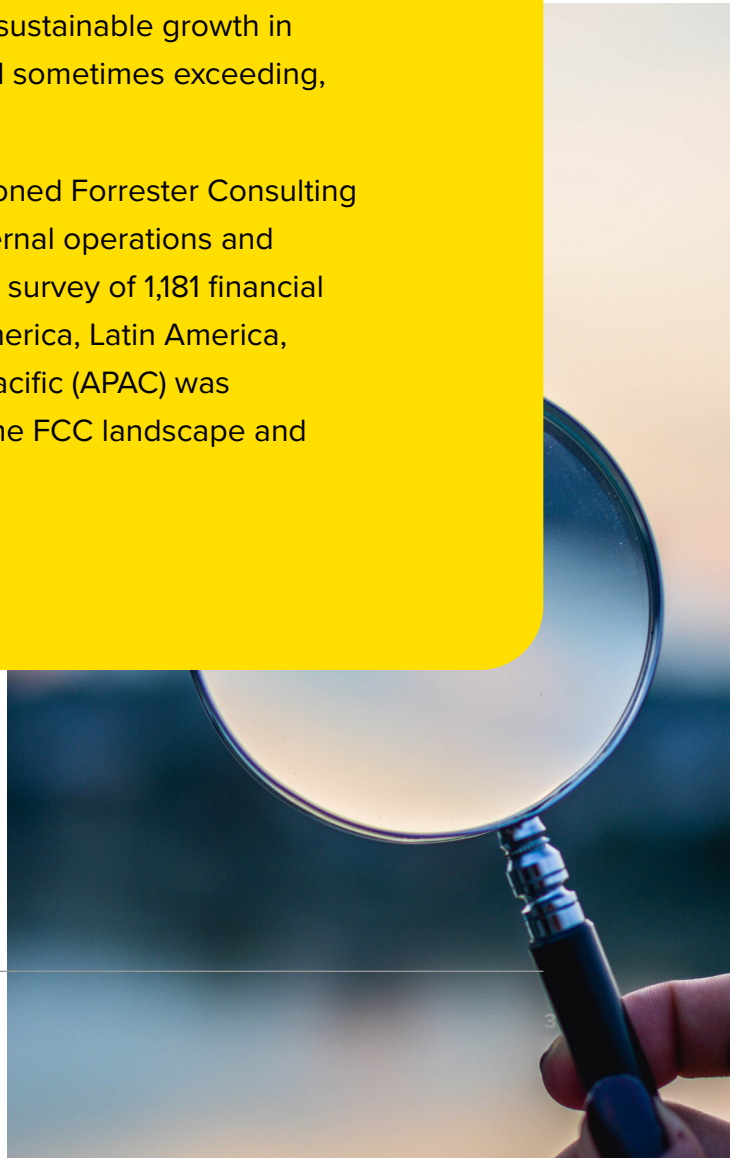
Forrester's Security & Risk research group

Executive Summary

The ever-changing technological and economic environment has redefined the compliance landscape for financial institutions. With 98% of institutions reporting an increase in financial crime compliance (FCC) costs, the economic pressures are undeniable. This uptick in costs is symptomatic of a broader spectrum of challenges. The shift to digital banking has amplified institutions' exposure to sophisticated financial crimes, especially via digital payments, cryptocurrencies, and AI technologies. Coupled with these new technologies are the complexities introduced by intricate and time-consuming know-your-customer processes during account onboarding. While digital transformation has ushered in growth opportunities, it has also exposed institutions to higher risks of financial crimes.

However, there are many opportunities to evolve FCC. As institutions start to do this, a focus on customer experience is key. Central to this is a proactive approach to financial crime risk management. With the right technologies and partnerships, financial institutions can achieve sustainable growth in customer numbers and revenue while meeting, and sometimes exceeding, applicable FCC requirements.

In June 2023, LexisNexis® Risk Solutions commissioned Forrester Consulting to establish how organizations are streamlining internal operations and enhancing efficiency in FCC management. A global survey of 1,181 financial crime and compliance decision-makers in North America, Latin America, Europe, Middle East, and Africa (EMEA), and Asia Pacific (APAC) was conducted to assess the evolving complexities of the FCC landscape and how financial institutions are adapting.[1]



Key Findings

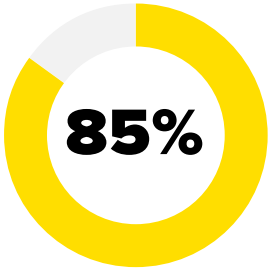
Complex regulations and sanctions hinder financial institutions from delivering great CX. The growing complexity of compliance regulations and ever-evolving criminal methodologies are a major difficulty for financial institutions. Balancing the imperative of regulatory compliance with delivering an exceptional customer experience is a challenge that financial institutions must learn to navigate.

Criminal use of advanced technologies is soaring. More than half of survey respondents reported a significant increase in financial crimes involving digital payments, cryptocurrencies, and AI technologies. This trend highlights the importance of adopting a multilayered approach that combines technology, expertise, collaboration, and compliance to successfully combat new types of crime.

Financial institutions plan to transform FCC operations for efficiency and experience. Financial institutions are reevaluating their existing financial crime compliance processes and planning improvements to data quality, know your customer (KYC), internal compliance, anti-money-laundering (AML), and transaction monitoring. Coupled with anticipated benefits like enhanced collaboration, simplified products, and improved efficiencies, these changes are projected to transform the compliance landscape while promoting improved customer and employee experiences.

Shaping The Future Of Financial Services By Prioritizing Compliance And Customer Experience

FCC is essential for safeguarding consumers' interests and the integrity, reputation, and stability of financial institutions and businesses. In a world that's becoming more complex and connected, the risk of financial crimes is growing. This risk is amplified by the growth of cryptocurrency and digital payments, along with the potential for fraud and supply chain/ trade-based money laundering. Organizations can build trust with customers, investors, and regulators by maintaining high standards of compliance, which also enhances their reputation and fosters sustainable growth and resilience.



of financial crime compliance executives say enhancing the customer experience is their top priority.

Balancing the drive for digital transformation with the desire for robust compliance, cost-effectiveness, and a superior customer experience is challenging. Organizations are reevaluating their priorities and identifying the key areas that need immediate attention to counter rising financial crime (see Figure 1). They are:

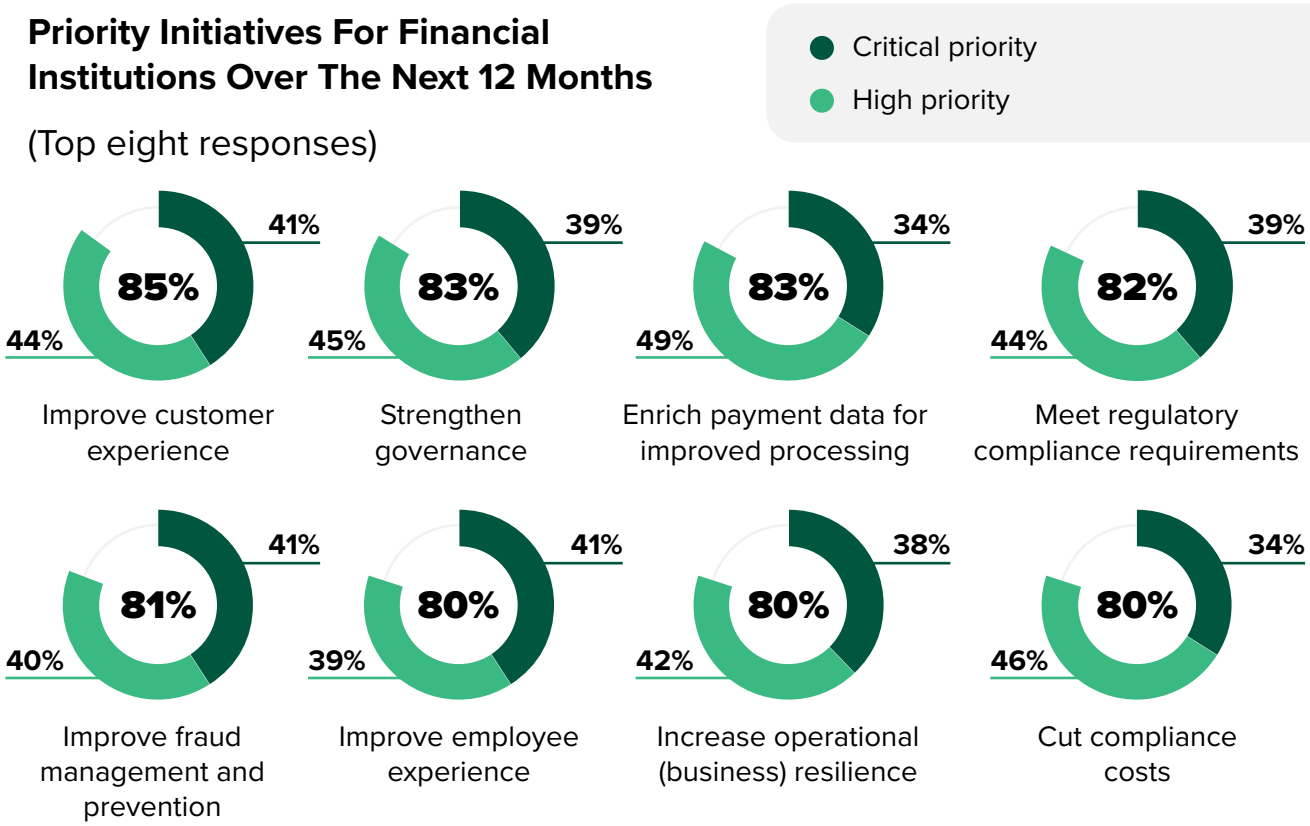
- **Amplifying customer-centricity.** The digitized world has seen a seismic shift in customer expectations. Responding to this trend, 85% of respondents have put enhancing CX on their priority list. This reaffirms a commitment toward fostering trust and delivering satisfaction, even in the face of proliferating financial threats.
- **Maintaining trust and reputation.** Sound governance practices and adherence to compliance standards build trust among stakeholders, including customers, investors, employees, and the public. Financial institutions recognize the crucial role of governance and compliance in ensuring stability, transparency, and ethical conduct: Respondents are focusing on strengthening governance (83%) and meeting regulatory compliance requirements (82%).

- **Using data for more accurate decision-making.** Data is the secret weapon in the fight against complex financial crimes, with 83% of respondents prioritizing harnessing enriched payment data. Enriched payment data leads to faster processing times, fewer payment rejections, and better risk management. It improves the customer experience while reducing the risk of noncompliance and exposure to financial crime.
- **Future-proofing themselves against unpredictable macroeconomic events.** Respondents are looking to increase their operational resilience (80%) to set their organizations up to withstand disruptions, recover quickly from challenges, maintain continuity, and ensure long-term sustainability. Respondents are putting equal focus on optimizing their compliance costs (80%) to improve profitability, remain agile in adapting to evolving regulatory requirements, and gain a competitive advantage in the market.

FIGURE 1

Priority Initiatives For Financial Institutions Over The Next 12 Months

(Top eight responses)



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

Unraveling The Compliance Conundrum Amid Rapid Change

While consumers have come to expect near-instant gratification when completing financial transactions (e.g., payment processing), financial institutions are having to introduce increasingly complex compliance regulations (e.g., verification and security checks), which creates roadblocks in the customer experience. This puts many financial institutions in the precarious position of balancing customer satisfaction and regulatory adherence. Our survey revealed the critical pain points in their journey (see Figure 2):

- **Growing compliance complexity is a barrier to business.** An overwhelming 78% of respondents say that the complex web of global regulations and sanctions has begun to restrain their business involvement. The intricacies of compliance have nudged these institutions toward seeking alternative processes that promise efficiency and cost-effectiveness, signaling an imminent transformation in their approach to compliance processes. To successfully complete this transition, financial institutions will need all the help they can get: 78% of respondents are looking to outsource some of their activities in the coming years.
- **Speed bumps clutter the adoption path of real-time payments.** Although instant payments are becoming the norm, 77% of respondents agree that the existing compliance models pose significant hurdles that obstruct this transition to real-time payments. These outdated compliance models not only cause payment processing delays but also put customer satisfaction — the Holy Grail of the financial world — at risk, according to 76% of respondents. The challenge lies in harmonizing instant transactions with robust compliance in order to meet and exceed customer expectations.
- **Rising workloads are a threat.** With payment volumes increasing, 79% of respondents have reported a parallel rise in screening alert numbers. This upswing signals a steep increase in compliance workloads that could potentially strain resources, putting these organizations' resilience to the test.

FIGURE 2

Navigating Regulatory Challenges: The Leading Priorities Are Crime Monitoring, Compliance Automation, And Process Overhaul

(Top 10 responses; showing "Strongly agree" and "Agree")

81% We have a formal process in place for identifying and tracking new types of crime and new criminal methodologies and assessing their impact on our business

80% Customers expect payments to be processed in near real time

80% Compliance departments are looking to automate some of their activities in the next three years

79% Screening alert numbers have been increasing with payment volumes

78% Complex regulations/sanctions create limitations on the type of business our organization can be involved with

78% Compliance departments are looking to outsource some of their activities in the next three years

77% Complex sanctions urge us to seek alternative, more cost-effective and efficient compliance processes

77% Recent FATF additions to gray and blacklists had a negative impact on the country my organization operates in

77% Current compliance models are preventing payments from becoming real time

76% Compliance procedures cause a delay in payment processing, which impacts customer satisfaction

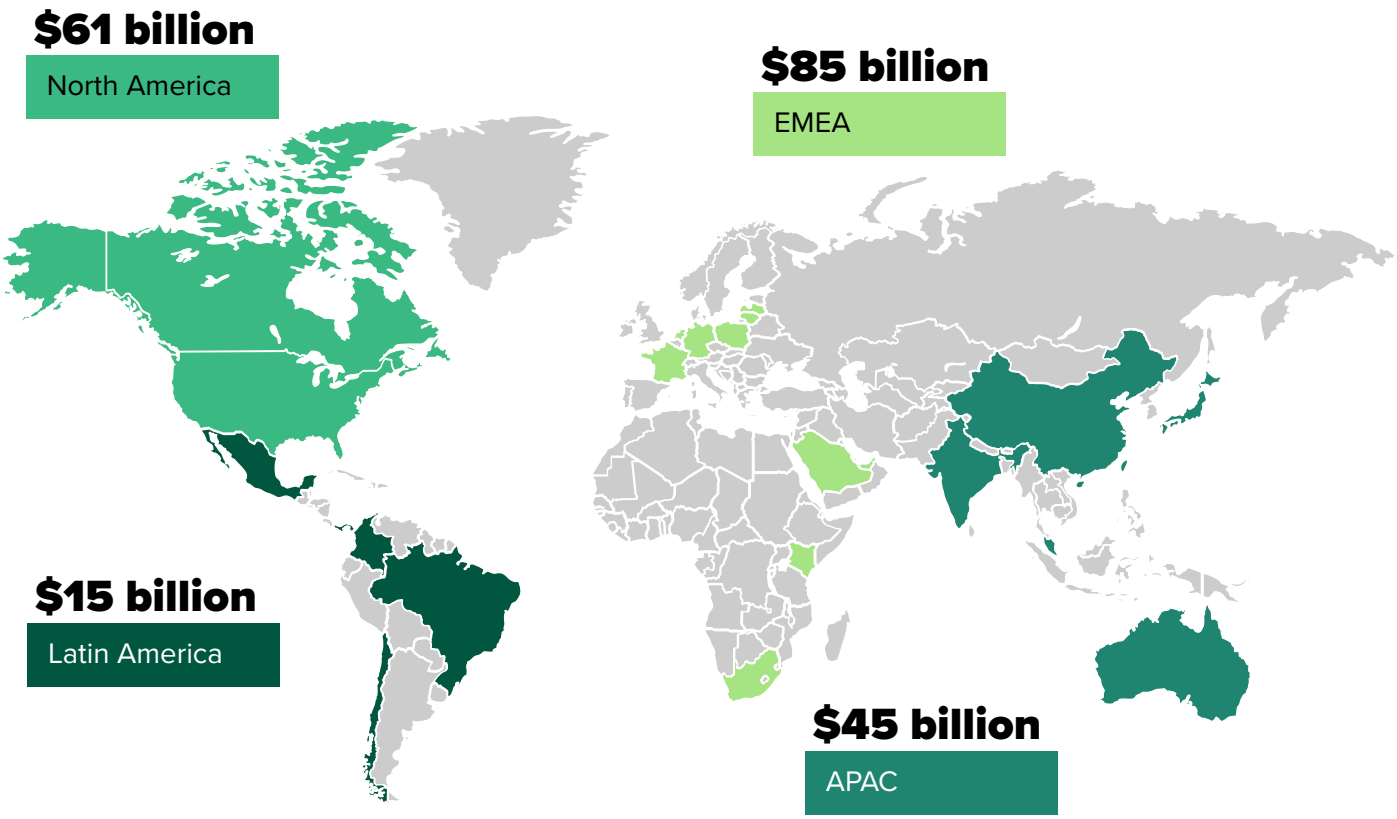
Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

THE KEY CONTRIBUTORS TO RISING COMPLIANCE COSTS

The total cost of FCC is soaring, with 98% of financial institutions reporting an increase in FCC costs. From a regional perspective, EMEA has the highest total cost at $85 billion; Latin America has the lowest at $15 billion (see Figure 3).

FIGURE 3

The Total Cost Of Financial Crime Compliance*



Total global costs: **$206 billion**

Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
*Note: The total annual cost of financial crime compliance is calculated using the number of financial institutions in the surveyed markets and survey data regarding financial crime costs. A spend amount is generated for each region by multiplying its average reported total cost of financial crime compliance operations by the number of financial institutions in that region.
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

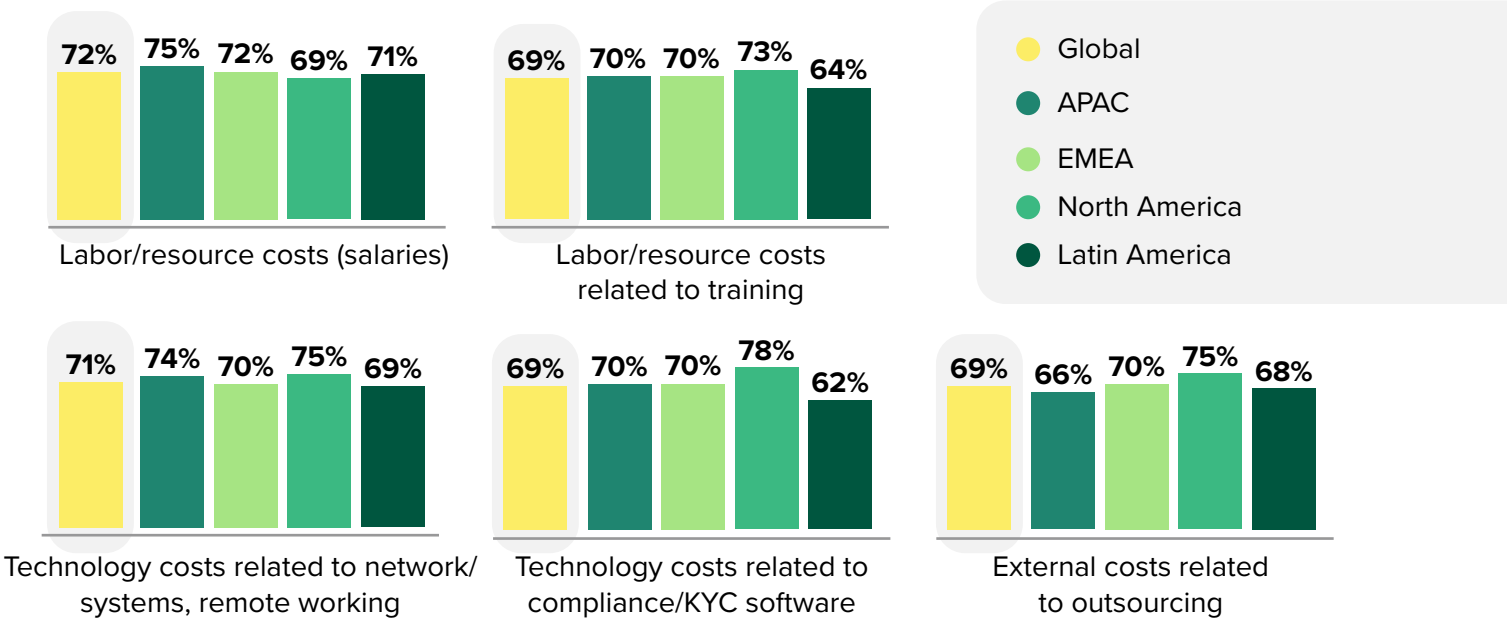
Driven by digital transformation, increasingly complex regulatory environments, and the need for highly skilled labor, these costs impact multiple areas of operations. Our study found that cost increases varied across regions (see Figure 4). Labor costs in the form of salaries were the biggest cost increase for APAC (75%), EMEA (72%), and Latin America (71%), while North America saw the highest increase in technology costs related to compliance and KYC software (78%).

Globally, the main cost components contributing to surging expenditure in FCC are:

- **The price of expertise and technology.** Salaries for full-time and part-time employees involved in FCC are escalating, impacting 72% of respondents. Additionally, as financial institutions pivot toward digital operations and remote working, related technology costs have increased for 71% of respondents. Furthermore, 69% of respondents cited a rise in compliance/KYC software-related costs, highlighting the expense of the technological investment needed to meet stringent compliance requirements.
- **The hidden cost catalysts of outsourcing and training.** Outsourcing is another significant contributor, with 69% of respondents noting an increase in these external costs. Moreover, the costs associated with staff training in FCC-related roles are also on the rise, impacting 69% of respondents. This emphasizes the reality that building in-house expertise, while essential, comes with its own price tag.

FIGURE 4

Percentage Of Companies Reporting An Increase* In FCC Costs In The Last 12 Months



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
*Note: Increase of 1% to 20% or more
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

The Rising Tide Of Technological Manipulation

The digital age has brought forth a plethora of opportunities for growth and innovation within the financial sector. However, this evolution is a double-edged sword: Our latest data reveals that these opportunities have also led to a new era of financial crimes. Once seen as catalysts for progress, cryptocurrencies, digital payments, and AI technologies are now also tools for illicit activities. Furthermore, increasingly sophisticated criminal methodologies are adding to the complexity of FCC management, while institutions must keep pace with an already complex regulatory landscape (see Figure 5).

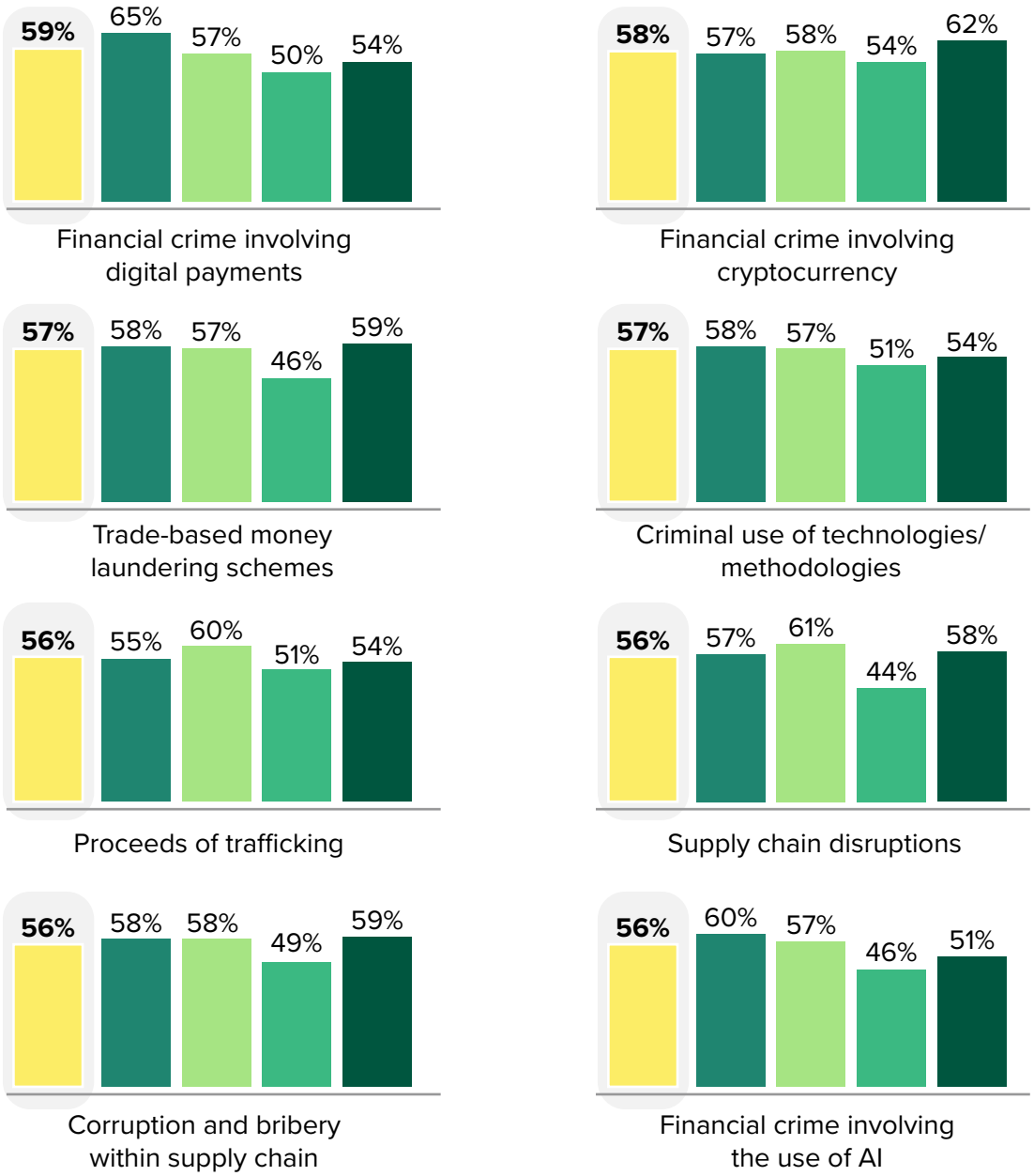
- **Digital payments bring in new kinds of digital fraud.** A striking number of respondents reported a surge in financial crimes facilitated by digital payments (59%), cryptocurrencies (58%), and AI technologies (56%). These attacks exploit vulnerabilities in digital payment systems by using sophisticated techniques to impersonate users, conduct phishing scams, or manipulate transactions. These findings reveal an immediate need to combine technological advances with forward-thinking regulatory measures.
- **Supply chain disruptions.** Exposure to both trade-based money laundering schemes (57%) and corruption within supply chains (56%) grew over the past year, indicating a significant risk in supply chain operations. Bribery and corruption are among the top five issues across all four regions. Criminals exploit corrupt practices to manipulate invoices, customs declarations, and shipping documents, facilitating undetected money flows. The complexity and vastness of global trade systems make them fertile ground for such schemes, requiring a meticulous and sophisticated approach to risk management.

> In North America and Latin America, financial crime involving cryptocurrency tops the list. Geopolitics is taking a toll on EMEA, with 61% reporting supply chain disruption. APAC respondents are particularly vulnerable to financial crime involving digital payments (65%) and AI (60%).

FIGURE 5

"Please rate the degree to which your firm's exposure to the following has increased during the past 12 months."

(Top eight responses; showing responses of "An increase of 11% to 20% or more")



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

UNPACKING FCC COST DRIVERS

The study exposes a potent mix of forces propelling a surge in FCC costs over the past year. Topping the list at 38% is the increasing burden of financial crime regulations, a testament to the ever-tightening regulatory environment. Simultaneously, the escalating demand for advanced automation, intricate data analytics, and powerful tools drives cost escalation for 32% of respondents, underscoring the shifting technological landscape (see Figure 6).

Meanwhile, evolving criminal threats pose a challenge for 29% of respondents, reflecting the sophistication of financial crime in our digital age. The aftershocks of the banking and financial crisis also add pressure for 29% of respondents, underlining the industry's inherent vulnerabilities. Last but not least is the necessity for integration into digital channels and the requirements for comprehensive electronic KYC (eKYC) controls; 27% of respondents mentioned this as driving increased costs.

These pivotal drivers highlight the complexity of the obstacles confronting today's financial institutions and underscore the need to adopt a robust, agile strategy when navigating the labyrinth of financial crime compliance.

FIGURE 6

The Top Five Most Significant Factors Driving An Increase In FCC Costs Over The Past 12 Months

(Showing top five responses)

Base: 1,156 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

Decoding The Intricacies Of Compliance Screening Operations

Compliance screening acts as the financial world's frontline defense, aiming to detect and deter financial crime, protect an institution's reputation, and satisfy regulatory demands. Vital processes such as KYC, risk profiling, and sanctions screening play a pivotal role in shaping a secure, compliant financial ecosystem. However, the complex and dynamic nature of these operations brings its own set of challenges, including (see Figure 7):

- **Navigating the maze of KYC for account onboarding.** The KYC process during account onboarding is the sternest challenge, ranking as respondents' primary concern. This vital checkpoint is designed to validate a customer's identity and assess their potential risks, but it often gets mired in complex and time-consuming procedures, creating potential bottlenecks and slowing down the onboarding process. Our study revealed that the top three challenges that decision-makers face with regard to KYC are identifying direct and indirect relationships between business entities (45%), the lack of critical identifying attributes of a business (44%), and the lack of effective KYC risk profiling of business entities (42%).

Financial institutions in North America and Latin America rank KYC for account onboarding as their number one challenge. Respondents in EMEA struggle the most with customer risk profiling, while APAC is most affected by regulatory reporting.

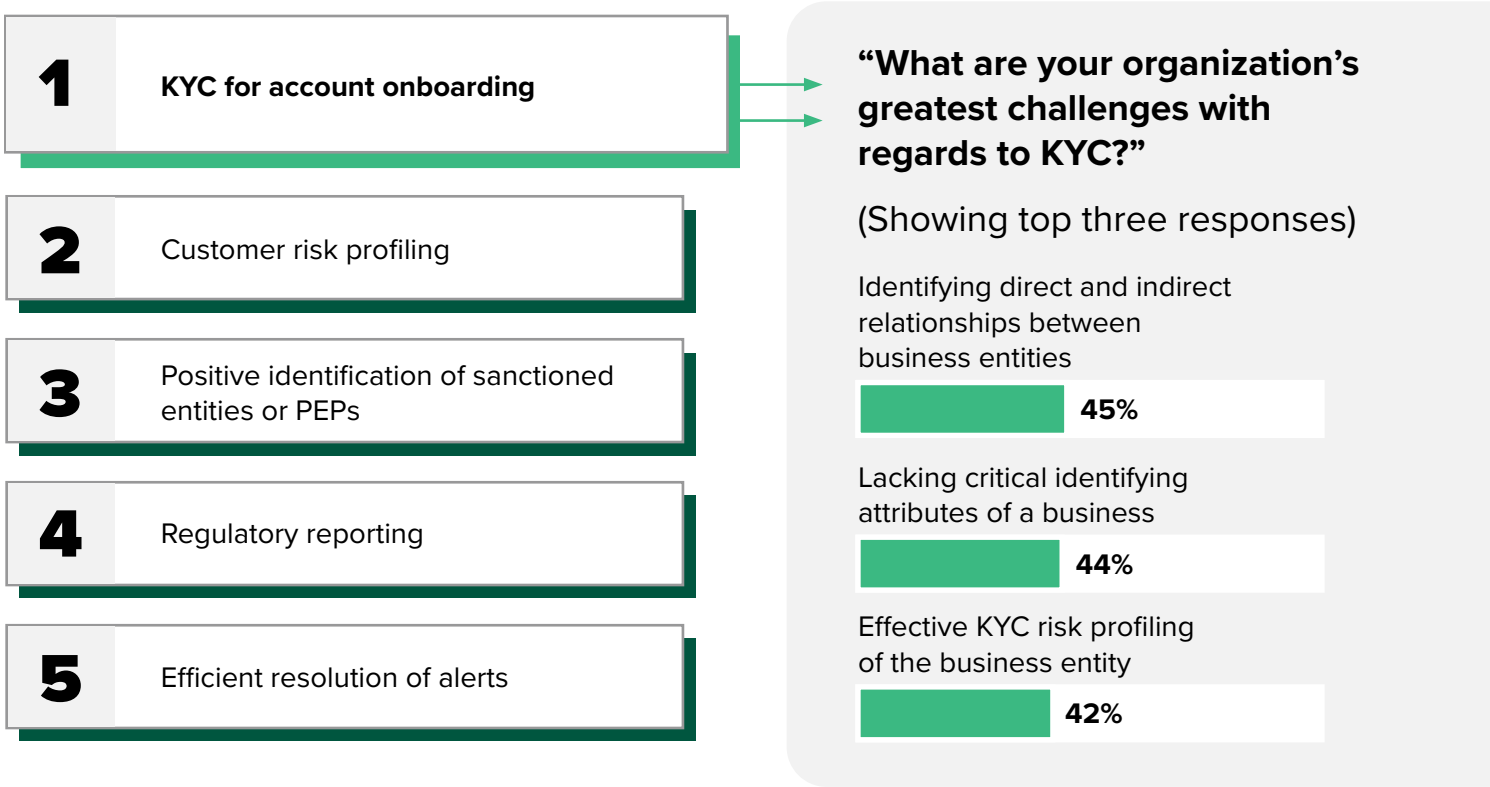
- **Mastering the art of customer risk profiling.** Customer risk profiling is the second key impediment for decision-makers. This task necessitates assessing a customer's risk level based on numerous, often-changing factors. The challenge of accurately categorizing risk profiles and updating them as variables shift can form substantial operational roadblocks. Successfully identifying sanctioned entities or politically exposed persons (PEPs) ranks as respondents' third-biggest challenge. With global sanctions constantly fluctuating and the status of PEPs being dynamic, maintaining up-to-date records becomes a formidable task, amplifying the intricacies of compliance operations.

- **Ensuring timely and accurate regulatory reporting.** Accurate and comprehensive regulatory reporting ensures that financial institutions comply with regulations by providing transparency to regulators and authorities. However, the complex regulatory landscape and frequent regulatory changes, paired with data and technology challenges, make regulatory reporting one of the main pain points that respondents identified.
- **Resolving alerts successfully.** It comes as no surprise that organizations struggle with efficient alert resolution because respondents reported an increase in screening alert numbers. False positives, data fragmentation, and regulatory pressure are likely just some of the reasons that make alert resolution a challenging task.

FIGURE 7

The Top Five Challenges For Compliance Screening Operations

(Top five responses that ranked among respondents' top three)



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

Charting The Future Of FCC: Reshaping Operations For Efficiency And Customer Experience

Financial institutions are compelled to reevaluate their existing FCC processes to tackle evolving cyberthreats, increased regulatory pressures, and the relentless pace of technological advances. Some of the measures planned over the next three to five years include targeting improved data quality, KYC procedures, internal compliance solutions, anti-money-laundering (AML), and transaction monitoring. Coupled with anticipated benefits like enhanced collaboration, simplified products, and improved efficiencies, these changes are projected to transform FCC management while promoting improved customer and employee experiences (see Figure 8). Respondents want to:

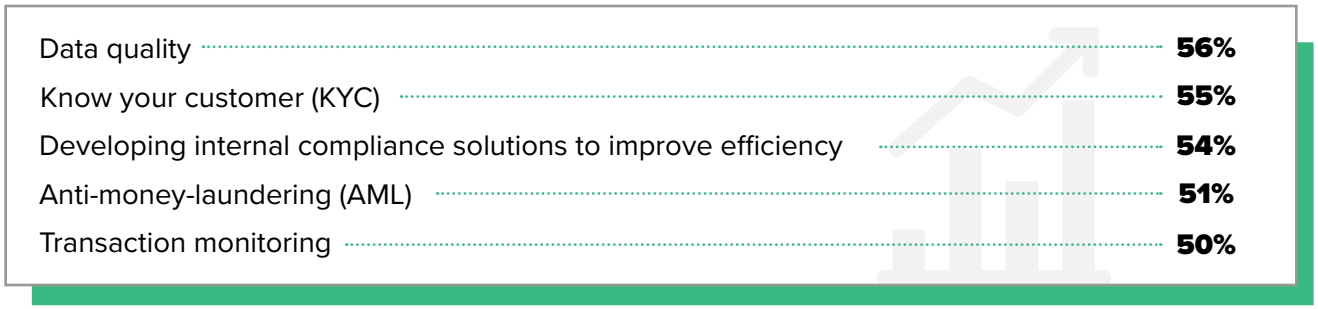
- **Raise the bar on data quality and KYC procedures.** Respondents are turning their attention to the foundation of their compliance process, with data quality (56%) and KYC processes (55%) topping the list of areas set for change. KYC and data quality are both integral to ensuring the integrity of the financial system and preventing financial crimes. High-quality data is essential for risk profiling, transaction analysis, and regulatory reporting; it also ensures a good customer experience by avoiding delays in account opening, onboarding, and transaction processing.
- **Unleash efficiency and control for internal compliance solutions and AML.** Our survey revealed that 54% of respondents plan to develop internal compliance solutions to improve efficiency, while 51% aim to overhaul their AML procedures. This indicates a shift toward self-reliance and optimizing existing operations, paving the way for greater control over compliance processes and the efficient detection and deterrence of illicit activities.
- **Envision a cohesive ecosystem to enhance collaboration and simplified experiences.** The expected benefits reveal an emphasis on internal collaboration and process simplification: 57% of respondents expect improved collaboration between compliance and payment teams, while 56% foresee simplified compliance products and integration into existing payment models. Organizations can strengthen their overall financial crime compliance efforts by leveraging each team's expertise and insights; this will reduce risks and enhance their ability to identify and hinder illicit activities.

These benefits not only promise improved operational efficiencies (53%) but also better customer (49%) and employee experiences (47%), indicating a holistic approach to revamping compliance processes.

FIGURE 8

"Which parts of the financial crime compliance process does your organization plan to change over the next three to five years?"

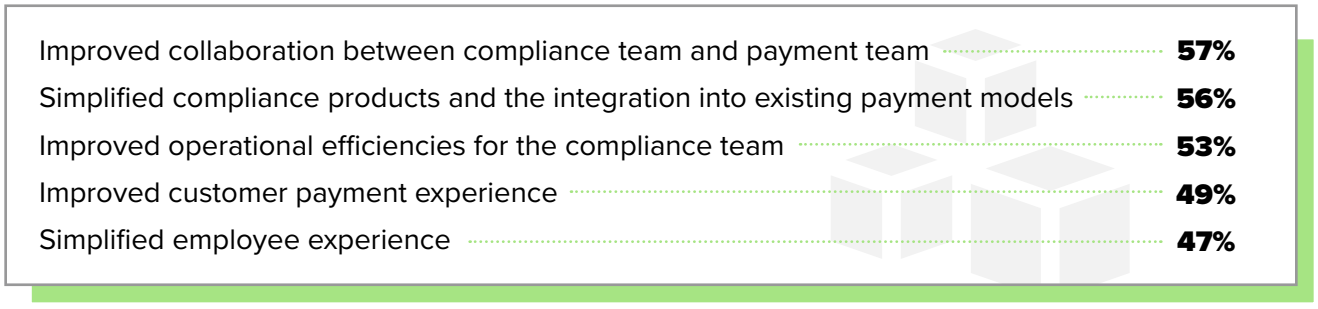
(Showing top five responses)



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

"What benefits do you expect as a result of changing your organization's financial crime compliance process?"

(Showing top five responses)



Base: 1,171 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

Unlocking Business Value With Enhanced Data Management

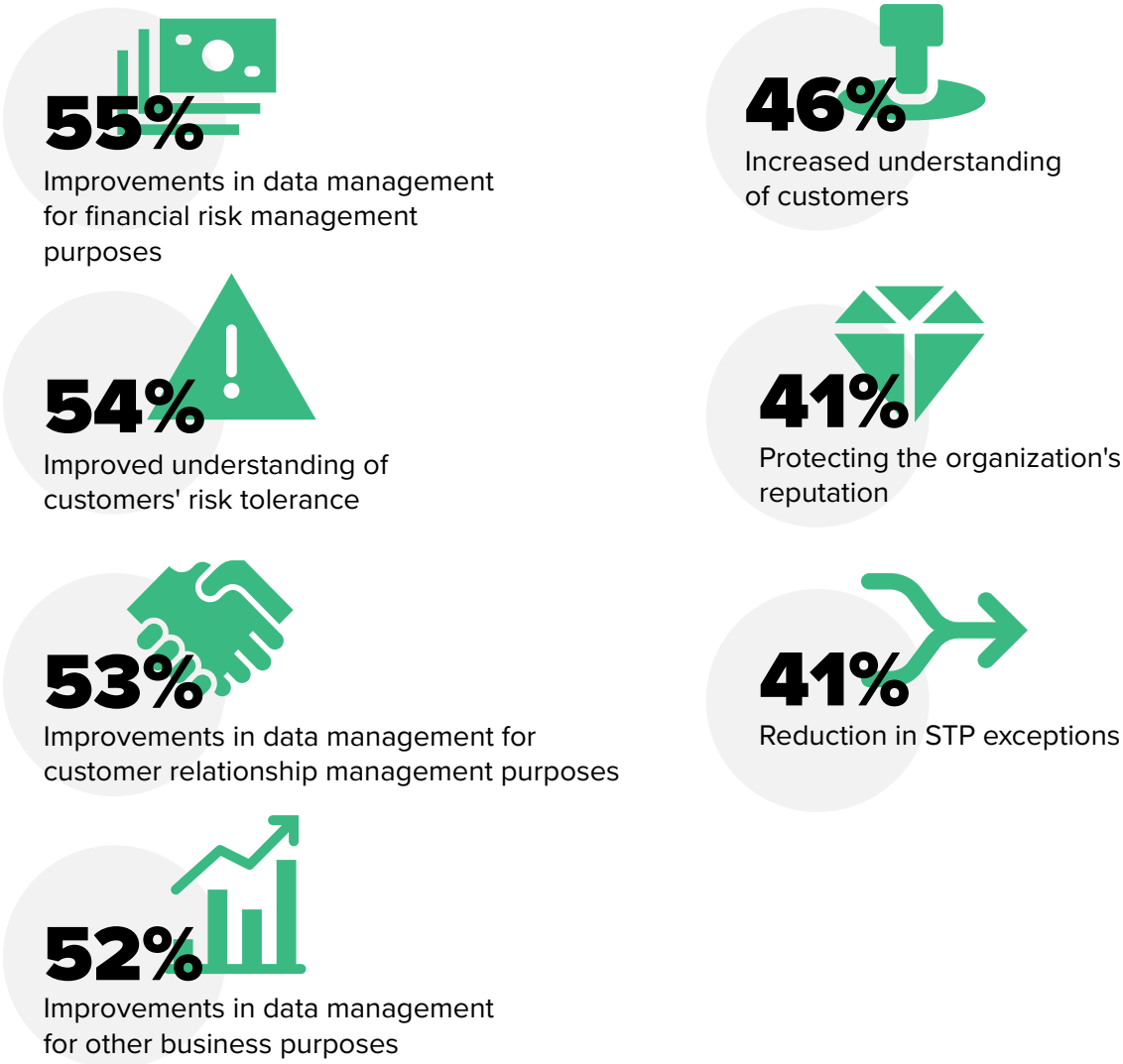
The expected business benefits for financial institutions offer a glimpse into their core objectives as they strategize about their future compliance landscape. At the forefront are data management improvements for financial risk management, an improved understanding of customers' risk tolerance (e.g., for suitability purposes), and better customer relationship management. Alongside protecting the organization's reputation and improving operational efficiency, these benefits make clear the dual role of compliance — safeguarding institutions while driving business value (see Figure 9). Respondents want to:

- **Elevate data management from a risk and relationship angle.** Institutions anticipate a significant upside to compliance changes in the realm of data management: 55% of respondents expect improvements in data management for financial risk management purposes, while 53% foresee enhancements in customer relationship management. These improvements are not only central to risk mitigation and regulatory reporting but also essential for nurturing customer relationships and ensuring personalized engagement. Organizations that prioritize data accuracy, integration, and advanced analysis are better positioned to detect and prevent financial crimes.
- **Incorporate customer insights into risk tolerance and understanding.** Understanding customers' risk tolerance (54%) and gaining increased understanding of customers (46%) rank high among the anticipated benefits. Institutions are increasingly recognizing the value of compliance processes in generating deep insights into customer behavior and risk profiles, enabling better suitability assessments and driving customer-centric decision-making.
- **Improve efficiency and safeguard their reputation.** The benefits extend beyond risk and relationship management, encompassing operational efficiency and reputation management: 41% of respondents anticipate a reduction in straight-through-processing (STP) exceptions; 41% expect a boost to the organization's reputation. These benefits underline the role of efficient compliance operations in enhancing process speed, reducing errors, and protecting the institution's brand image.

FIGURE 9

"Which of the following do you see as benefits to the business brought by financial crime compliance?"

(Showing top seven responses)



Base: 1,181 global decision-makers at financial institutions with responsibility for financial crime compliance strategy
Source: A commissioned study conducted by Forrester Consulting on behalf of LexisNexis® Risk Solutions, June 2023

Key Recommendations

While the rapid shift to real-time payments and digital channels has accelerated global business, it is imperative that this doesn't come at a cost to compliance. Current economic and geopolitical uncertainties have added even more complexity to financial crime compliance. Financial institutions must reexamine their compliance functions to identify the actions and investments that are crucial to keeping pace with change and managing compliance costs effectively while continuing to deliver instant and secure financial services to their customers.

Forrester's in-depth survey of 1,181 global decision-makers at financial institutions about financial crime compliance yielded several important recommendations:

Balance compliance effectiveness with customer experience.

In the digital era, financial institutions are in a battle to acquire and retain customers. Those that can deliver seamless customer onboarding and transaction experiences will be the winners. Striking the balance between CX and FCC efficiency entails streamlining KYC and onboarding processes, reducing false positives, and letting a higher number of legitimate transactions go through without inconveniencing the customer.

Find the right FCC partner to manage costs and improve efficiency.

Labor costs top the list of FCC spending and contribute to the biggest cost increases in APAC, EMEA, and Latin America. While in-house compliance teams with expertise are essential, financial institutions should also leverage external FCC technology providers to help reduce some of the labor costs and improve compliance efficiency. To find the right partner, organizations should zoom in on their future fit capabilities, such as proven FCC expertise for digital financial services, ease of integration, data management capability, advanced analytics, lightweight software-as-a-service deployments, and the ability to balance FCC effectiveness with CX.

Embrace new technologies to respond to new financial crimes.

Criminals are increasingly using new technologies such as AI, cryptocurrencies, and digital channels to carry out their activities. To beat the cybercriminals and thwart their more sophisticated financial crimes, financial institutions must be equipped with advanced AI- and ML-based compliance models; they must also leverage privacy-preserving technologies and advanced analytics in their FCC solutions to identity new crime patterns rapidly.

Appendix A: Methodology

In this study, Forrester conducted an online survey of 1,181 senior decision-makers at financial institutions in EMEA, APAC, North America, and Latin America to evaluate the cost, current state, and challenges presented by financial crime compliance operations. Survey participants included decision-makers for financial crime compliance. Questions provided to the participants asked about organizations' priorities; exposure to financial crime activities; financial crime spend and factors driving an increase in financial crime costs; challenges in compliance screening operations; the benefits of financial crime operations; and future implementation plans. Respondents were offered a small incentive as a thank-you for time spent on the survey. The study began in May 2023 and was completed in June 2023.

Appendix B: Demographics

REGION	
EMEA	**41%**
APAC	**23%**
Latin America	**23%**
North America	**13%**

AREAS OF RESPONSIBILITY*	
Financial crime compliance	**75%**
KYC/customer due diligence	**56%**
Anti-money-laundering policies and procedures	**50%**
Internal audit and reporting	**49%**
Transaction monitoring	**46%**
Risk assessment and effective risk management	**45%**
Reporting SARs and DAMLs	**45%**
Sanctions monitoring	**44%**
Managing compliance data/IT systems	**30%**

TOTAL ASSETS UNDER MANAGEMENT (AUM)	
Small (AUM<$10B)	**36%**
Medium/large (AUM>$10B)	**64%**

TYPE OF FINANCIAL INSTITUTION	
Investment bank/securities firm	**20%**
Retail bank	**20%**
Wholesale/commercial bank	**19%**
Insurance company	**17%**
Asset management firm	**16%**
Money services business (MSB)	**7%**

JOB-LEVEL	
C-level executive	**24%**
Vice president	**34%**
Director	**42%**

Note: Percentages may not total 100 due to rounding.
*Note: Respondents must have responsibility for one or more of these areas.

Appendix C: Endnotes

[1] For the purposes of this research, Mexico is classed as part of Latin America.

FORRESTER®