True Cost of Financial Crime Compliance Study

INDIA EDITION

LexisNexis®
RISK SOLUTIONS

BACKGROUND & OBJECTIVES

LexisNexis® Risk Solutions has conducted a global survey of its True Cost of Financial Crime Compliance study. The following report presents findings for the India market.

Specific objectives included to:

- **Identify the drivers and influencers** impacting financial crime compliance;

- **Understand spending trends** for financial crime compliance, including:
  - How spending is divided by cost of compliance area (e.g., sanctions, transaction monitoring, technology, KYC due diligence, etc…);
  - The human resources component of these costs, particularly numbers of FTEs for compliance and sanctions screening; and
  - The processing time component (e.g., length of time to complete customer due diligence by type of client/entity);

- **Determine the business impact** of the financial crime compliance environment, particularly with regard to new regulations and provisions; and

- **Identify any challenges and impacts** associated with the COVID-19 pandemic.

LexisNexis® RISK SOLUTIONS

METHODOLOGY

LexisNexis® Risk Solutions retained KS&R, a global market research firm, to conduct this research study.

Data was collected by phone during September and October 2020 with a total of:

50 completions across the **India** market

Respondents included decision makers within the financial crime function who oversee KYC remediation, sanctions monitoring, financial crime transaction monitoring and/or compliance operations. Organisations represented banks, investment firms, asset management firms, and insurance firms.

LexisNexis® Risk Solutions was not identified as the sponsor of the research in order to lessen potential for brand bias.

In this report, **firms are referred to in terms of their asset size** and defined as:

- Small asset size – having <$10B total assets
- Mid/large asset size – having $10B+ total assets.

All currency references in this report are based on USD.

KEY FINDINGS

1. **The cost of financial crime compliance** is higher for larger Indian financial institutions; labour is a contributing factor regardless of size.

2. **Customer risk profiling**, KYC for account onboarding, increasing alert volumes, and alert clearance times have negatively impacted productivity and customer acquisition efforts.

3. **The COVID-19 pandemic** has added to financial crime compliance operations challenges and costs. Most mid/large firms expect to spend more over the next 12 - 24 months to address continued negative impacts; much of this will be in risk technology.

4. Though they can be challenging, **financial crime compliance activities provide various benefits** to Indian financial institutions, allowing for more effective risk management and management of customer relationships.

5. **Financial institutions that have invested in technology solutions**, to support financial crime compliance efforts, have experienced less severe impacts to cost and compliance operations.

LexisNexis® RISK SOLUTIONS

KEY FINDING 01

The cost of financial crime compliance is higher for larger Indian financial institutions; labour is a contributing factor regardless of size.

The total projected cost of financial crime compliance across financial institutions in India is $5.51B.

Not surprisingly, the average annual cost of financial crime compliance is significantly higher for mid/large financial firms, that employ larger teams and have higher screening volumes than smaller ones.

Regardless of firm size, spend is more heavily weighted toward labour and KYC programs.

Background & Objectives

Methodology

Key Findings

Key Finding 01

Key Finding 02

Key Finding 03

Key Finding 04

Key Finding 05

Implications

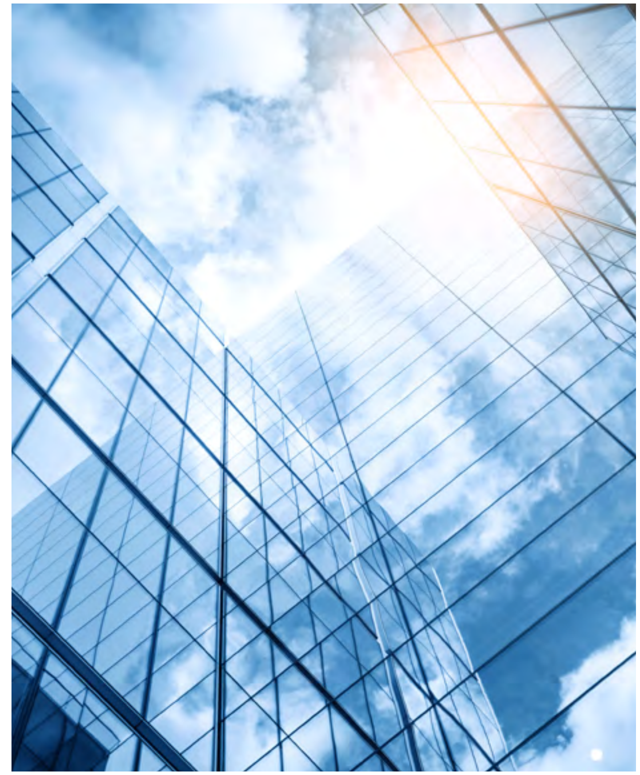
KEY FINDING 01
Projected Total Cost of Financial Crime Compliance Across Financial Institutions

The total projected cost of financial crime compliance across financial firms in India is $5.51B for 2020.

Given recent changes in legislation, as well as the number of organisations – such as Primary Agricultural Credit Societies (PACs) – that do not currently fall under the purview of the Prevention of Money Laundering Act, 2002 (PMLA), this number could be higher.

$5.51B

Projected Total Cost of Financial Crime Compliance* Across Financial Firms



Q5: Please give your best estimate of the total annual cost of your financial crime compliance operations in USD. This includes resources/labour, systems/solutions/data and other governance activities for all aspects of compliance such as customer due diligence, sanctions screening, transaction monitoring, investigations, etc…

* Total annual cost of compliance across firms within the India market is calculated using two sources of information: 1.) secondary data that provides a list of all FIs in each market, along with the total assets for each organisation; and, 2.) survey data regarding financial crime costs as a percent of total assets. A spend amount is generated for each FI by multiplying its reported total asset amount by the average percent that financial crime costs represent of that amount. As demonstrated above, the average percent of spend-to-assets varies by organisation size; therefore, this calculation is conducted separately for each asset-size category and then summed for an overall total. While the survey included range of decision makers for financial crime compliance, it can be difficult for some portion of them to know the exact spend as more compliance work gets delegated down to operational and business units. Therefore, there could be some variance in the total cost amount. However, a census-type calculation, as described above, brings rigor to the process and should ensure a good estimation of total spend in the India market.

KEY FINDING 01
Background and Financial Crime Compliance Cost Drivers

While India has made strides to improve its AML framework, including to propose regulations to manage anti-money laundering (AML) and know-your-customer (KYC) compliance related to cryptocurrencies, it continues to face ongoing money laundering risks. Hawalas, complex onshore and offshore corporate structures, and enforcement capacity constraints remain challenges.

REGULATORY PRESSURES

- Though operating under the Prevention of Money Laundering Act, 2002 (PMLA) and additional amendments introduced in 2019 to broaden the definition of "proceeds of crime", India is categorised as a major money laundering, drug transit, and precursor chemical country by the 2019 U.S. International Narcotics Control Strategy Report.[1]
- India has been advised to address shortcomings in the criminalisation of money laundering and its domestic framework for confiscation and provisional measures, including to:[2]
  —ensure all relevant Designated Non-Financial Businesses and Professions (DNFBPs) comply with AML regulations
  —extend its safe harbour provision to cover all bank employees
  —use data and analytics to systematically detect trade anomalies that could indicate customs fraud, Trade-Based Money Laundering (TMBL), and counter-valuation in informal financial networks
- The Reserve Bank of India (RBI) issued guidelines to regulate payment aggregators/payment gateways that act as intermediaries facilitating online payments, taking effect from April 1, 2020. All non-bank PAs are now required to obtain RBI licenses and comply with the guidelines' requirements on: net worth, governance, KYC/anti-money laundering and combatting the financing of terrorism (AML-CFT), etc.[3]
- Additionally, RBI has introduced risk-based internal audit norms for large urban cooperative banks (UCBs) and non-banking financial companies (NBFCs), as part of measures aimed at improving governance and assurance functions at supervised entities.[4]

STATE OF CRYPTOCURRENCY

- Cryptocurrencies are more vulnerable to criminal activity and money laundering, by providing greater anonymity than other payment methods – the public keys engaging in a transaction cannot be directly linked to an individual.[5]
- This, in part, led the Reserve Bank of India (RBI) to implement an order in 2018 prohibiting banks from providing services to entities dealing with cryptocurrencies. This forced crypto traders to use peer-to-peer crypto trading platforms, which allow direct transfer of cryptocurrencies into individual accounts without the intervention of any financial institution or government authority.[6]
- However, India's Supreme Court overturned the restriction in March of this year. India currently lacks a regulatory framework, but proposed regulations hope to address the risks of cryptocurrency, by bringing it under existing regulations, while also setting up a supervised space for start-ups to develop in the sector. The proposal also involves developing an open-source interface to track crypto transactions and manage anti-money laundering (AML) and know-your-customer (KYC) compliance.[7]
- Prior to the ban, India was doing well in terms of trading volumes, contributing about $50 million to $60 million per day. With the lifting of the ban, India has the potential to become one of the largest crypto markets.[8]

ONGOING MONEY LAUNDERING RISKS

- India faces various money laundering vulnerabilities, including Informal remittance systems (or hawala), complex onshore and offshore corporate structures, and enforcement capacity constraints. Most common money laundering methods in India include intermingling criminal proceeds with licit assets, purchasing bank checks with cash, routing funds through employees' accounts, and complex legal structures.[9]
- Hawala is a way to transmit money without any currency actually moving, providing anonymity, as official records are not kept and the source of money that is transferred cannot be traced. While used to conduct legitimate remittances, it is also a vehicle for money laundering.[10]

1 2020 INCSR Money Laundering Report, US State Department
2 Ibid.
3 https://www.irglobal.com/article/new-guidelines-regulating-payment-aggregators-and-payment-gateways-in-india/
4 https://www.thehindu.com/business/Industry/rbi-tightens-oversight-of-nbfcs-ucbs/article33252974.ece
5 https://www.prsindia.org/billtrack/draft-banning-cryptocurrency-regulation-official-digital-currency-bill-2019
6 https://www.coindesk.com/after-court-victory-indian-exchanges-gear-up-for-crypto-trading-surge
7 https://www.coindesk.com/india-crypto-regulatory-sandbox
8 Ibid.
9 2020 INCSR Money Laundering Report, US State Department
10 https://www.investopedia.com/terms/h/hawala.asp

LexisNexis® RISK SOLUTIONS

KEY FINDING 01
Background and Financial Crime Compliance Cost Drivers

In addition to this and potential future risks, financial crime compliance costs have been driven higher by COVID-19.

REGULATORY SETBACKS

- Laws tied to anti-money laundering and tax evasion are now potentially viewed as a hindrance to growth. Where India was enjoying economic growth of about 9% three years ago, the rate of expansion has fallen to half that.[11]
- In an effort to reverse this slump and grow the economy to a targeted $5 trillion, the Government of India, is planning to decriminalise the Income Tax Act and the Prevention of Money Laundering Act (PMLA). They believe that decriminalizing corporate laws, settling tax disputes, and rapid privatization of state-run firms are necessary steps to reach this goal.[12]

COVID-19 IMPACTS

- FATF's review of India's anti-money laundering and terrorist financing regime was scheduled for this year, as part of a regular review cycle after 10 years. However, in light of the pandemic, this on-site review has been postponed until January or February of 2021.[13]
- While on lockdown during the pandemic, India compliance teams were forced to work at home, where internet connectivity isn't always reliable, creating a backlog of work.[14]
- Based on the findings of this surveys, financial crime compliance professionals attribute 20% of recent cost increases, on average, to the impact of COVID-19.

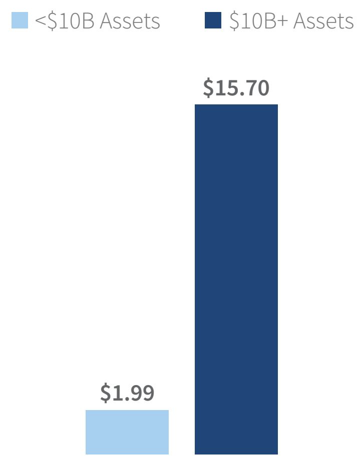
11 https://www.acfcs.org/acfcs-regional-report-india-country-pulls-back-on-aml-to-bolster-sagging-economy-on-cusp-of-fatf-visit/
12 Ibid.
13 https://www.thehindu.com/news/national/coronavirus-pandemic-pushes-fatf-review-of-indias-anti-money-laundering-and-terror-financing-regime-to-2021/article32196685.ece
14 https://www.forbes.com/sites/tomgroenfeldt/2020/04/27/software-fills-in-for-india-based-compliance-teams-in-covid-lockdown/?sh=2574281063a0

KEY FINDING 01
Annual Average and Distribution of Financial Crime Compliance Costs

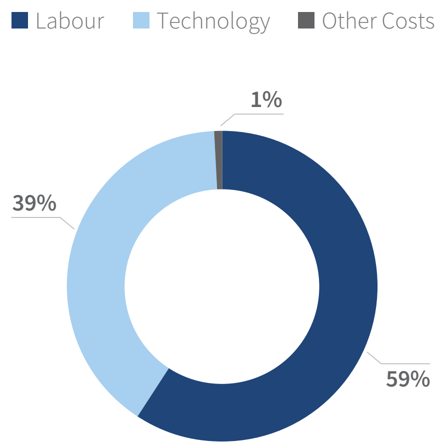
Not surprisingly, average annual compliance costs are higher for Mid/Large financial firms. But regardless of size, spend is more heavily weighted toward labour than technology.

By activity, spend is highest for KYC programs, with the remainder spread across remaining activities.

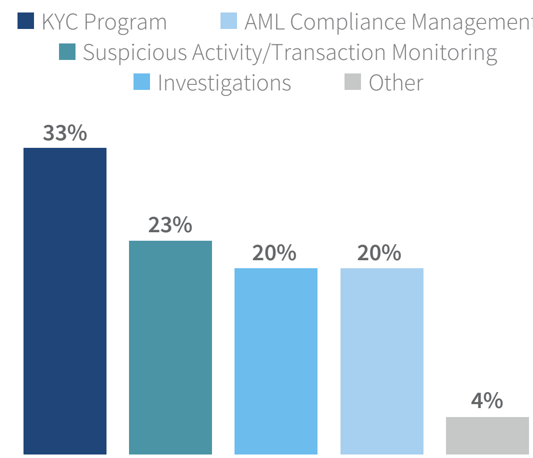
Average Annual Financial Crime Compliance Operations Costs per Organisation: ***Pre-COVID-19***
(Costs in US$ Millions)



Average Distribution of Financial Crime Compliance Operations Costs



Distribution of Financial Crime Compliance Costs by Compliance Activity

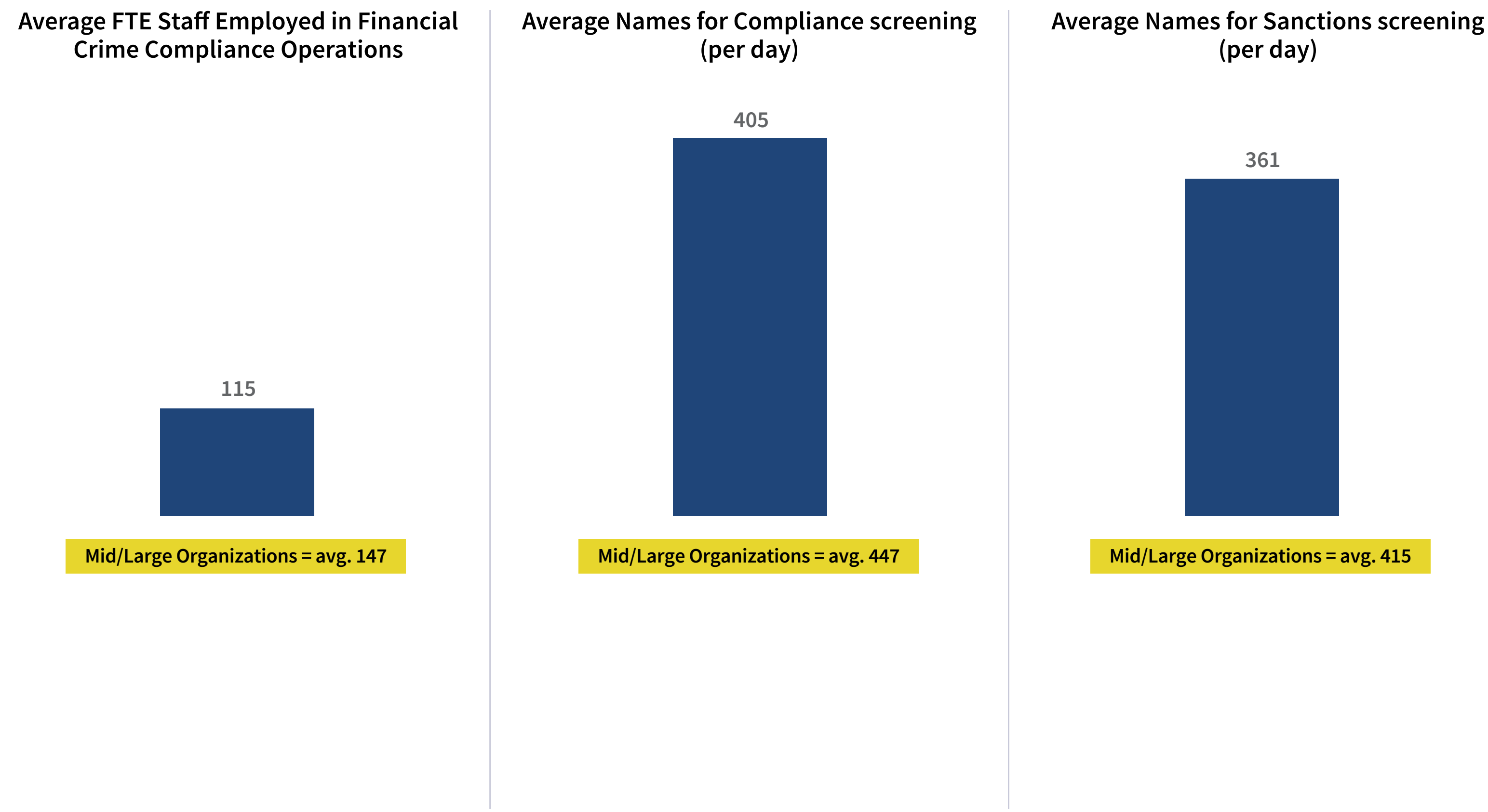


Q5: Please give your best estimate of the total annual cost of your financial crime compliance operations in USD. Q5b. What % would you say is related to labour, technology/ solutions, and other? Q6: Thinking again about the estimated total annual cost of your financial crime compliance operations, please give your best estimate of the percentage that is spent on each of the following areas.

KEY FINDING 01
Screening Volumes and Labour Contributing to Compliance Costs

Compliance teams are reported to be sizeable, with an average of 115 FTEs. These resources support screening volumes of 350+ names per day.

Teams and screening volumes are even high among mid/large financial firms.



Q2c: Please indicate your best estimate of the number of FTE staff employed in the financial crime compliance operations departments.
Q3: On average, how many names are screened per day across all of the FTE analysts in your financial crime compliance screening operations?
Q4: On average, how many names are screened per day across all of the FTE analysts in your sanctions screening operations?

LexisNexis® RISK SOLUTIONS

KEY FINDING 02

Customer risk profiling, KYC for account on-boarding, increasing alert volumes, and alert clearance times have negatively impacted productivity and customer acquisition efforts.

Retail, e-commerce, real estate, and legal/accounting are reported to pose the highest risk for financial crime.

Customer risk profiling and KYC for account on-boarding were cited as leading compliance screening challenges.

Alert volumes are increasing, with AML transaction monitoring and periodic watch-list filtering taking up to 16 hours to clear. In addition to tightening regulations, the increased use of mobile payments may be contributing to these challenges, as people are concerned with using cash during the pandemic.

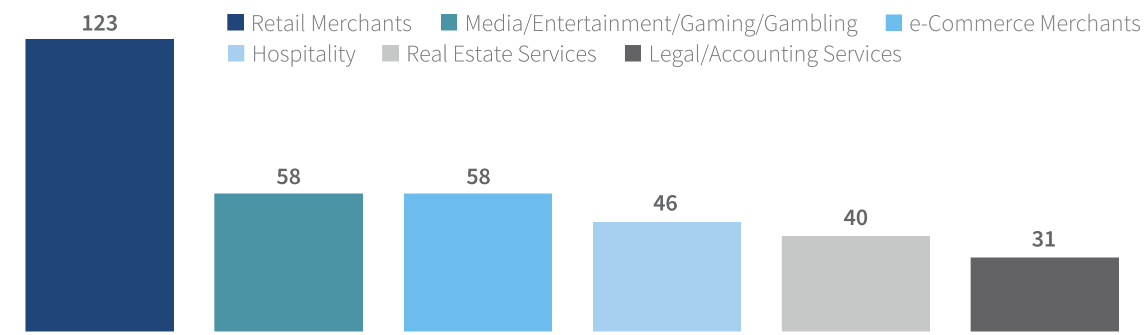
This overextends compliance teams, which decreases productivity and harms customer acquisition efforts, which, in turn, increases costs.

KEY FINDING 02
New Account Openings/Risks

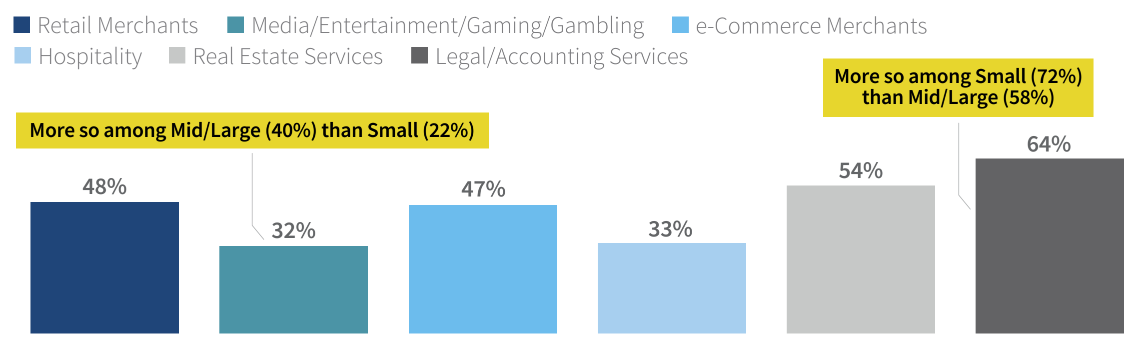
Though Indian financial firms open a number of new retail accounts per month, these are among the sectors reported to pose the highest risk for financial crime, along with e-commerce, real estate, and legal/accounting services.

Transnational criminal organisations use offshore corporations and trade-based money laundering to disguise the criminal origins of funds, and companies use TBML to evade capital controls. In fact, it is not uncommon for businesses/ professionals to collaborate with each other to use shell companies for converting illegal wealth into legitimate assets. Illicit funds are laundered through real estate transactions, as well as gold purchases, charities, election campaigns, and educational programs.[15] The most recent statistics found during the writing of this report indicate that the real estate sector accounts for 35% of money laundering cases in India.[16]

Number of New Accounts Opened Monthly



TOP 3 Sectors That Pose the Highest Risk of Money Laundering



Q1b: For each of the following, please give your best estimate of the number of new accounts opened monthly. Q1c: Please select the TOP 3 sectors that pose the highest risk of money laundering for your financial institution.

15 2020 INCSR Money Laundering Report, US State Department
16 https://indianexpress.com/article/india/enforcement-directorate-real-estate-black-money-real-estate-indian-economy-money-laundering-4930435/

LexisNexis® RISK SOLUTIONS

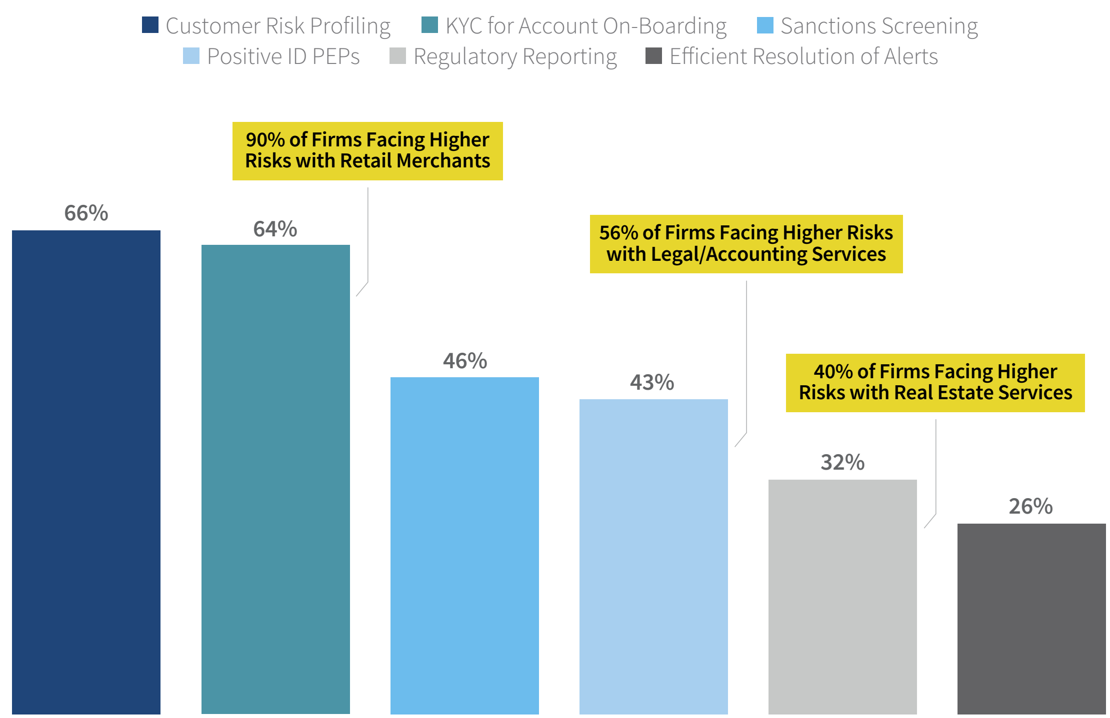
KEY FINDING 02
Financial Crime Screening Challenges

Customer risk profiling and KYC for account on-boarding lead among compliance screening challenges.

Given the widespread use of offshore and shell companies, establishing personal/customer relationships and determining ultimate beneficial ownership is likely arduous, particularly for firms that face higher risks with retail accounts.

Firms that face higher risks with legal/accounting services reported experiencing challenges with positive identification of PEPs, while those facing risk with real estate services are more likely than others to encounter issues with regulatory reporting.

Key Challenges for Compliance Screening Operations
(% Ranked Among Top 3)



Q25: What areas in your compliance screening operations face the largest challenges?

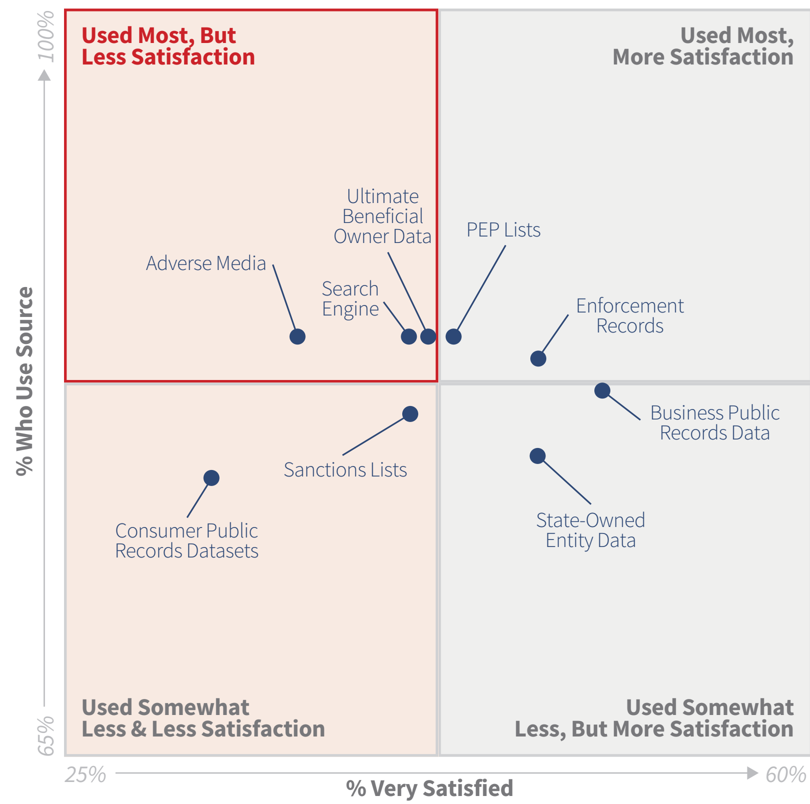
KEY FINDING 02
Financial Crime Screening Challenges

Various sources are used to screen for customer due diligence, most commonly including:
- ultimate beneficial owner data,
- PEP lists,
- adverse media,
- enforcement records, and
- search engine.

Where satisfaction tends to be lower, it is for adverse media, search engine, and UBO data.

In countries such as India, there can be hundreds of individuals with same name. Media screening, for example, will not be as simple as conducting an internet search. Compliance professionals have to consider unique identifiers to reach the conclusion that "person A" is or isn't the same "person A" found in a news article. This approach not only increases the time and costs of due diligence, but can also lead to false positives.[17]

Satisfaction With Sources Used to Screen Against Customer Due Diligence



Q17c. How satisfied are you with the quality of data you use for screening?)

17 https://indiaforensic.com/certifications/adverse-media-information-on-high-risk-customers/

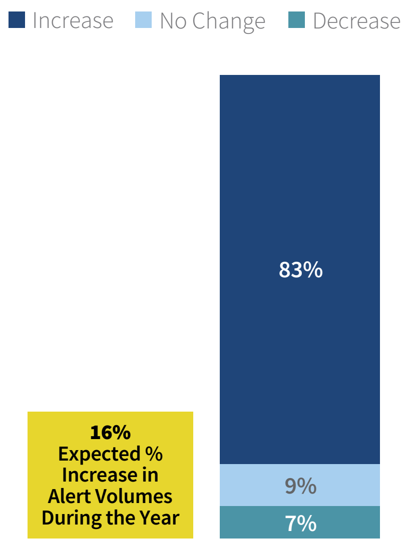
KEY FINDING 02
Alert Resolution Challenges and Impacts on Organisations

A majority expect alert volumes to increase this year, by an average of 16% compared to last year.

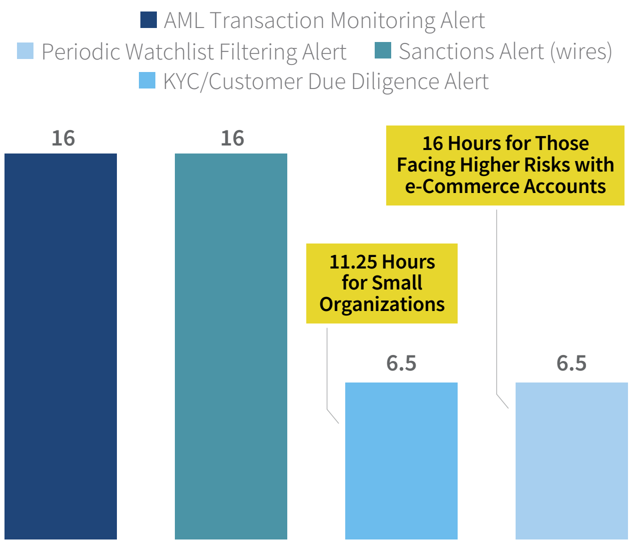
Additionally, the median time required to clear these alerts is as high as 16 hours for AML transaction monitoring and periodic watch-list filtering. Part of this is an impact from COVID-19, where a number have experienced increased alert volumes and decreased productivity/efficiency. This could be related to the increased use of mobile payments, as the pandemic has created fears around using cash and caused a need for social distancing.[18]

This growing workload causes concern, with a majority of Indian financial firms concerned with the satisfaction of their compliance employees.

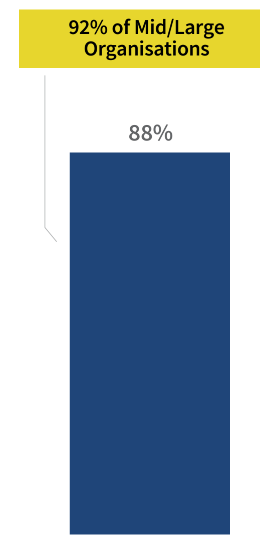
Alert Volume Expectations



Median Hours to Clear the Following Types of Alerts



% Somewhat to Very Concerned About Job Satisfaction of Compliance Staff



Q19a: Do you expect alert volumes to increase or decrease in 2020? Q18: What is the average time required for an analyst to clear each of the following alert types? Q14: How concerned are you with job satisfaction in your compliance department?

18 https://www.spglobal.com/marketintelligence/en/documents/indiamobilepayments_2020finalreport.pdf

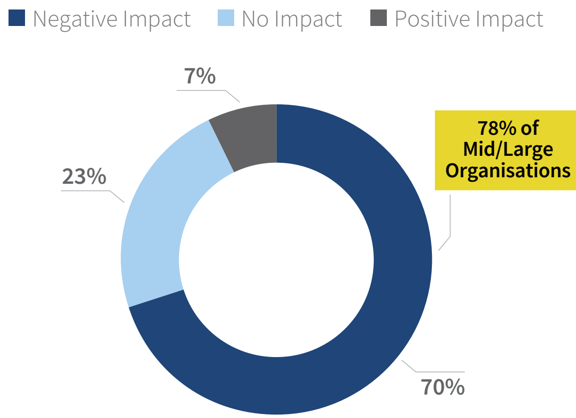
KEY FINDING 02

Impact of Financial Crime Compliance Challenges on Productivity and Customer Acquisition

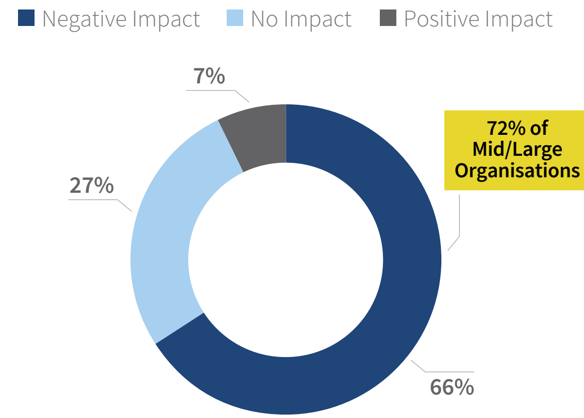
As a result of these challenges, productivity and customer acquisitions efforts have been impacted negatively for many, especially mid/large firms that experience higher screening and alert volumes.

Over half of firms are losing at least 100 hours of productivity per FTE, as well as 5% or more of customer opportunities due to refused accounts/walkouts during onboarding.

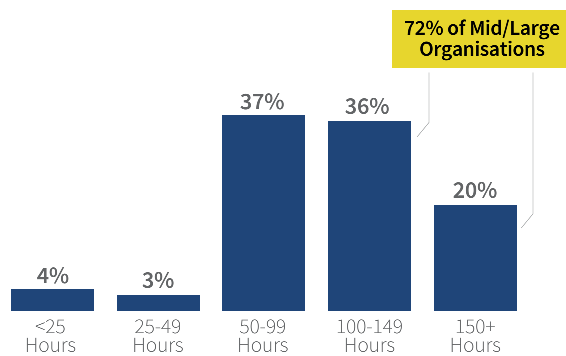
Financial Crime Compliance Impact on Productivity



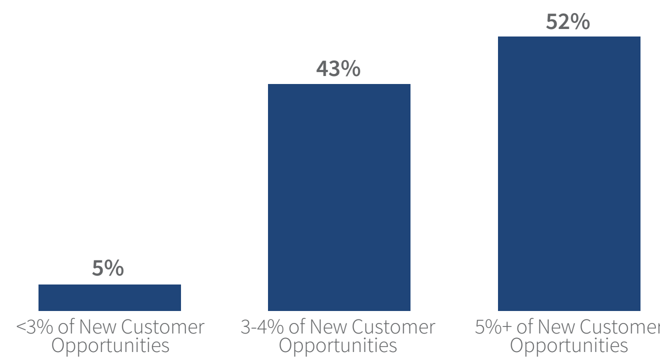
Financial Crime Compliance Impact on Customer Acquisition



Annual Loss in Productivity Due to Financial Crime Compliance



Estimated Annual Opportunity Cost of Refused Accounts or Customer Walkouts Due to Financial Crime Compliance



Q20a: What kind of impact does the financial crime compliance process have on LoB productivity? Q21: What is your best estimate of the annual loss in LoB productivity due to financial crime compliance at your firm, expressed in average hours of lost productivity per line-of-business FTE? Q22: What kind of impact does the financial crime compliance process have on customer acquisition? Q24a: What do you estimate is the annual opportunity cost of refused accounts or customer walkouts due to financial crime compliance, expressed as a percentage of new account applications?

18 https://www.spglobal.com/marketintelligence/en/documents/indiamobilepayments_2020finalreport.pdf

KEY FINDING 03

The COVID-19 pandemic has added to financial crime compliance operations challenges and costs. Most mid/large firms expect to spend more during the next 12 - 24 months to address continued negative impacts; much of this will be in risk technology.

COVID-19 has added to compliance costs, especially for mid/large financial institutions.

Financial crime compliance operations were significantly impacted by COVID-19, in areas such as sanctions screening, KYC, identification of PEPs, and alert resolution. As a result, Indian financial institutions have had to contend with resource and due diligence inefficiencies.

A majority of Indian financial firms, especially larger ones, expect COVID-19 to cause additional financial crime compliance spend over the next 1 - 2 years, with increased spend on technology.

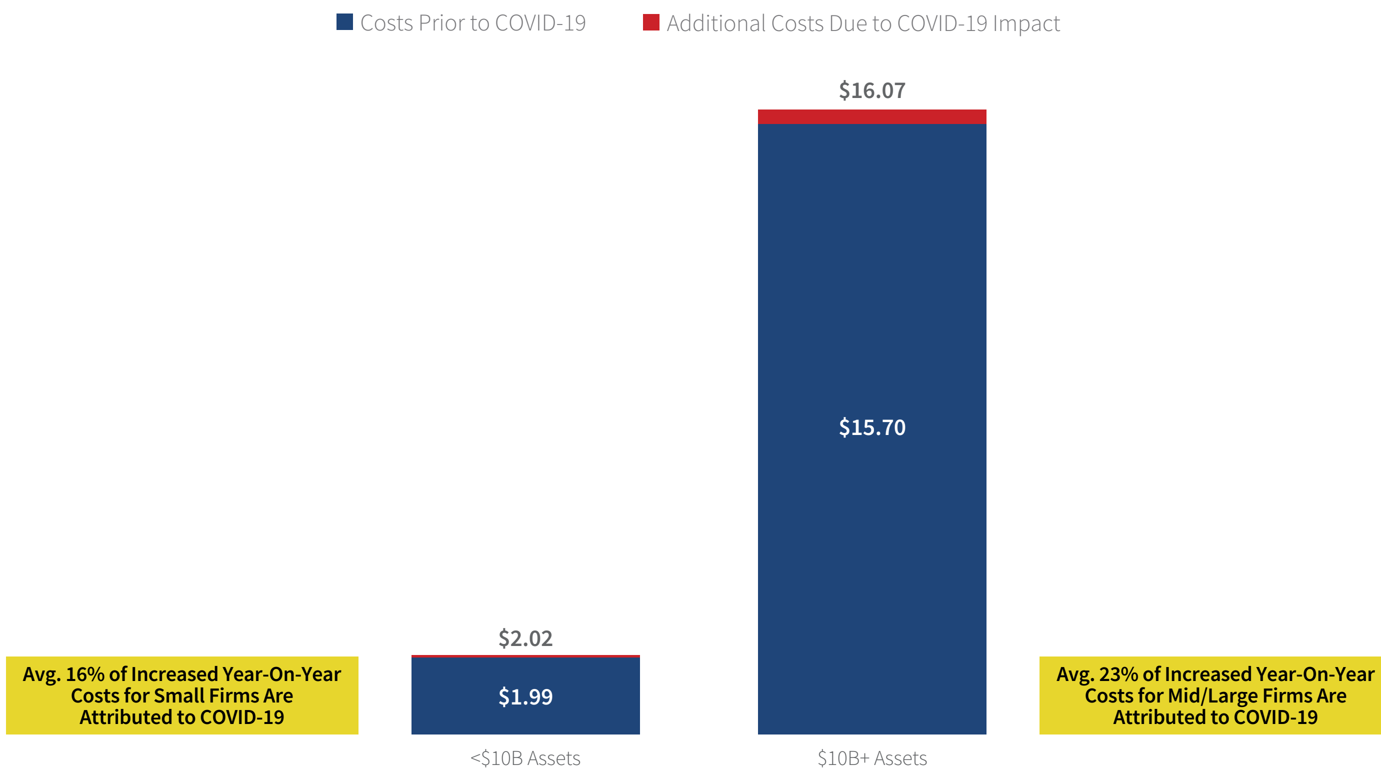
LexisNexis® RISK SOLUTIONS

KEY FINDING 03
COVID-19 Impact on Financial Crime Compliance Costs

COVID-19 added to year-on-year compliance cost increases, particularly for larger Indian financial firms.

On average, mid/large financial institutions attributed 23% of their annual compliance cost increases to the pandemic. The actual percentage that COVID-19 contributed to the cost increases could be more, given the negative impacts on the compliance process; it may be too early to assess actual cost effects.

Average Annual Financial Crime Compliance Operations Costs per Organisation: ***Including COVID-19 Impact***
(Costs in US$ Millions)

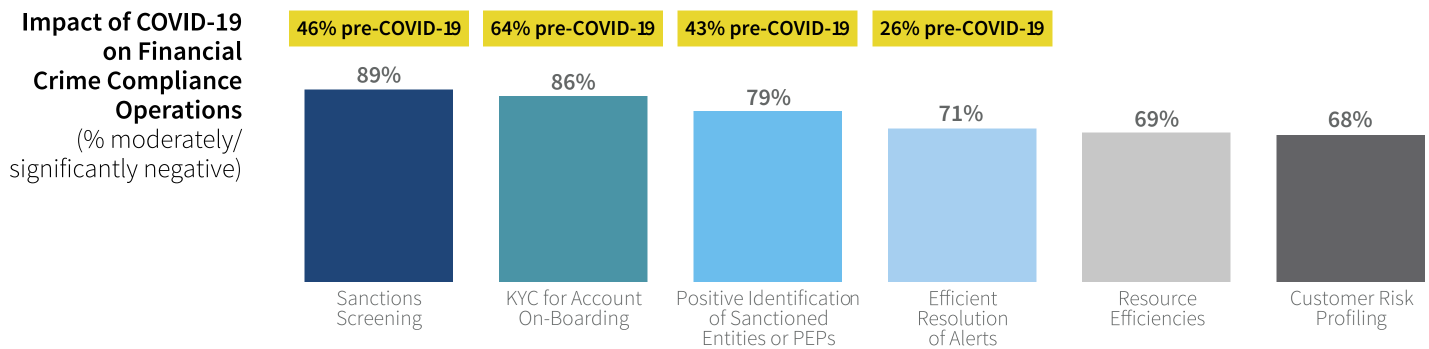


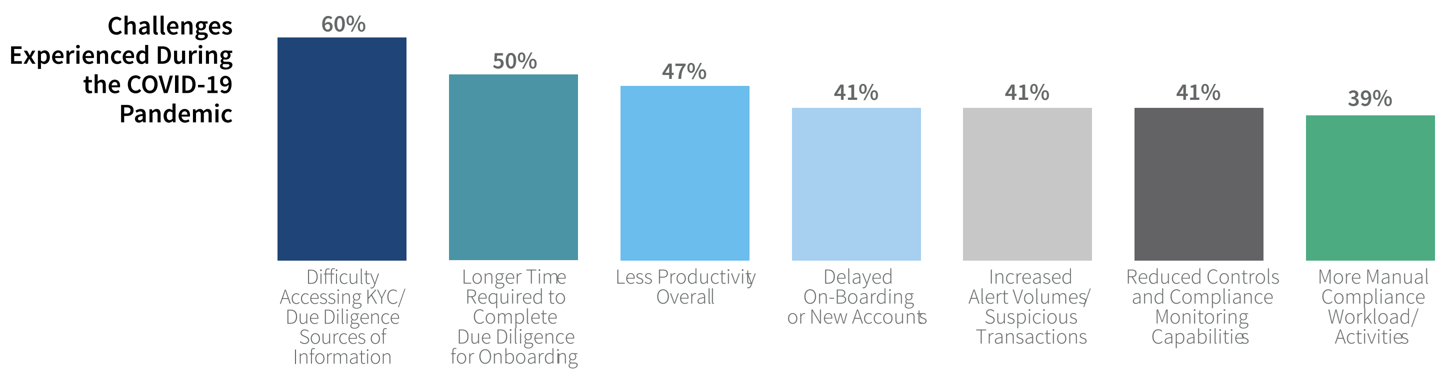
Q5: Please give your best estimate of the total annual cost of your financial crime compliance operations in USD. This includes resources/labour, systems/solutions/data and other governance activities for all aspects of compliance such as customer due diligence, sanctions screening, transaction monitoring, investigations, reporting, etc.

LexisNexis® RISK SOLUTIONS

KEY FINDING 03
COVID-19 Impact on Financial Crime Compliance Operations

Financial crime compliance operations were significantly impacted by COVID-19, especially around sanctions screening, KYC, identification of PEPs, and alert resolution, as more firms indicated these as challenges compared to pre-COVID-19.

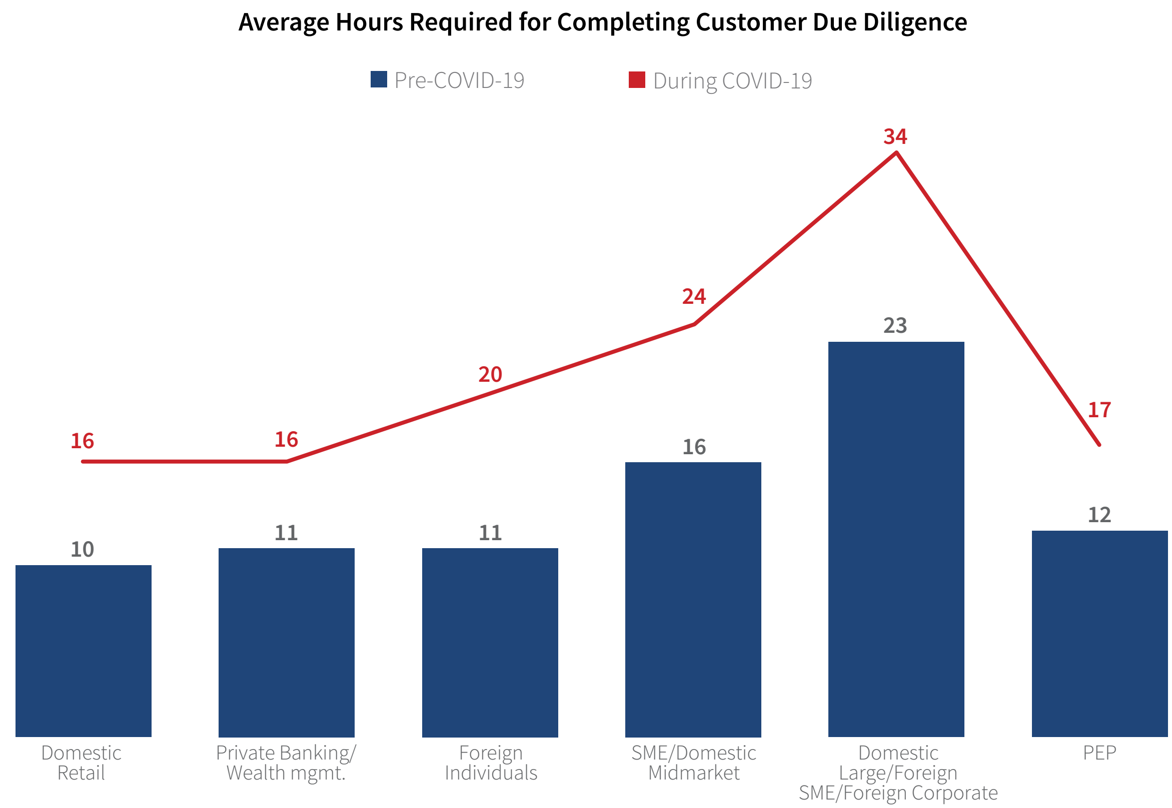




Q33: To what degree has the Covid-19 pandemic and subsequent remote working requirements negatively impacted your financial crime compliance efforts for the following: Q34: Which, if any, challenges has your financial crime compliance organisation experienced during the Covid-19 pandemic and the remote working period?

KEY FINDING 03
COVID-19 Impact on Financial Crime Compliance Costs and Operations

As a result, average due diligence times have taken between 42% - 82% longer during the pandemic, and take the longest among of time for larger and foreign business accounts.



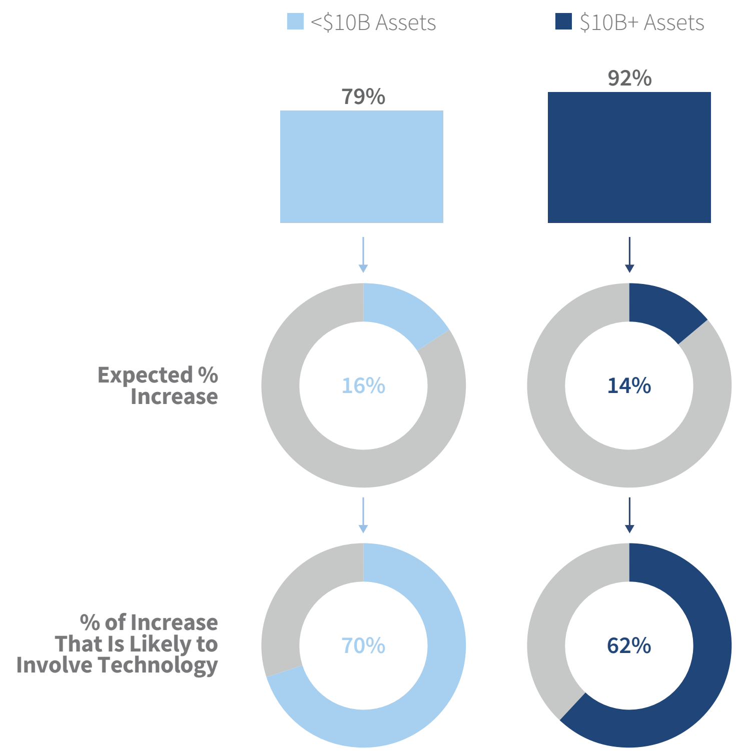
Q17a: What would you say is the average time required for completing customer due diligence on the following? Q35: Thinking only about the time period involving the Covid-19 pandemic and subsequent remote working requirements, what would you say has been the average time required for completing customer due diligence on the following?

KEY FINDING 03
Expected COVID-19 Impacts into 2021

A majority of Indian financial firms, especially larger ones, expect COVID-19 to cause additional financial crime compliance spend over the next 1 - 2 years. They estimate they could spend up to 16% on average more than they would typically.

This includes a sizeable investment in technology. Part of this could be related to the growth in mobile payments. It is predicted that social distancing measures and concerns around using cash will prompt merchants to further promote contactless payments. The widespread prevalence of low-cost, Quick Response codes could further strengthen the dominance of mobile payments. Small merchant stores, for example, are increasingly adopting standard QR codes that are compatible with solutions offered by all popular payment companies.[19]

% Expecting COVID-19 to Cause Further Financial Crime Compliance Spending over Next 12–24 Months



Q36C. Do you expect the Covid-19 pandemic to cause your organisation to spend more on financial crime compliance over the next 12 – 24 months than it ordinarily would have had the crisis not occurred? D. Distributing 100 points, what percent of these increased costs over the next 12 – 24 months, based on the Covid-19 impact, do you expect to be for technology versus labour / human resources?

19 need source

LexisNexis® RISK SOLUTIONS

KEY FINDING 04

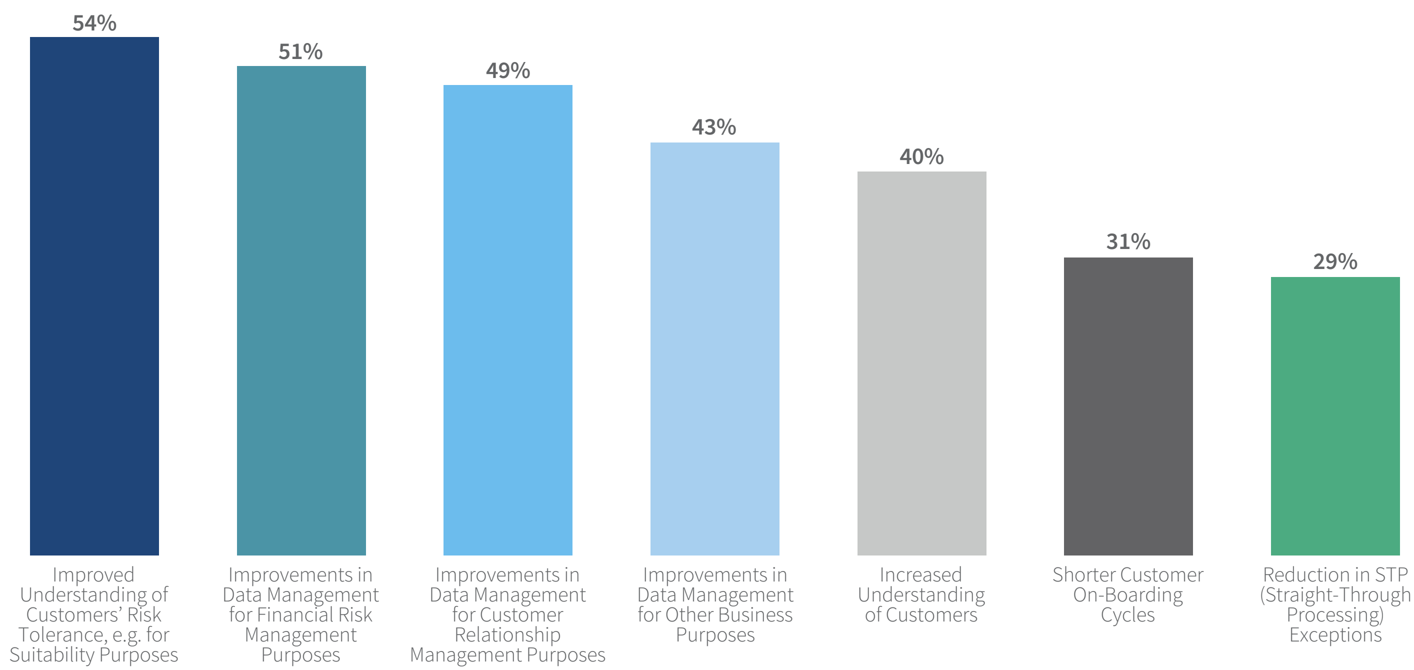
Though they can be challenging, financial crime compliance activities provide various benefits to Indian financial institutions, allowing for more effective risk management and management of customer relationships.

Knowing more about customers not only supports risk assessment, but also ways in which customer relationships and business opportunities can be managed.

KEY FINDING 04
Financial Crime Compliance Processes Provide Benefit to the Wider Organisation

Though financial crime compliance activities have been particularly challenging this year, financial institutions recognise the benefits of having improved data for risk management/customer relations/other purposes and an increased understanding of their customers.

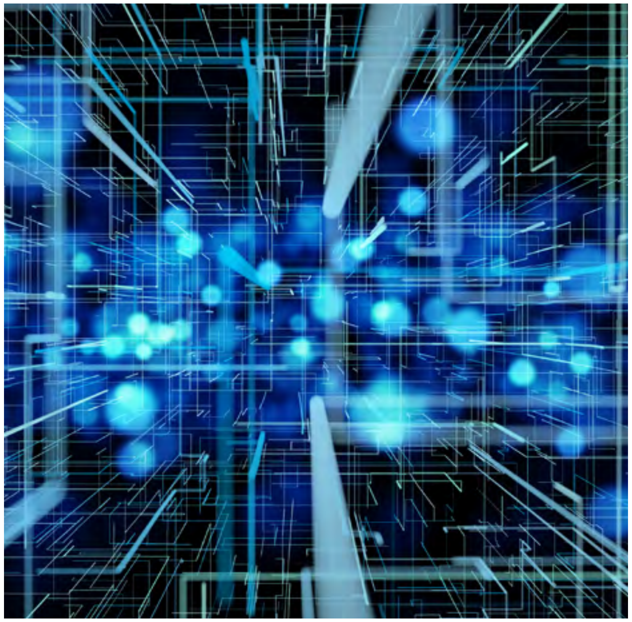
Benefits from Financial Crime Compliance
(% Ranked Among Top 3)



Q26: Which of the following do you see as benefits to the business brought by financial crime compliance?

KEY FINDING 05

Financial institutions that have invested in technology solutions, to support financial crime compliance efforts, have experienced less severe impacts to cost and compliance operations.



- Annual average compliance spend is less among those allocating more spend to technology.
- Greater efficiencies are realised among those allocating more spend to technology.
- Fewer pandemic-related challenges are cited among those allocating more spend to technology.

LexisNexis® RISK SOLUTIONS

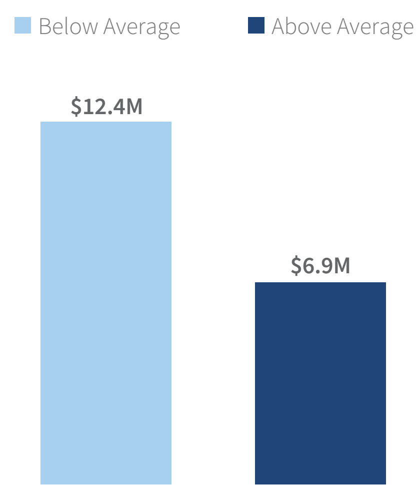
KEY FINDING 05
Compliance Technology Reduces Costs and Challenges

Indian financial institutions that allocate a larger share of their financial crime compliance costs to technology experience less severe impacts to cost and compliance operations.

Also, fewer of these firms experienced negative impacts from COVID-19 on their compliance operations; established use of technology helped them be more prepared. The average distribution of annual compliance operations costs for technology is roughly 40%. Findings show that firms allocating above average spend have realised the following:

A lower cost of compliance

Average Annual Compliance Costs
(2020 Costs in Millions)



Annual Compliance Spend on Technology

Fewer negative impacts from compliance requirements overall and during COVID-19

Annual Compliance Spend on Technology

% Indicating the Following as Compliance Challenges Overall	Below average	Above average
Sanctions Screening	51%	37%

% Indicating Significantly Negative Impact from COVID-19	Below average	Above average
Efficient resolutions of alerts	78%	57%

% Ranking the Following as a Top Challenge Based on COVID-19	Below average	Above average
Efficient resolutions of alerts	46%	29%
Longer time to complete due diligence	55%	39%
Delayed on-boarding of new accounts	47%	30%
Reduced controls and compliance monitoring capabilities	51%	20%

LexisNexis® RISK SOLUTIONS

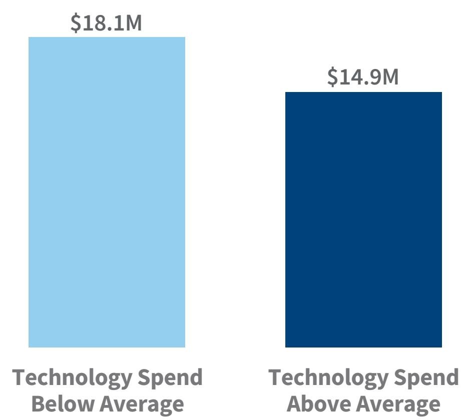
KEY FINDING 05
Compliance Technology Reduces Costs and Challenges

Indian financial institutions that allocate a larger share of their financial crime compliance costs to technology also have lower cost per compliance professional compared firms that allocate more of their costs to labour.

Below is an illustration based on mid/large financial firms in India.

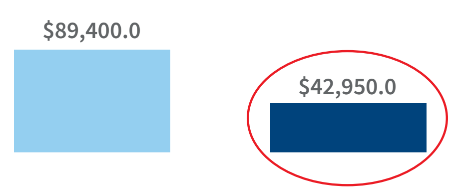
Average of AML Compliance Spend:

Mid/Large Financial Institutions
(Annual Cost USD in Millions)



	Technology Spend Below Average	Technology Spend Above Average
% Costs for Labor	64%	45%
Average Cost of Labor	$11.8M	$6.7M
Average # Compliance Staff	132	156

Average Cost of Compliance per FTE
(Annual Cost USD in Thousands)



IMPLICATIONS

1 India financial institutions need to be extremely prepared for increased risks of financial crime for the foreseeable future.

- It is unclear what the landscape will look like over the next 1 - 2 years as shaped by the COVID-19 pandemic.
- Financial institutions could be faced with greater spikes in financial crime for at least for the foreseeable future – particularly as digital/cryptocurrency transactions provide criminal opportunities.

2 Skilled compliance professionals will continue to be in demand, as financial crime grows in complexity. But, financial firms should consider fast-forwarding efforts towards compliance technology to counter challenges and costs to compliance operations.

- Financial firms which have invested in compliance solutions will be more prepared to deal with the new normal and any further sudden changes. As the cost of doing business rises in this COVID-19 environment, the *added* cost of compliance may become a negative tipping point; there comes a point of diminishing returns with more labour resources added.

3 A multi-layered solution approach to due diligence and financial crime risk assessment is essential to financial institutions.

- As financial crime complexity grows in the digital age, while regulations require more due diligence on beneficial ownership and risk assessment, in-house compliance solutions may be challenged to keep pace.
- There are unique risks that emerge from individuals, transactions, and contact channels. It is Important to assess both the individual and the business, with a particular need for real-time behavioral data/analytics in this digital age.

4 In addition to technology, it is essential to have robust and accurate data. Without the support of expanded sources, bad data can lead to bad decisions. Good data can lead to lower risks with benefits to the wider organisation.

- Having accurate data and highly capable solutions generates a degree of utility for not just compliance, but other functional areas as well. This includes business development and marketing; knowing more about customers can help inform the right products and services to position with customers.

LexisNexis® RISK SOLUTIONS

WE CAN HELP.

Description	Firco Insight®	Firco Filter	Firco Compliance Link	Firco Online Compliance	Firco Global Watchlist	Firco Trade Compliance	Firco Continuity
Accounts Screening Validate customer databases against sanction lists, Politically Exposed Persons (PEPs), Reputationally Exposed Persons (REPs) and other watchlists to determine potential risk.	✔	✔	✔	✔	✔		✔
Trade Screening Deliver speed and precision to trade finance screening and automate customers screening, dual-use goods, locations, and transportation vessels against sanctions, politically exposed persons (PEPs) and other lists.			✔		✔	✔	
Payment Screening Provide accurate Know Your Customer (KYC) intelligence to reduce compliance burden		✔	✔		✔		✔

Click here to read case studies on how our Financial Crime Screening products have helped organizations achieve operational efficiency and effective compliance risk mitigation.

Firco Insight
- Feature-rich customer and third-party screening and alert management platform.
- Combine high-performance processing with advanced filtering using proprietary risk scoring.

Firco Filter
- Unique filtering technology provides world-class screening in highly configurable solutions.
- Can be finely tuned to fit specific operational requirements and limit false alerts.

Firco Compliance Link
- Automate the assessment of sanctions and money laundering risk
- Screen customers, vendors, third-party relationships, financial transactions and trade activity against financial crime data.

Firco Online Compliance
- Fast and robust online lookup tool ideally suited to organizations with low volume but high-value accounts.
- Enables search on individuals against sanctions and politically exposed person (PEP) lists, and manually review information against a range of data points

Firco Global Watchlist
- Proprietary compilation of multiple regulatory and enhanced due diligence lists including sanctions watchlists, law enforcement agencies, Politically Exposed Persons (PEP) data, and adverse media from around the world

Firco Trade Compliance
- Robust trade compliance screening solution that automate customers, dual-use goods, locations and transportation vessels screening against sanctions, politically exposed persons (PEPs) and other lists

Firco Continuity
- Seamlessly screen large volumes of transactions against a wide range of sanctions lists in real time.

Accuity and LexisNexis Risk Solutions have merged operations. Both businesses are RELX companies and leaders in their respective focus areas in the global financial crime compliance sector with complementary solutions. Learn more about the Firco suite of account, trade and payment screening solutions at https://accuity.com

LexisNexis® RISK SOLUTIONS