Study reveals annual cost of financial crime compliance totals $85bn in EMEA

LexisNexis Risk Solutions released the findings of its latest *True Cost of Financial Crime Compliance Study – Europe, The Middle East and Africa.*

Source: Pexels

The commissioned study, conducted by Forrester Consulting, reveals that financial crime compliance costs increased for 98% of financial institutions in 2023. The total cost of financial crime compliance in EMEA has reached $85bn.

Financial institutions (FIs) are seeking ways to reduce costs while complying with regulations, with 35% identifying the escalation of financial crime regulations and regulatory expectations as the primary factor driving increases in compliance costs. Eighty-one percent (81%) are prioritising compliance programme cost cutting in the next 12 months.

Financial institutions are confronting a growing screening workload as the challenge of keeping up with the complex sanctions environment intensifies, with the number of screening alerts increasing with payment volumes at 78% of organisations in EMEA.

Key findings from the study:

- Labour costs are driving increases in expenses for financial institutions, emphasising the substantial investment

required in highly qualified resources to meet stringent compliance requirements.

Specifically, 72% of organisations noticed rises in labour costs related to full-time employees and part-time salaries in the past 12 months, while labour costs associated with training have increased at 70% of FIs.

- Financial institutions experienced significant increases in compliance costs related to technology. Specifically, technology costs associated with networks, systems, and remote work have risen at 70% of organidations in the region, particularly at 74% of firms in the Middle East, 72% in Africa and 67% in Europe.

  Similarly, 70% of financial institutions have experienced cost escalations for technology related to compliance and know-your-customer (KYC) software.

- Cryptocurrencies, digital payments and AI technologies are emerging as tools for illicit activities. Financial institutions are grappling with the impact of these sophisticated criminal methodologies within an already complex regulatory background.

  When asked about the types of financial crime FIs had observed significant increases of more than 20% in the past 12 months, 25% of companies identified financial crime involving digital payments, while 23% reported heightened use of both cryptocurrencies and AI.

- Trade-based money-laundering and financial crime threats in the supply chain are increasingly concerning. Fifty-eight percent (58%) of FIs noticed an increase in trade-based money-laundering, while 59% of respondents recognised a higher prevalence of corruption and bribery within the supply chain.

  “The cost of financial crime compliance is clearly rising for financial institutions across EMEA which is being felt by teams across the entire compliance workflow,” said Matt Michaud, global head of financial crime compliance at LexisNexis Risk Solutions.

SA's cybercrime hotspot status intensifies need for cybersecurity in logistics

27 Feb 2024

“Skilled in-house compliance teams are essential, but businesses should be actively seeking ways to reduce labour costs while improving compliance efficiency. Criminals adapt quickly and FIs require a partner with advanced tools, data and analytics to not only keep pace but to stay ahead."

The True Cost of Financial Crime Compliance Study – Europe, The Middle East and Africa compiles responses from 482 senior decision-makers responsible for financial crime compliance at financial institutions in the EMEA region including the Baltic States, France, Germany, Kenya, Poland, Saudi Arabia, South Africa, the Netherlands, and the UAE.

It highlights key pain points related to the cost, current state and challenges presented by financial crime compliance operations.

Recommendations for combating financial crime:

- **Balance compliance effectiveness with customer experience.** Financial institutions are grappling to acquire and retain customers in the digital era.

  The winners will be those that can deliver seamless customer onboarding and transaction experiences. Striking

the right balance between customer experience and financial crime compliance efficiency involves streamlining KYC and onboarding processes, reducing false positives and allowing legitimate transactions to proceed without inconveniencing the customer.

- **Embrace new technologies to counter emerging financial crimes.** Criminals are increasingly using new technologies for their activities. In addition to deploying advanced AI- and ML-based compliance models, financial institutions should leverage privacy-preserving technologies and advanced analytics to swiftly identify new crime patterns to outpace cybercriminals and counter sophisticated financial crime.

- **Leverage compliance technology and analytics to manage costs and enhance efficiency.** Labour costs rank highest in financial crime compliance spending.

  While in-house compliance teams with expertise are crucial, partnering with an experienced and proven technology provider will alleviate some labour costs and enhance compliance efficiency.

  To identify the right partner, organisations should focus on their future-fit capabilities, including proven expertise in digital financial services, ease of integration, robust data management, advanced analytics, lightweight software-as-a-service deployment and the ability to balance effectiveness with customer experience.