COVID-19
Financial Crime & AML

Disclaimer

- The information provided does not, and is not intended to, constitute advice; instead, all information, content, and materials are for general informational purposes only.

- No person should act on the basis of information set out herein, without first seeking appropriate advice in the relevant jurisdiction.

- The views or opinions expressed herein are those of the individual author, writing in their individual capacity only, and are not those of Atrato. All liability with respect to actions taken or not taken based on the contents are hereby expressly disclaimed.

- The content is provided "as is;" no representations are made that the content is error-free.

THE COST OF COMPLIANCE IN A DIGITAL WORLD

THE COST OF NON COMPLIANCE

- Compliance Week highlighted violations increased by 141% between 2019 and 2020 with a total price tag of $10.4 billion in 2020, with the UK making up $199 million of that.[1]
- There were $46.4 billion for breaches relating to anti-money laundering (AML), know your customer (KYC), data privacy, and MiFID (Markets in Financial Instruments Directive) since 2008. [1]
- Each service provided needs to be weighed against the costs associated with any relationship.
- Clients and transactions carry with them an element of “regulatory risk” (a fine at some future date)
- Firms fined for financial misconduct tend to perform worse compared to those not under litigation.[2]

1. Fines against financial institutions hit $10.4B in 2020 Available at: https://www.complianceweek.com/surveys-and-benchmarking/report-fines-against-financial-institutions-hit-104b-in-2020/29869.article
2. ESRB (2015). Report on misconduct risk in the banking sector. Technical report, European Systemic Risk Board.

THE COST OF COMPLIANCE

- The “RegTech” market was estimated at $5.3 Billion in 2019 and is expected to reach $33.1 Billion by 2026.[1]
- AML compliance activities such as know your customer (KYC) are being outsourced, something that has not gone unnoticed by competent authorities.
- Paradoxically, the ever increasing costs of compliance to mitigate financial crime may be impacting smaller, underserved customers where compliance costs have rendered the business relationships commercially unattractive.
- Carrying out customer due diligence (CDD) on smaller clients often has additional costs and perceived risks (in many cases, there is insufficient documentation or data to assess their crime risk).
- While a “RegTech” solution may reduce administrative burdens, the risks to a firm remain, and the true cost of compliance may much higher.

1. “RegTech Market By Application (Compliance Management, Regulatory Intelligence, Risk Management, Identity Management, Fraud Management, and Regulatory Reporting), By Organization Size (Large enterprise and SME’s),- Global Industry Perspective, Comprehensive Analysis, and Forecast, 2020-2026”

COMPETENT AUTHORITY CONSENSUS

Atrato

- Concerns about FinTech firms' lack of understanding of their AML obligations.[1]
- Overreliance on outsourcing to RegTech solutions, including remote onboarding "may often cause challenges with the identification and verification of customers".[1]
- Digital Operational Resilience Act ("DORA") is intended to harmonise the EU's currently fragmented regulatory landscape regarding digital operational resilience testing and the oversight of critical third-party service providers.[2]
- National lockdowns and social distancing measures have forced the use of online tools and other alternative measures in order to meet AML obligations.
- COVID-19 has accelerated discussions around the use of "Digital Identities".

1. Opinion of the European Banking Authority on the risks of money laundering and terrorist financing affecting the European Union's financial sector." Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf
2. See: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Financial-services-improving-resilience-against-cyberattacks-new-rules-

DIGITAL IDENTITY

- Covid-19 has shown that the ability to prove identity digitally has become more urgent and more valuable.
- The Financial Action Task Force (FATF) has stated it "strongly supports the use of new technologies…"[1]
- Compared to digital identification for individuals, digital identification for corporates is in its infancy.
- The goal for the financial sector as it seeks to enable its clients to operate in an increasingly digitised world, should be to find a straightforward way to prove identity and make that verification clear to others.
- Like any IT system, digital ID systems are not immune to cyber attacks and the stakes are high, building robust systems and controls to prevent the risk of data breach.

1. FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

PROCESS AND TECHNOLOGY

- Reliable and secure RegTech solutions and digital ID systems are stepping stones to combating financial crime and should be used in conjunction with a firms internal controls with its risk based approach, informing the process.
- There is no one size fits all approach to mitigating the risk of financial crime within an organisation.
- Final liability for CDD will always lie with the firm itself, rather than any third party provider. A clear understanding of the underlying data source is required.
- The US National Institute of Standards and Technology, described two basic components of a digital ID process:
  - **"Who are you?"** (essential) – This involves collecting, validating and verifying identity evidence and information about a person; and
  - **"You are you"** (essential) – It establishes, that the person is indeed who he or she claims to be.[1]

1. FATF (2020), Guidance on Digital Identity, FATF, Paris, www.fatf-gafi.org/publications/documents/digital-identity-guidance.html

THE COVID-19 PARADIGM

ORGANISED CRIME AND COVID-19

- Measures to contain COVID-19 are impacting on the criminal economy and changing criminal behaviour.[1]
- "Never let a good crisis go to waste" – criminal behaviour, creates vulnerabilities but may present the opportunity build resilience against threats.
- The most notable immediate impact has been in the areas of cybercrime, the trade in counterfeit and substandard goods as well as different types of frauds and schemes linked to organised property crime.[2]
- Other emerging risks resulting from COVID-19 are:
  - Cybercrime
  - Counterfeit and substandard goods
  - Philanthropic fraud
  - Economic

1. EUROPOL, "Pandemic Profiteering. How Criminals Exploit the COVID-19 Crisis." Available at https://www.europol.europa.eu/publications-documents/pandemicprofiteering-how-criminals-exploit-COVID-19-crisis
2. . EUROPOL, "Beyond the pandemic how COVID-19 will shape the serious and organised crime landscape in the EU." Available at https://www.europol.europa.eu/publications-documents/beyond-pandemic-how-covid-19-will-shape-serious-and-organised-crime-landscape-in-eu