# Why are regulated institutions still not getting their Fraud and AML (FRAML) due diligence right?

*By MoData 22/12/2021*
*Clive Gungudoo, Director Financial Crime and Risk Management*

Managing financial crime risk continues to remain a major priority for regulated institutions, with millions of dollars being invested every year into upgrading systems and processes around prevention, detection, investigation and reporting of such crimes.

Despite these massive investments and strategy refreshes, financial Institutions, and now real estate companies, law firms, the gaming industry and casinos are still not winning the face off with criminals to outsmart each other, and fraud, cybercrimes and fines for AML breaches are increasing year on year over recent decades.

There has been a call to action from regulators;

- According to the United Nations Office on Drugs and Crime (UNODC), the estimated value of money laundered globally is 2 - 5% of global GDP per annum, $2 trillion in current US dollars. As a result of covid and the related acceleration of digital adoption by most businesses this has probably been long surpassed,
- Regulators are announcing plans to strengthen the know your customer (KYC) and anti-money laundering (AML) checks required for remote customer onboarding.
- The Financial Crimes Enforcement Network (FinCEN) has issued a new notice that aims to increase ownership transparency and target the use of shell companies that are used to hide the proceeds of crime.
- The Financial Action Task Force (FATF) has called for a global move against illicit profits generated from environmental crimes.
- The European Banking Authority (EBA) has issued guidelines on AML/CFT cooperation and information exchange between prudential supervisors, AML/CFT supervisors and financial intelligence units under Directive 2013/36/EU.

Whilst some inroads have been made in certain regions in public-private partnership models to fighting financial crime, banks and other regulated organisations are still managing financial crime in silos within the same organisation and across the industry without hardly any real collaboration, conversely fraudsters and money launderers continue to collaborate in this face off. According to the Association of Certified Fraud Examiners (ACFE), only 29% of organisations currently contribute to a data-sharing consortium to help prevent and detect financial crimes with another 21% willing to contribute to one in the future.

The global pandemic has permanently shifted the way business is conducted but is also providing criminals with new ways to increase the complexity and sophistication of FRAML.

Fraud and Money Laundering in the e-commerce space alone is set to grow in excess of $200 billion by 2025. Apart from fake e-commerce merchants with store fronts to launder money, the introduction of Buy Now Pay Later (BNPL) and Gift Cards is popular amongst the Gen Z but equally compelling for criminals. With instant loan disbursements, we're seeing an increased risk in double stacking – taking out multiple loans fraudulently before its reported to the credit bureaus

Let's take a brief look at the challenges from a FRAML due diligence perspective.

Firstly, there is no convergence of offline and online identity and authentication from a device intelligence and behavioural biometrics perspective. Similarly, no convergence in KYC, document forgery detection, AML screening and FRAML transaction monitoring, enterprise or industry wide. Organisations are unable to follow the flow of funds across the complete transaction journey, especially between fiat and cryptocurrencies and other digital assets. They simply can't run multi-chain virtual asset service provider (VASP) screening, wallet screening, transaction monitoring and forensics in real time. This means more placement, integration, layering of illicit funds into the global financial system.

Secondly, the data sources used for customer onboarding and ongoing due diligence are limited, not updated in near real time and don't link people, organisations and other related parties connected to financial crimes in an intelligent manner. This results in latency risk of manual updates to watchlists but also limited open source and social media data sources which are becoming the new social network for rich customer activity data. Effectively, not getting a total risk profile of the client and business means onboarding and sheltering criminals to hide the proceeds of crime and the price to pay is hefty regulatory fines for these critical capability gaps.

Thirdly, there is no real time industry data-sharing in a trusted model across the customer lifecycle.

Combine these challenges and the result across customer journeys is low FRAML detection rate, high false positives, more customer friction, revenue leakage and the deployment of large operational teams to manage the workload and late or non-reporting of suspicious activity and transactions to the regulators. Both the Capex and Opex investment is still negated in the end. Banks employ anywhere between 70 to 600 staff, based on size of the organisation, to investigate fraud and AML alerts at an average investigation cost of $24 per alert. Where 80 to 90% of these alerts are false positives, the headcount cost amounts to $1m - $20m per annum as result of ineffective monitoring. The investment in antiquated technology on top of that can amount anywhere between $2m-$5m per annum. Yet fraud and money laundering continue to escalate and even more so in the digital space.

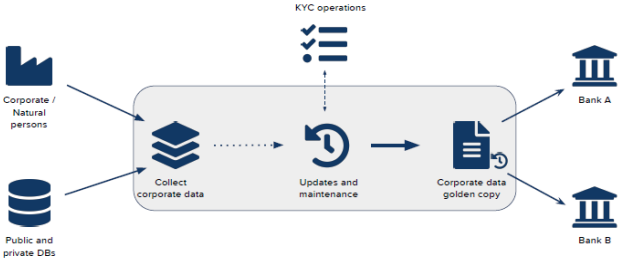
Onboarding trustworthy customers during the account opening process is the first critical step in effective FRAML compliance programs. Thereon, effective ongoing monitoring becomes extremely important to dynamically risk rate customers and business lines within the organisation and across the regulated industry sectors.

MoData is leading the industry collaboration in the fight against financial crimes with the first to market distributed ledger (DLT) technology and confidential computing to enable game changing results in FRAML compliance programs.

1. **Decentralised KYC**

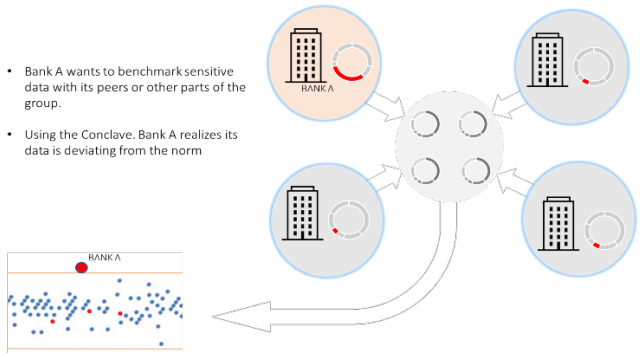
   Based on our experience, FI's save between 45% and 55% of their costs and create a far better end user experience;

   - Eliminate duplicate KYC verification work by having an up-to-date, golden copy of client data
   - Reduce Capex and Opex
   - Shared KYC utility that respects business privacy
   - Tamper-proof utility
   - Data monetization & new revenue streams

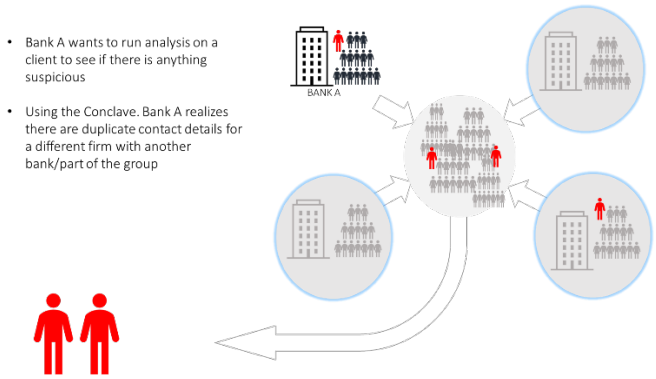


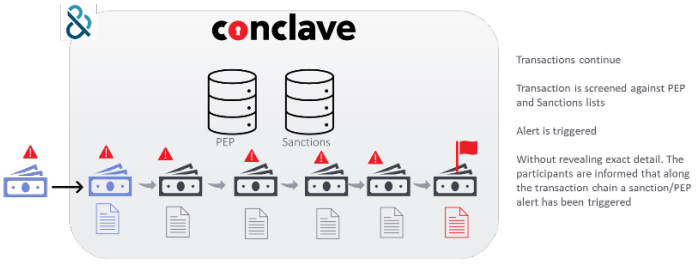
2. **Multi Party Collaboration using secure data processing within a DLT and confidential computing Conclave**

   - Behaviour (improve cross industry FRAML detection rates and stop fraud and money laundering in real time)

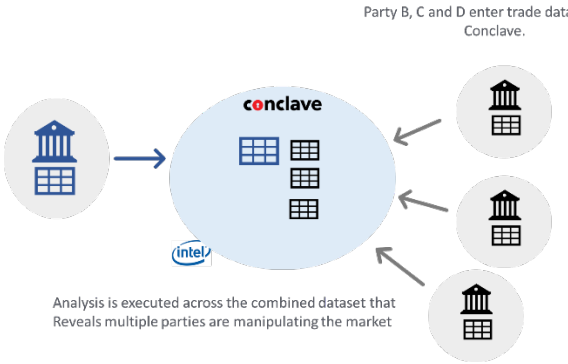



   - KYC and AML (detect cross industry client risks and unify the client onboarding and ongoing monitoring due diligence in real time)



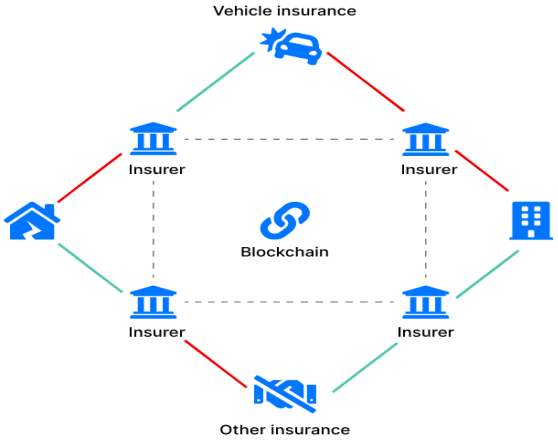




   - Collusion (real time detection of syndicated Fraud and Corruption)




   - ClaimShare (real time detection and prevention of double dipping fraud in the short-term insurance space)

     Insurers are investing heavily in fraud prevention mechanisms, leveraging the newest technologies to perform deep analysis and to identify patterns of fraudulent behaviour. Unfortunately, they are limited to their internal data for these purposes. There is no industry standard for data sharing and there is no production-grade technology to facilitate industry-wide data sharing given the regulatory constraints of sharing sensitive, personal information.




Our solution provides a consortium of insurance companies a quick and automatic way to identify and eliminate the duplication of claims for the same loss event, while also complying with all regulations. Customers' privacy is respected, and no sensitive information is revealed to any competitors. To do so, the content of a claim is divided into public and private data. The 'Public' part of the verified claims is shared with all insurers in the network on a distributed ledger. The 'Private' part of claims is not shared but is used to confirm fraudulent duplicate claims.

**Conclusion**

Real time data sharing through a trust model is absolutely key to the success of industry collaboration in the fight against financial crime and aiding regulators to improve the risk posture and safety in the global financial ecosystem. MoData is first to market this DLT and confidential computing capability to enable such a trust model without compromising customer or business privacy. MoData is also first to market the only affordable, real-time software-as-a-service (SaaS) marketplace, MoData Digital Services (MDS), for all financial crime and risk management operations. This customer value proposition removes the upfront investment barriers and where organisations can select bespoke FRAML services they need to stitch into their customer journeys while availing a monthly pay-as-you use license and support model. MoData brings a collective 86 years of financial crime and risk management experience as passionate financial crime fighters, thought leaders with subject matter expertise and industry collaborators during this tenure.

For more information, contact us on:
Info@modata.com
www.modata.com