

Potential Solutions:

Examples provided from a TechSprint on Financial Crime and AML

1. How could the detection and reporting of suspicious activity within the capital market be improved?
2. How can technology aid in looking at transaction flows across jurisdictions when a centralized way of data sharing is not possible?
3. How can the quality of feedback provided to firms from SARs be improved without breaching data privacy and AML tipping-off restrictions?
4. How can financial crime patterns be efficiently and effectively identified and codified in such a form that the algorithms can be shared across borders and between institutions?
5. How can robotic process automations be applied to improve the efficiency and/or effectiveness of regulated institutions financial crime and money laundering detection and prevention activities?
6. How can natural language processing aid in the investigation, automation, and production of analysis from suspicious activity reports?
7. How can one institution's suspicions of fraud be recorded in such a way as to reduce the risk of laundering those financial gains at another institution while managing the risk of tipping off and protecting personal data?
8. How can appropriate sanctions, money laundering and fraud assessment and interventions be implemented in distributed ledger payment systems?

9. How might cryptographic tokenization be used to aid identification and tracing of units of value through the international financial system?
10. How new technologies, big data can be leveraged to measure the incidence of financial crime, money laundering, terrorist financing aid firms and regulators/agencies in understanding the effectiveness and impact of compliance, prevention, and prosecution activities?
11. How can network analytics be used to analyze trends and patterns across the network to give a meaningful network risk score?
12. How can machine learning and behavioral science be used to facilitate decision making and operational support systems?
13. How might technology/machine learning and AI assist in the more effective identification of authorized payment fraud eg. where consumer are tricked into sending money to a fraudster
14. How meta-data around transactions such as IP address, card authorizations, addresses and unique identification details of mobile phone and laptop computers, browsing data that can be incorporated in the analytical process
15. How can technology be used to facilitate efficient onboarding of a new customer while at the same time ensuring a robust KYC process and giving the customer the ability to protect their own data?