

# Balancing Innovation and Financial Crime Risk in Saudi Arabia's Digital Economy

**Ahmed Amonette** - Senior Associate - Litigation

a.amonette@tamimi.com - Riyadh



Saudi Arabia has set its sights on becoming a leader in the digital economy, and to achieve that goal, authorities in the Kingdom have been working to provide an environment where investors, entrepreneurs, start-ups and innovators can flourish. One key aspect of these efforts has been the legal reforms that are being implemented at a rapid pace. This article seeks to offer current or potential investors or entrepreneurs in the Saudi digital economy with an update on the recent regulatory developments in the area of anti-financial crime.

One of the Saudi government's targets under Vision 2030 is to move its economy away from cash and increasing the use of cashless payments to 70%. While this is indeed an ambitious goal, it is one that Saudi Arabia is well positioned to achieve given that a majority of its population is under the age of 30 and are highly digital literate and quick to adapt to new technologies. This ambitious plan, coupled with the need for online-based solutions arising out of necessity due to COVID-19 pandemic, has already led to a financial technology ("FinTech") boom in the Kingdom, best exemplified by the first billion-dollar valuation of a FinTech unicorn in the Middle East, STC pay, towards the end of 2020.

More recently, to demonstrate the digital boom in the Kingdom, in June this year Saudi Arabia's Cabinet approved the licensing of two digital banks in the Kingdom. The first license provides approval for STC Pay to become a local digital bank ("STC Bank"), with a capital of SAR 2.5 billion. While the second license was awarded to a number of companies and investors, led by Abdul Rahman Bin Saad Al-Rashed & Sons Company, which will establish a local digital bank ("Saudi Digital Bank") to conduct banking business in the Kingdom, with capital of SAR 1.5 billion.

# Financial Crime in the Digital Economy

The digital transformation that is taking place in Saudi Arabia has inevitably led to new risks and challenges, due to the increased possibilities of regulatory gaps and loopholes brought on by innovations in FinTech, which may also lead to new potentials for financial-crime activities. The sheer diversity of actors involved in the digital economy, including e-commerce merchants and the financial institutions that process payments, as well as the anonymous nature of cross-border transactions, all serve to intensify the challenges of financial crime prevention, and jurisdictions everywhere have been faced with the challenge of keeping pace with technological developments.

With that said, it seems that Saudi Arabia is uniquely positioned to potentially become not only a global leader in FinTech, but also in related anti-financial crime regulation. This is in light of recent and planned regulatory changes that are in line with the Kingdom's broader regulatory reform plans under Vision 2030.

## SAMA's Regulatory Approach

This optimistic outlook is supported by the proactive approach taken by the Saudi Central Bank, previously known as the Saudi Arabian Monetary Authority ("SAMA"), in its most recent regulations and guidelines. As an example, SAMA's Payment Services Provider Regulations, issued in January 2020, provide that *"Payment Service Providers are required to comply with the AML Law and the applicable rules and regulations on anti-money laundering and counter-terrorism financing issued by SAMA."* Additionally, the Licensing Guidelines and Criteria for Digital-Only Banks issued by SAMA in February 2020 seem to open up the door for the use of new regulatory technology ("RegTech") for processes like e-KYC, by providing that applicants *"demonstrate the compliance of the AML/CTF regulations in the fully digitalized environment."*

This means that FinTech companies operating in the Saudi market will need to ensure that their internal policies and procedures are in conformity with the Saudi AML law as well as SAMA's regulations on anti-money laundering and counter-terrorism financing. RegTech providers on the other hand, will also need to stay up to date on the ever-changing regulatory landscape in the Kingdom, as they work to provide their clients with processes like e-KYC.

## Looking ahead to Open Banking

Open banking refers to a banking practice that provides third-party financial service providers with open access to consumer banking, transaction, and other financial data from banks and non-bank financial institutions.

Earlier this year SAMA announced that it plans to issue a framework for open banking in the Kingdom, most likely in early 2022. This decision presents significant opportunities for FinTech companies in Saudi Arabia as it will allow third-party developers to access customer data (with their permission) from their banks and act as a bridge to financial technology platforms like accounting and personal finance apps. This will likely enable customers and businesses to have greater control over their finances and access bespoke financial services, which in turn will open up the Saudi market to a broader range of FinTech services and greater innovation.

However, it remains to be seen as to how SAMA will balance the competing interests between enabling

innovation while also managing financial crime risks, as open banking will inevitably create new fraud risks for Saudi banks by opening up their systems to third parties. However, open banking also has the potential to improve the abilities of Saudi banks to conduct anti-money laundering and KYC, since data can be across multiple providers, enabling institutions to form a more complete picture of customers and their transactions.

## **KSA's New Financial Fraud Law**

Earlier this year, Saudi Arabia issued a new Law for Combating Financial Fraud and Breach of Trust, issued by Royal Decree No. (M/79) of 1442 H (2021G) (the "Financial Fraud Law"). This is particularly relevant in the context of the developments taking place in the Kingdom's digital economy and the related increase in financial crime risk, as typically, fraud can be considered a gateway to money laundering, as proceeds generated illegally will typically require that they be cleaned up through the financial markets and banking system.

SAMA defines fraud in its guidelines as *"any act involving deceit to obtain a direct or indirect financial benefit by the perpetrator or by others with his help, causing a loss to the deceived party."* This definition encompasses not only financial gain, but other benefits as well, such as gaining access to or obtaining information by means of deceit or other dishonest conduct.

The Financial Fraud Law provides for punishment of up to seven years in prison and maximum fines of SAR 5 million for those who appropriate funds by engaging in fraud and imposes punishment of up to seven years and fines of up to SAR million on those who unlawfully appropriate funds entrusted to them. Furthermore, the law criminalizes the attempt of these criminal acts, as well as the acts of incitement, agreement or collusion to carry out such acts.

This new law, along with the recent regulations issued by SAMA, demonstrate that the Kingdom is fully aware of the importance of providing an effective anti-financial crime regulatory environment and we can expect that Saudi authorities will continue to revise and issue new laws and regulations governing the digital economy, particularly when it comes to anti-financial crime. With that in mind, FinTech companies that are keen on entering the Saudi market or that are already operating in the Kingdom would be wise to seek expert legal advice when it comes to their financial crime compliance measures.