



Financial Crime and Fraud

March 2021






Contents



The UK	3
The FCA	3
The SFO	3
Fraud and cyber-crime	4
Key Contacts	5
Germany	6
Updates	6
Key Contacts	6
Poland	7
The PFSA	7
AML Legislation	7
Key Contacts	8
UAE	9
Key Contacts	10
Saudi Arabia	11
Key Contacts	11



Find out more about DWF

-  dwfgroup.com
-  enquiries@dwf.law
-  [linkedin.com/company/dwf](https://www.linkedin.com/company/dwf)

In the three months since our last update, the FCA's actions have demonstrated the words that preceded them; "there is no amnesty for firms that tackle financial crime poorly"¹.

The FCA

There has been a noticeable uptick in public outcomes relating to financial crime; only last week the FCA announced its first criminal prosecution of a bank under the Money Laundering Regulations 2007 ("**MLRs**"). The FCA has been trying to secure a criminal prosecution under the MLRs for some years and has opened several enforcement investigations into financial institutions for failures under the legislation. However, this is the first criminal prosecution of a bank under the MLRs by the FCA and provides further evidence of the FCA's resolve to act when it perceives failures to comply with obligations to combat financial crime. The alleged failures relate to determining, conducting and demonstrating risk sensitive due diligence and on-going monitoring of customer relationships to prevent money laundering. The FCA has confirmed that no individuals have been charged and the bank is due to appear in court in April.

The prosecution follows two final notices against banks last year for failures relating to anti-financial crime systems and controls (reported in our last newsletter). It is also noteworthy that those two fines (GBP 37.8 million and GBP 48.3 million) represent two of the three highest imposed over the course of the financial year to date. The FCA's announcement of its first prosecution under the MLRs serves as a timely reminder to all regulated firms to ensure their anti-financial crime systems and controls are regularly tested and enhanced when necessary, especially in light of public outcomes against other institutions. This is particularly the case in the wake of the pandemic when the FCA has expressed concerns on multiple occasions throughout the last year that the pandemic has afforded criminals new opportunities to commit economic crimes.

In early March the FCA imposed a fine and prohibition order on a trader for market abuse and in February, the FCA announced that it had commenced criminal proceedings against four individuals for insider dealing, two of the four being simultaneously prosecuted for fraud by false representation. Further, in January an individual convicted of insider dealing in 2019 was ordered to pay in excess of GBP 3.8 million perceived to be the proceeds of crimes he committed. The FCA's message is clear; financial crime

remains a top priority and the regulator will not hesitate to take action, imposing significant fines as a deterrent.

The SFO

Is the SFO clearing its decks and preparing for post-pandemic activity?

The SFO saw an influx of large cases in the wake of the financial crisis in 2008 relating to both the LIBOR and foreign exchange scandals, for example. Given the recent activity summarised below, it appears that the SFO may well be 'clearing the decks' in preparation for another similar increase in cases arising out of the pandemic.

In January this year, the SFO announced that it was closing its investigation into an international tobacco company following an investigation that had lasted over three years. The SFO noted that "*following extensive investigation and a comprehensive review of the available evidence*", the evidential test for prosecution was not met.

This outcome follows shortly after similar decisions in May and June last year to close investigations into two other global organisations. The SFO also agreed a number of Deferred Prosecution Agreements in 2020, including one agreed in July and another in October.

As a result, the SFO has concluded at least five of its large cases since May of last year. The Director, Lisa Osofsky, has been clear in stating that the SFO expects to commence pandemic related investigations. In a speech entitled "[Future Challenges in Economic Crime: A View from the SFO](#)" given by Osofsky in October 2020, she stated that the SFO expects to see an increase in reports relating to Investment Fraud being made as a result of the pandemic.

The SFO is also expecting an increase in the number of bribery cases caused by the pandemic during which businesses have been placed under extreme stress, thereby creating greater temptation to try and win contracts by "*any means necessary*"².

Osofsky has recently stated that two legislative developments in particular are at the top of her agenda:

¹ [Mark Steward, FCA Executive Director of Enforcement and Market Oversight in November 2020](#)

² Taken from the speech "[Future Challenges in Economic Crime: A View from the SFO](#)", given by Lisa Osofsky in October 2020

1. A failure to prevent economic crime offence; and
2. A "tipping off" offence in relation to notices issued under Section 2 of the Criminal Justice Act 1987 ("CJA").

Whilst an amendment to the Financial Services Bill that would have held those "authorised or registered by the Financial Conduct Authority" liable for fraud and money laundering offences (amongst others) committed by employees was discussed in Parliament in January, it was dismissed pending the current Law Commission review on corporate criminal liability. The SFO's Director is, therefore, likely to have to wait some time before there are any significant developments in relation to a new economic crime offence.

In relation to the suggested "tipping off" offence, the SFO's desire to limit any internal investigations conducted by recipients of Section 2 Notices so as to limit the risk of alerting those who may have been involved in the commission of a crime can significantly hinder any internal investigations and hamper the 'business as usual' operation of a corporate. The key to mitigating the effect of this is to maintain an open and co-operative dialogue with the SFO, informing them of any proposed actions, which may impact on the investigation and explaining the difficulties caused by any restrictions imposed on internal investigations.

Given the SFO's predictions and the FCA's rhetoric around financial crime and fraud over the past year, financial services firms would be well-advised to ensure that their systems and controls are being regularly re-assessed for new, and emerging, financial crime risks. Any such assessments should be well-documented, including the rationale for any decisions arising out of them. Firms should also ensure that their reporting obligations to financial crime agencies are well considered and understood, with legal advice being sought when necessary.

R (on the application of KBR, Inc) v Director of the Serious Fraud Office [2021] UKSC 2

Following a legal battle between KBR, Inc and the SFO over the past three years concerning the extent of the SFO's powers under section 2(3) of the Criminal Justice Act 1987 ("CJA") (a "Section 2 Notice") to compel a foreign company to produce documents it holds overseas, the Supreme Court finally determined the matter on the 5 February 2021.

The Supreme Court unanimously ruled that the SFO does not have the power under a Section 2 Notice to compel a foreign company with no registered office, fixed place of business or business activities in the UK to produce material to it. In reaching this conclusion, the Supreme Court considered that UK legislation is generally not intended to have extra-territorial effect; Parliament did not intend section 2(3) of the CJA to have extra-territorial application because there is no such express wording or clear indication within the Act that it ought to apply extra-territorially.

As such, KBR, Inc, a company incorporated in the USA (but with UK subsidiaries ("KBR UK"), with no fixed place of business in the UK and having never carried out business in the UK, fell outside the reach of the SFO's Section 2 powers.

What does this mean in practice?

It should be noted that a UK based company is still required to produce documents that it holds overseas in response to a Section 2 Notice. Further, a Section 2 Notice can still be legitimately served upon companies that have a registered office or fixed place of business in the UK, or companies that carry on business in the UK.

The SFO is also able to use other avenues to obtain material held by foreign companies, such as the use of Mutual Legal Assistance through its partner agencies abroad, albeit that this can be time consuming and cumbersome.

International companies currently under investigation and those who receive a Section 2 Notice should carefully consider whether the material they hold falls within the scope of a Section 2 Notice, following this judgment before responding to and producing documents to the SFO.

Following the Supreme Court ruling, the SFO has closed its investigation into KBR, Inc.'s UK subsidiaries citing that the evidence did not meet the evidential test required within the Code for Crown Prosecutors. This brings the SFO's four year bribery and corruption investigation into KBR UK to a close.

For further specialist advice on this topic, please contact [Imogen Makin](#) and [Kelly Wilson](#).

A more detailed consideration of this important judgment and its implications can be found [here](#).

Fraud and cyber-crime

Under-reporting of fraud and cyber-crime offences

Estimates compiled by the Office for National Statistics (ONS) suggest that only a fraction of fraud and cyber-crime offences are being reported to the authorities. Estimates put the volume of cyber-crime offenses at 1.7 million in the 12 months to September 2020 (similar to prior year figures), but police recorded offense data from the National Fraud Intelligence Bureau (NFIB) showed that only 29,094 offences were referred to the NFIB. That equates to just 1.7% of the estimated total volume of cyber-crimes perpetrated.

Some expert commentators have indicated that there is a general perception that there is limited action the public authorities can or will take to find and punish offenders. However, when considering the ability of the authorities to take action it must be noted that if they are not even being told about offences, they have little opportunity to attract the right level of funding, skills and other resources required to be effective in fighting cyber-crime. In turn

this creates an environment where criminals go unpunished, continue to perceive cyber-crime as high-reward low-risk endeavour, and the burden of tackling cyber-crime continues to be placed on individuals and organisations being targeted by criminals.

In the financial services sector, the statistics were more positive. UK Finance and Action Fraud data for the banking sector showed significant increases in offenses reported in the categories of; remote banking and card fraud, business email compromise, social media account compromise, and computer viruses and malware.

Looking ahead; possible NIS2 Directive

On 22 February, the European Parliamentary Research Service (EPRS) announced that the NIS2 Directive is under deliberation. This is intended to expand the Directive on Security Network and Information Systems, on which the UK Network and Information Systems (NIS) Regulations 2018 are based. In particular, the NIS2 Directive aims to create a high common level of cybersecurity across the EU Member States, respond to growing threats posed with digitalisation and the surge in cyber-attacks, strengthen the security requirements, introduce stricter supervisory and enforcement measures, as well as increase the scope of entities covered by the original NIS Directive.

While the Directive will not be binding on the UK, it is possible that the UK may update the NIS Regulations in line with it which will likely impact the Financial Services sector.

Payment Systems Regulator Consultation - Authorised Push Payment (APP) Fraud

APP fraud is where a fraudster tricks a customer into authorising the payment of money to them. The PSR is consulting on APP fraud given notified losses amounts to GBP 208 million in H1 2020. New measures might include:

1. requiring banks publish outcomes and statistics for APP fraud including reimbursement figures;
2. mandating bank data sharing to prevent scams in the first place; and
3. extending customer protections through changes to payment system rules.

The consultation closes 8.4.21. More information on this subject can be found [here](#).

Key Contacts

Financial Services



Martin Pugsley
Head of Financial Services Sector
M +44 7718 130 683
E Martin.Pugsley@dwf.law

Financial Services Regulatory Legal



Richard Burger
Partner
M +44 7545 100510
E Richard.Burger@dwf.law



Imogen Makin
Legal Director
M +44 7842 608 194
E Imogen.Makin@dwf.law



Kelly Wilson
Senior Associate
M +44 7708 487763
E Kelly.Wilson@dwf.law

Financial Services Litigation



Ben Johnson
Partner
M +44 7968 559 314
E Ben.Johnson@dwf.law



Mark Hendry
Director
M +44 7821 867712
E Mark.Hendry@dwf.law



Germany



Updates

The German Parliament is due to discuss the draft law on electronic securities, which if implemented in its current form, will waive the strict paper requirements for issuing bonds and interests in investment vehicles. Instead, a mere electronic entry in either a centralised register or a decentralised Blockchain register will be sufficient for issuing electronic securities. However, according to the proposed law, even Blockchain registers will require a licensed registrar in order to register electronic securities. This would create the potential for extensive liability for such registrars with the consequence that not many market players may dare to take up such role. Yet, from a legal perspective, the comprehensive good faith provisions surrounding entries on Blockchain registers are quite compelling; they include not only ownership but also transfer restrictions. According to the current draft, shares in funds may also be issued solely in electronic form (a provision which had not been included in the initial ministerial draft), however, not on the basis of a decentralised Blockchain.

An amendment to the anti-money laundering rules regarding cryptocurrencies is also being proposed. According to draft legislation currently going through parliament, the transfer of crypto values exceeding the equivalent of EUR 1,000 between natural or legal persons in the context of the provision of financial services, or the operation of banking transactions within the meaning of the German Banking Act (Kreditwesengesetz), requires KYC obligations to be fulfilled by in-scope entities. This also includes transactions that are carried out outside of a business relationship, but expressly does not include services exclusively concerning crypto custody (within the meaning of Section 1 (1a) sentence 2 number 6 of the German Banking Act). This legislative proposal aims to implement FATF recommendation 15, interpretative guide section 7a), according to which in-scope entities must fulfill general duties of care when transferring crypto assets outside of a business relationship and above a threshold value of EUR 1000.

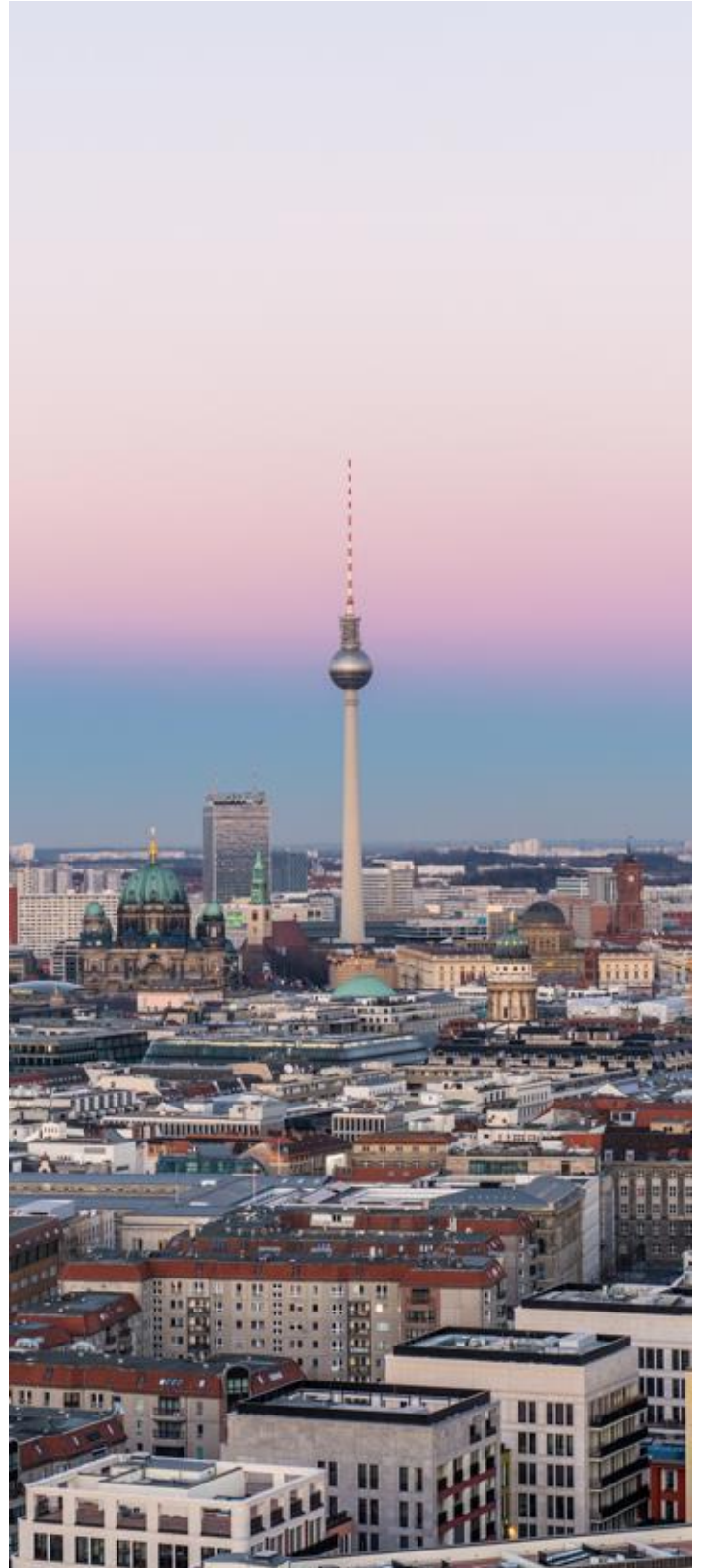
Key Contacts



Nina-Luisa Siedler
Partner
M +49 151 14368441
E Nina.Siedler@dwf.law



Axel von Goldbeck
Partner
M +49 170 5543936
E Axel.VonGoldbeck@dwf.law



Poland

The PFSA

The PFSA has recently published advice on investing in cryptocurrencies and other digital assets. The PFSA warns against hastily investing savings in financial instruments that are difficult to understand. Many people may be motivated to invest in cryptocurrencies due to low interest rates on savings offered by banks and due to the increase in the valuation of some digital currencies. However, the PFSA warns that investing in cryptocurrencies may easily result in the loss of some or all of the funds.

The PFSA has reminded investors that the cryptocurrency market is not regulated, and is not supervised by the PFSA or any other regulator in Poland. Therefore, there is no means of redress for investors to recover their money in a situation where, for example, a cryptocurrency exchange declares bankruptcy. The PFSA also noted that the cryptocurrency market is characterised by high volatility, which, on the one hand allows investors to gain large profits, but on the other, may easily lead to losing a large part of the invested capital. As a proof of this volatility, the PFSA presented a chart of the bitcoin exchange rate, which initially recorded huge increases, and later a spectacular decline.

The PFSA pointed out that any possible pursuit of claims from unreliable entrepreneurs (such as cryptocurrency exchanges, brokers, etc.) may be very difficult, especially given the fact that often these are entities based and registered abroad.

The PFSA warned that cryptocurrencies such as Bitcoin or Ethereum are not issued or guaranteed by the central bank of the state, nor are they money. Their value does not depend on the value of another asset (e.g. gold, euro, dollar) and is determined on the basis of their popularity among investors.

The PFSA indicated that cryptocurrencies may be used to commit various types of crimes, such as creating financial pyramids (Ponzi scheme) or false initial coin offerings, where issuers disappear once they obtain financing, and cryptocurrencies paid-up by investors are never issued.

The PFSA has helpfully published information about the rules governing the market on cryptocurrency investments. It includes, for example, definitions of payment tokens, stablecoins, investment and utility tokens, cryptocurrency mixers and cryptocurrency wallets. Therefore, it may be a valuable source of information for those who are interested in the world of crypto assets and are looking for a compendium of knowledge about it.

More information on this subject can be found [here](#).

AML Legislation

Counteracting money laundering and the financing of terrorism - implementing the Fifth Anti-Money Laundering Directive ("AMLD V") into Polish law

The Council of Ministers has adopted a draft amendment to the Act on counter money laundering and terrorist financing, thereby implementing AMLD V.

The proposed new law extends the scope of institutions subject to anti-money laundering/terrorist financing obligations by adding those conducting the following activities:

1. trading or brokerage in works of art, collectors' items and antiques; and
2. the storage, trade or brokerage of these goods (in respect of transactions with a value of EUR 10,000 or more, regardless of whether the transaction is carried out as a single operation or several operations which appear to be related to each other).

The new regulations specify the definitions of, among others, a beneficial owner, a Member State and a group. Moreover, they extend the scope of statistics and data collected by the Polish General Inspector of Financial Information and specify the rules concerning the application of financial security measures by in scope institutions, as well as activities undertaken by them, in relation to high-risk third countries.

In addition, the draft law specifies the rules for in-scope institutions storing documents and information obtained as a result of KYC/AML checks.

The new law obliges EU Member States to publish and update the list of public posts and functions that qualify as politically exposed positions under national laws. It also introduces mechanisms for verifying data contained in the Central Register of Ultimate Beneficiaries and the obligation to register "*entities providing currency exchange services between virtual and fiduciary currencies*" and "*providers of virtual currency accounts*".

The bill is currently being reviewed by the Polish parliament. As soon as the parliament completes its works, which is expected to be soon, the bill shall be delivered to the President for the sign-off. The new law shall enter into force 14 days following its publication in the Journal of Laws, however, some provisions of the new law shall be effective 6 months following the publication. Financial institutions should follow the works on the new law and plan adjustments to new requirements to be imposed on them.

Key Contacts



Adam Stopyra
Partner
M +48 571 244 772
E Adam.Stopyra@dwf.law



Michał Toronczak
Senior Associate
M +48 692 003 532
E Michal.Toronczak@dwf.law



Updates

The regulatory framework that governs the financial crime and fraud in the UAE is multi-layered, which includes federal legislation, as well as legislation issued by each Emirates. A number of offshore jurisdictions, like the Dubai International Financial Centre ("**DIFC**") and Abu Dhabi Global Markets have also issued supplementing regulations. The Central Bank of the UAE ("**CBUAE**") also regulates the activities relating to financial institutions and money exchanges.

In 2020, the Financial Action Task Force (FATF) and the Middle East and North Africa Financial Action Task Force (MENAFATF) assessed the UAE's anti-money laundering and counter terrorist financing ("**AML/CFT**") system. The FATF/MENAFATF determined that the UAE has taken significant steps to strengthen relevant laws and regulations and had put in place a range of committees to improve national coordination and cooperation. However, the framework was relatively new, and further time was needed to determine its effectiveness. Further, authorities had access to a broad range of financial information in their investigations of terrorist financing, fraud and other offences. The UAE has achieved positive results in investigating and prosecuting the financing of terrorism, but its limited number of money laundering prosecutions and convictions, particularly in Dubai, are a concern given the country's risk profile.

The regulators have been actively taking steps to address the concerns raised by FATF, and there has been an increase in enforcement actions being taken by the regulators.

Since the beginning of 2021, the following significant cases have been reported:

- In 2018 the UAE issued the updated Federal Decree Law No. (20) of 2018 on Anti-Money Laundering and Combating the Financing of Terrorism and Financing of Illegal Organisations which was followed by regulation issued by the UAE Cabinet and various decisions of the CBUAE board. All banks in the UAE were provided with a grace period in which to update their compliance and align it with the AML/CFT.

The CBUAE recently fined 11 banks operating in the UAE a total amount of AED 45.75 million for failing to achieve appropriate levels of AML & Sanctions Compliance Frameworks within the grace period afforded by the CBUAE. The CBUAE has stated that it will continue to work closely with all financial institutions in the UAE to ensure AML/CFT compliance and will continue to impose administrative and/or financial sanctions, for non-compliance by such institutions.

In another instance, the CBUAE fined the Bank of Baroda, GCC Operations in Dubai, AED 6,833,333 for non-compliance with AML/CFT.

- The Abu Dhabi Criminal Court has handed down a 15-year prison sentence to the former Chairman of the Board of Directors of a government-owned Abu Dhabi company, and the CEO of the same company, in relation to money laundering. Both individuals were ordered to pay fines and return approximately AED 8 billion of money received by them. The court also ordered the seizure of the proceeds of crime and the property of equivalent value and ordered the deportation of the CEO after he has served his sentence

The two individuals were accused of misusing their position with the company they worked for by using the name of the parent company to create two clone companies, which were used to contract with companies based abroad. They used the two "clone" companies (with the same name as the parent company) to enter into parallel and identical agreements with the companies based abroad. The money the two individuals received pursuant to the agreements was transferred to the two clone companies and then to the personal accounts of each individual, while the obligations in relation to the executed contracts remained with the parent company.

- A former relationship manager of a private bank in the DIFC has been fined AED 165,000 for his involvement in anti-money laundering law breaches and for hindering the investigation of the Dubai Financial Services Authority ("**DFSA**"). A distinction was made by the DIFC that the employee was not judged to have engaged in money laundering but was found guilty of being involved in breaches of the applicable anti-money laundering law.

The employee established the BVI entity (in which he was a director and registered beneficial owner) with the help of an individual that would often act as an "*introducer*" for the bank. The employee arranged for the introducer's referral fees to be paid by the bank to the BVI company. The bank believed that company was owned by the introducer and did not conduct any verification in relation to ownership of the BVI company. Some of the employee's clients also provided instructions whereby their money was transferred from the bank to the BVI company.

Money was then routed from the BVI company to personal accounts of the employee. The employee's involvement with the BVI company had not been disclosed to his employer. The DFSA said the banker's involvement with the offshore firm was not disclosed to his employer and this warranted action to be taken by the DFSA "*in order to maintain the integrity and reputation of the DIFC, and to protect direct and indirect users of the financial services industry*" in the DIFC.

Furthermore, the DFSA has clearly stated that it expects complete honesty and transparency from all financial institutions and the employees of such institutions that it licenses.

It is clear from the recent trends that regulatory authorities are keen to investigate and hold financial institutions and their employees accountable for any breaches of applicable financial laws and regulations. Specifically, authorities are looking to proactively enforce the anti-money laundering laws issued in the UAE whether such laws are issued for onshore financial institutions or those in the free zones.

Key Contacts



Umera Ali
Partner, Head of Banking, Finance & Corporate (UAE)
M +971 52 3859126
E Umera.Ali@dwf.law



Aisha Gondal
Director
M +92 3007 091978
E Aisha.Gondal@dwf.law



Saudi Arabia



Updates

The Central Bank of Saudi Arabia ("**SAMA**") is the main regulator responsible for monitoring and enforcing these regulations, and there has been a significant increase in enforcement actions.

– Thirty-two people have been arrested as part of a corruption investigation into the bribery of bank employees, and money laundering of approximately SAR 11.6 billion out of the KSA. The Oversight and Anti-Corruption Authority ("**Nazaha**") initiated the investigation in cooperation with the SAMA. The authorities discovered that certain bank employees had received bribes from a group of residents and businessmen in exchange for depositing large sums of cash from unknown sources before transferring the money out of the KSA, in breach of a number of KSA laws and regulations including the anti-money laundering law.

Of the thirty-two arrested, twelve were bank employees who have been accused for their involvement in bribery, fraud, exploitation of their positions for financial gain and money laundering.

Nazaha has also arrested around forty-eight government employees from seven different ministries as part of their continued efforts against corruption and money laundering. Employees from the Presidency of State Security, the Saudi

Food and Drug Authority and the General Authority of Meteorology and Environment Protection were arrested, accused of bribery, abuse of influence and power, as well as fraud and forgery.

– Authorities in the KSA have recently disbanded an organized crime gang that was involved in money laundering. The accused were found to have laundered approximately SAR 64.86 million (including large quantities of gold) and were given different sentences by the courts with a combined imprisonment of sixty four years. The expatriates who have been imprisoned will be deported once they have completed their sentences.

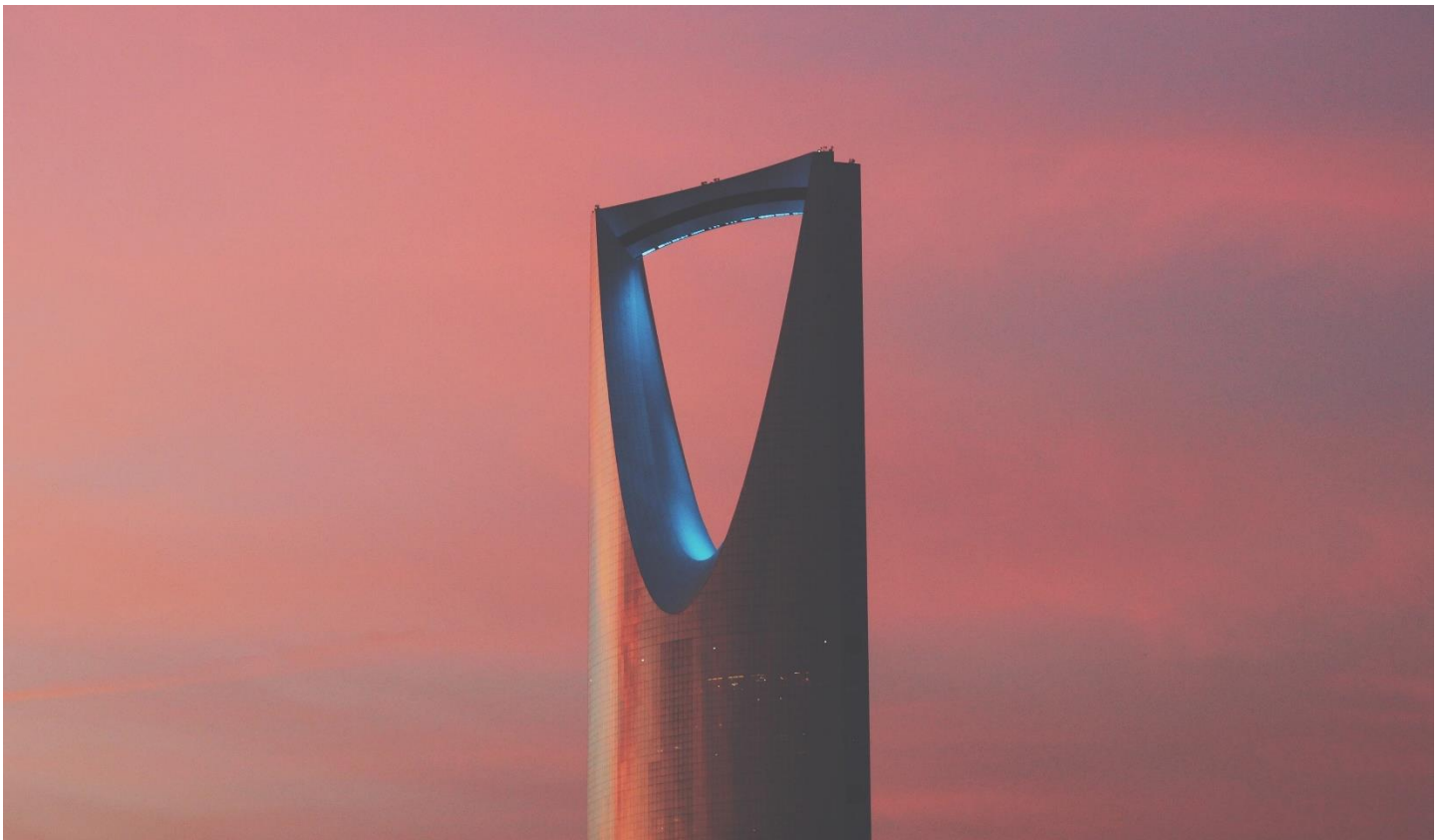
Key Contacts



Umera Ali
Partner, Head of Banking, Finance & Corporate (UAE)
M +971 52 3859126
E Umera.Ali@dwf.law



Aisha Gondal
Director
M +92 3007 091978
E Aisha.Gondal@dwf.law





Beyond borders, sectors and expectations

DWF is a global legal business, connecting expert services with innovative thinkers across diverse sectors. Like us, our clients recognise that the world is changing fast and the old rules no longer apply.

That's why we're always finding agile ways to tackle new challenges together. But we don't simply claim to be different. We prove it through every detail of our work, across every level. We go beyond conventions and expectations.

Join us on the journey.