CCL
GOVERNANCE | RISK | COMPLIANCE

ISSUED 15th July 2020

Regulatory Update

Middle East Edition

JUNE 2020

INDEX

CONTACTS

NIGEL PASEA
Managing Director
NPasea@cclcompliance.com

JADE ASHPOLE
Managing Consultant
JAshpole@cclcompliance.com

1.0 DIFC AND DFSA LATEST DEVELOPMENTS

1.1 DFSA Publishes Cyber Thematic Review Report

The Dubai Financial Services Authority (DFSA) has published a thematic review report on cyber risks. The review was launched in July 2019 to assess:

- IT/cyber risk governance frameworks
- IT/cyber hygiene practices
- IT resilience programmes

The review was conducted in two phases:

Phase 1 – a high level, mainly multiple-choice questionnaire on each firm's cyber security practices. This was sent to 490 firms and the DFSA received 392 responses.

Phase 2 – twenty firms of a varying range of business models and financial services activities had desk-based reviews and onsite visits as well as a review of cyber risk management documentation.

The findings were grouped into three areas: governance, hygiene, and resilience – each has room for improvement and a summary of the findings can be found below:

Governance

- A significant number of firms have not implemented a cyber risk management framework.
- A significant number of firms perform only a limited cyber risk assessment and don't pay sufficient attention to the sensitivity of processed data. In addition, they have a tendency to identify cyber risks only in relation to availability of IT systems.
- In many instances, neither the board nor senior management oversight of cyber risk management was sufficient, with a lack of evaluation by senior management of cyber security audits, reviews and tests.
- Only half of all firms have a due diligence process to assess whether third-party service providers meet the firm's cyber security requirements.
- The vast majority of firms mostly focus on IT equipment only when classifying their IT assets.
- A significant number of firms have not established a comprehensive and regular cyber security training programme or campaign to enhance the overall cyber security awareness.

Hygiene

- A significant number of firms have not performed vulnerability assessments or penetration tests of their critical information systems in the past year. Firms using off-the-shelf systems see it as a responsibility of the system vendors, rather than having oversight of the system themselves once it has been bought.
- In cases where critical information systems are accessible from the internet, some firms rely on basic user authentication using usernames and passwords and have not implemented strong password policies.
- A significant number of small and medium-sized firms do not enforce encryption of workstation hard drives and portable devices to protect sensitive data.

Resilience

- Half of all firms do not have continuous identification and response capabilities for managing cyber incidents in regard to all critical information systems. Small and medium-sized firms rely mainly on manual processes to monitor their infrastructure only during working hours or do not have monitoring capabilities at all.
- The majority of firms have implemented some form of a cyber incident response plan to respond to, and limit the consequences of, a cyber incident. However, in many cases, the cyber response procedures are addressed in general terms as components of the business continuity plan and are not tailored specifically to

cyber threats.

- Less than half of all firms have implemented a crisis management communication plan that addresses external stakeholders (e.g. clients, media, critical service providers, regulators, law enforcement) and even fewer firms have implemented an internal crisis communication plan (designed for relevant business units, senior management, board of directors, etc.).
- More than half of firms' cyber incident response plans do not include a formal requirement for periodically testing their response to a cyber incident. Moreover, where firms do have a periodic testing requirement, the DFSA identified that a significant number of firms have not tested any component of their cyber incident response plans in the past year.
- Some small and medium-sized firms use professional forums or groups to get information about cyber threats but tend not to share information about cyber incidents. Firms noted lack of sufficient detection capabilities and potential reputational harm as the main reasons for not sharing information about cyber incidents.

Firms are strongly encouraged to consider the DFSA findings and implement enhancements to their cyber security frameworks, where necessary.

1.2 DFSA and Deloitte Middle East Publish Discussion Paper on Digital Assets Custody

The DFSA and Deloitte Middle East have published "A Market Overview of Custody for Digital Assets" to highlight the importance of digital asset custodians and the key role they play. The overview contains analysis of the current digital custody landscape, market solutions currently available, and the challenges and uncertainties currently faced by the industry.

The different categories of digital assets including security tokens, utility tokens, cryptocurrencies, stablecoins and e-money tokens are explored in the paper, as are the reasons why custody of such digital assets is becoming increasingly important. The custody of digital assets stands to:

- Reduce risk and complication
- Increase security
- Introduce recourse for investors
- Be safer than exchanges
- Enhance operational efficiency

Key regulatory considerations regarding digital assets and their custody include the safety of the asset itself, whether the custodians are trusted with the security of the asset delegated to them and the classification of the digital assets. An example of the classification of digital assets may include security, commodity or currency.

The paper also highlights the key parts that the regulator, the custodian, and the investor must play in the increasingly popular - but not yet fully navigated - landscape of digital assets.

1.3 DIFC and DFSA Host RegTech Event

The DFSA and DIFC hosted their first Regulatory Technology ("RegTech") 'RegTech Live' event on the 2nd and 3rd of June. The event, held in partnership with the Dubai International Financial Centre Authority (DIFCA), drew over 600 delegates from the financial sector around the globe, centering on the theme of driving compliance through innovation.

The webinar event focused on discussions and thoughts around regulatory compliance technology and included keynote speeches, demonstrations, and insights into many emerging RegTech trends such as Know Your Customer ("KYC"), onboarding processes and transaction monitoring. The event also provided an insight into regulatory expectations around eKYC and digital onboarding technologies.

RegTech advances within the DIFC include the DFSA's introduction of chatbots to address queries on the DFSA Rule Book and the introduction of automated licence approval for low-risk entities, which will be introduced later in 2020.

Further information
If you have any questions or concerns regarding these DFSA and DIFC developments and requirements, please contact Jade Ashpole.

2.0 ADGM AND FSRA LATEST DEVELOPMENTS

2.1 FSRA Proposes Updating its Regulatory Framework for Money Services

The FSRA has released Consultation Paper No.1 of 2020 "Proposals for Revision of the Regulatory Framework for Providing Money Services in ADGM".

This paper amends the previous framework for Providing Money Services ("PMS") that was released by the FSRA.

The amendments include:

- Revision of the regulated activity
  - Expanding the activities under PMS to reflect the provision of payments accounts. Payment accounts are now considered alongside the activities of selling or issuing payment instruments and stored value collectively referred to as "Payment Services" under PMS.
  - Money Transmission will be rebadged as "Money Remittance" and will cover "receiving money or monetary value for transmission remittance, including electronic transmission remittance, to a location within or outside the Abu Dhabi Global Market, without the use of a Payment Account, Payment Instrument or stored value"
- Introduction of a new chapter to the Conduct of Business Sourcebook ("COBS")
  - The new chapter will reflect the provision of payment accounts and aims to clarify regulatory requirements for money remittance and stored value.
  - The FSRA defines new terms including "Framework Contract", "Low Value Payment Instrument", "Single Payment Service Contracts" and "Relevant Money".
  - All firms undertaking PMS will no longer need to classify clients in accordance with the current COBS Chapter 2, due to the nature of the business models in this sector and the underlying activities they encompass.
- Base Capital Requirement ("BCR") and Expenditure Based Capital Minimum ("EBCM") Changes
  - As PMS currently falls under prudential Category 3C, the BCR component is set at $250k for the calculation of the minimum capital requirement ("MCR"). The EBCM component is either 18/52nds or 13/52nds of Annual Audited Expenditure. The FSRA is proposing an additional component of the calculation of the MCR, i.e. a variable capital requirement for all PMS firms other than those that provide currency exchange, on the basis that this would be more risk-sensitive than the BCR or the EBCM (where applicable). This will vary for firms who offer stored value, money remittances and payment accounts.
- Fee changes
  - The authorisation fee for firms seeking PMS permissions will increase. The proposed authorisation and annual supervision fee would be $15,000 for currency exchange or money remittance services, $25,000 for payment services or $25,000 for both permissions.
- Implementation date and transitional period
  - All money remitters and Payment Service Providers ("PSPs") currently operating in ADGM would have a period of twelve months from the implementation date of the revised requirements to comply with them, and the same transitional period would also apply to applicants having received as of that date an "in-principle approval" to operate as such in ADGM.

- Anti-Money Laundering and Sanctions Rules and Guidance ("AML") Changes
  - Changes will be implemented into the AML Rulebook in order to ensure that firms engaged in PMS conduct and appropriate AML oversight of all agents involved in their business activities. They will be required to train, oversee and assess the AML compliance of their agents on a continuing basis as necessary.
- Other proposed amendments
  - There will be a limit on aggregate funds and transaction volumes for individual customers.
  - A guidance will be issued for the authorisation of PSPs which will highlight appropriate interpretation of threshold conditions.
  - A supplementary application form will be introduced for firms seeking authorisation.

2.2 RA Issues Public Consultation on Updates to its Decision Procedures and Enforcement Manual

The ADGM's Registration Authority (RA) has released Consultation Paper No.2 of 2020 with a proposed update to the Decision Procedures and Enforcement Manual.

Previously, the RA had a Registry Decisions Committee ("RDC") that was used in the decision-making process for enforcement action. The RA has decided to disband the RDC and may choose to appoint a delegate decision maker on a case-by-case basis.

The appointed delegates would be senior executives of the RA and would not be involved in establishing evidence in the case.

2.3 ADGM and FSRA Make Amendments to Regulations

The ADGM and FSRA made the following amendments to the regulations in June 2020:

- The FSRA has published amendments to the Common Reporting Standard Regulation, including two new sanctions for non-compliance by account holders or controlling persons, and reporting financial institutions.
- The FSRA has amended its Schedule of Contraventions and applicable fines including changes to Commercial Licensing Regulations 2015 (Fines) Rules 2020.

Further information
For any questions or concerns regarding the ADGM or FSRA, please contact Kareem Wahid.

3.0 MIDDLE EAST REGULATORY UPDATES

3.1 SCA Launches a New Version of its Digital Platform

The UAE's Securities and Commodities Authority ("SCA") has updated its digital platform to support the recently increased reliance on technologies for business continuity and to increase efficiency.

The updated version of the application uses a chatbot, or "automated responder technology" to provide customers with automated responses to their general and legislation related questions, using the SCA's legislation database.

The updated application also enables users to access all the data and information published by the SCA, including legislation, circulars, and news and also complements the Licensing Department's existing system which facilitates licensing requirements, applications and procedures.

4.0 INTERNATIONAL UPDATES

4.1 FATF Proposes Amendments to Recommendation 1 to Include Proliferation Financing Risk

The Financial Action Task Force ("FATF") has proposed that Recommendation 1 of the FATF Recommendations which recommends that countries "identify, assess, and understand the money laundering and terrorist financing risks for the country, and should take action…" ought to include proliferation financing.

Proliferation financing is the act of providing funds or financial services which are used, in whole or in part, for the manufacture, acquisition, possession, development, export, transshipment, brokering, transport, transfer, stockpiling or use of nuclear, chemical or biological weapons and their means of delivery.

The FATF has recommended that countries should identify, assess, and understand the proliferation financing risks in their jurisdiction and mitigate these risks effectively.

The proposed amendments seek to reinforce the implementation of targeted financial sanctions, by obliging financial institutions and DNFBPs to assess the risks of breach, non-implementation and evasion of targeted financial sanctions related to proliferation financing.

4.2 FATF Update Jurisdictions with Increased Monitoring

The FATF has updated its "grey list" of jurisdictions which are actively working with them to address strategic deficiencies in their regimes against money laundering, terrorist financing and proliferation financing.

Due to COVID-19, the FATF gave jurisdictions on the grey list an additional four months to meet their deadlines. Two jurisdictions on the list, Mongolia and Iceland, declined the extension and were reviewed within the original timeline. Both Mongolia and Iceland made good progress and will receive an onsite visit as soon as possible from the FATF.

The grey list remains as follows:

- Albania
- The Bahamas
- Barbados
- Botswana
- Cambodia
- Ghana
- Jamaica
- Mauritius
- Myanmar
- Nicaragua
- Pakistan
- Panama
- Syria
- Uganda
- Yemen
- Zimbabwe

Further information
For any questions or concerns regarding these updates, please contact Jade Ashpole.

5.0 ENFORCEMENT ACTION

5.1 Deutsche Bank Fined $150million for Compliance Failures

The New York State Department of Financial Services has fined Deutsche Bank $150 million for compliance failures in connection to its relationship with Jeffrey Epstein, and correspondent relationships with Dankse Bank Estonia and FBME Bank.

Deutsche Bank failed to adequately monitor the activities of its customer, whom the Bank itself had deemed high risk. Within the banking relationship the bank knew of Mr. Epstein's criminal history and did not detect or prevent millions of dollars' worth of suspicious transactions.

Suspicious transactions included:

- Settlement payments totaling over $7 million, as well as dozens of payments to law firms totaling over $6 million, for what appear to have been the legal expenses of Mr. Epstein and his co-conspirators.
- Periodic suspicious cash withdrawals - in total, more than $800,000 over approximately four years.

Regarding Danske Estonia and FBME, the Department concluded that Deutsche Bank failed to properly monitor the activities of its foreign bank clients with respect to their correspondent and dollar clearing business.

5.2 Swedish SEB Fined for Poor Anti-Money-Laundering Measures

The Swedish regulator, Finansinspektionen, has fined Skandinaviska Enskilda Banken ("SEB") $107 million for failing to implement adequate anti-money laundering ("AML") measures in its subsidiaries based in Baltic countries. An investigation was launched in 2015 and concluded that "customers with a higher risk of money laundering" had made a "substantial portion of the subsidiary banks' business volumes and transactions".

The regulator found that the bank had been exposed to an elevated risk of money laundering due to:

- A substantial portion of the subsidiary bank's business volumes and transactions coming from customers with a higher risk of money laundering.
- A deficiency in identifying and managing the risk of money laundering associated with non-resident customers and resident customers with non-resident owners.
- A failure to rectify deficiencies identified by the bank's control bodies.
- A failure to have sufficient resources for internal control functions and transaction monitoring.

SEB's Estonian subsidiary is also receiving a fine from the Estonian financial supervisory authority for breaches of local AML requirements.

Further information
If you have any questions or concerns regarding enforcement action, please contact Jade Ashpole.

ABOUT CCL

CCL has been providing a comprehensive range of regulatory compliance services to firms in the financial services industry since 1988, with offices in London, Dubai, Abu Dhabi, and Mumbai. We combine a long history and extensive experience in financial services compliance with the expertise of a team of practitioners that includes former regulators, senior compliance professionals, lawyers and accountants.

Consultancy Services & Support

- Compliance Advisory
  - Assurance Reviews
  - Compliance Remediation
  - Financial Crime Prevention
  - Corporate Governance
  - Risk Management
  - Prudential Rules & Regulatory Reporting
- Authorisation
- Outsourcing (Compliance Officer & MLRO)
- Documentation
- Regulatory Technology – CCL C.O.R.E

Training (through CCL Academy)

- Compliance
- AML & Financial Crime Prevention
- Rules & Regulations
- Senior Management & The Board
- Finance Induction
- CISI Qualifications

If you wish to discuss how CCL can assist you with any of the issues raised in this Regulatory Update, please contact us the details below:

Email: **info@cclcompliance.com**
Website: **www.cclcompliance.com**
Tel: Dubai +971 4 323 0800 | Abu Dhabi +971 2 440 2146

or write to us at:

CCL Limited
Level 2, Gate Village Building 7,
Dubai International Financial Centre (DIFC),
Dubai, PO Box 506733,
United Arab Emirates

This Regulatory Update provides information about the consultative documents and publications issued by various regulators which are still current, proposed changes to the Rules and Guidance set out in Handbooks, actual changes to Rules and Guidance that have occurred in the months leading up to the update and other matters of relevance to regulated firms. This Regulatory Update is intended to provide general summarised guidance only, and no action should be taken in reliance on it without specific reference to the regulators' document referred to.