

New Central Bank Guidance for UAE Financial Institutions on Suspicious Activity/Transaction Reporting

August 19, 2021

Introduction

On June 7, 2021, the UAE Central Bank issued [new guidance](#) requiring all UAE financial institutions to file suspicious activity reports (SARs) or suspicious transaction reports (STRs) with the UAE's Financial Intelligence Unit (FIU) using the goAML portal within 35 calendar days of detection of any conduct that they reasonably suspect may be linked to money laundering, terror financing or other criminal activity.

The guidance memorializes the UAE Central Bank's "expectations" of UAE financial institutions and is intended to be read in conjunction with the UAE Central Bank's earlier [Procedures for Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations](#), dated June 13, 2019, and [Guidelines on Anti-Money Laundering and Combating the Financing of Terrorism and Illicit Organizations for Financial Institutions](#), dated June 23, 2019.

Reasonable Grounds for Suspicion Trigger the Reporting Obligation

The guidance begins by reminding UAE financial institutions that, under the UAE's anti-money laundering (AML) and countering the financing of terrorism (CFT) legal and regulatory framework, including [Federal Decree-Law No. 20 of 2018 on Anti-Money Laundering and Combatting the Financing of Terrorism and Financing Illegal Organizations](#) (AML-CFT Law), dated October 30, 2018, their obligation to report to the FIU is not confined to instances where they have actual knowledge of an underlying crime. Rather, possessing "reasonable grounds to suspect" that the relevant funds are related to a crime triggers their reporting obligation. See our previous analysis of the UAE AML-CFT Law [here](#).

Importantly, the UAE requires the reporting of suspicious activities, as well as suspicious transactions. The new guidance explains that the following would all constitute reportable suspicious activities: customers being subject to adverse media; customers matching against sanctions lists; customers refusing to answer or reluctantly answering questions at account opening; and customers providing false documentation. The new guidance also reminds UAE financial institutions that there is no minimum reporting threshold and, therefore, all suspicious activities and transactions, including attempted transactions, should be reported regardless of value.

Best Practices for Drafting SARs/STRs and Mandatory goAML Filings

The new guidance identifies best practices for drafting SARs/STRs, including identifying the transacting parties, especially the ultimate originator and beneficiary, as well as beneficial owners, directors, officers and authorized signatories, and the "instruments and mechanisms ... being used to facilitate the suspicious activity or transaction(s)." On that final point, the factors to consider will, of course, vary from one UAE financial institution to the next (for example, a depository institution versus an insurance company, which offer dissimilar products and services to their respective customer bases).

The information supplied in SARs and STRs allows the UAE FIU to identify vulnerabilities and threats to the UAE financial system, to identify and communicate emerging trends and typologies, and to assist law enforcement to detect and arrest criminal actors. All entities under CBUAE's supervision, including all UAE financial institutions and Designated Non-Financial Businesses and Professions (DNFBPs), are required to register for the UAE's goAML system immediately upon receipt of their financial services/commercial licenses. The goAML system is an integrated digital platform through which financial institutions and DNFBPs can submit SARs/STRs to the UAE FIU, and through which the UAE FIU can distribute notifications and guidance to financial institutions and DNFBPs.

New Expectations Regarding Timely Alert Dispositioning and SAR/STR Filings

The new guidance also addresses regulatory expectations concerning efficient alert management and timely alert dispositioning and suspicious activity/transaction reporting. UAE financial institutions are directed to apply a risk-based approach to the alert review process by prioritizing alerts commensurate to their risk ratings. For instance, alerts related to suspicious activities or transactions of high-risk customers should be risk-scored higher and prioritized for review. Ultimately, UAE financial institutions are responsible under the AML-CFT Law to report suspicious activities or transactions "without delay." Failure to do so, whether intentionally or by gross negligence, is a federal crime in the UAE and punishable under the AML-CFT Law by imprisonment and a fine of up to one million dirhams.

The new guidance sets out maximum timelines by which UAE financial institutions must identify and report suspicious activities and transactions. Specifically, by the end of the first 20 calendar days from alert generation, a case investigator must have analyzed the alert or other indicator of suspicion, conducted any further investigation that may be necessary, and made an internal recommendation to the MLRO as to whether a SAR/STR filing is warranted. Also within those first 20 calendar days, the MLRO must have reviewed the case report, considered the recommendation, and finally dispositioned the alert or activity. By the end of a further 15 calendar days, the MLRO must have filed a SAR/STR with the FIU in respect of anything determined to be suspicious.

The new guidance recognizes that, in some cases, for example where a law enforcement authority identifies for a financial institution an ongoing money laundering scheme, or where a financial institution harbors serious concerns a transaction pertains to terror financing, an alert or case may need to be dispositioned and a SAR/STR filed more rapidly than usual processes contemplate. In such an instance, the relevant financial institution should submit to the FIU a SAR/STR within 24 hours of the MLRO dispositioning the alert or activity as suspicious.

In other cases, UAE financial institutions will encounter potentially unusual or suspicious activity that is of a “complex” nature. In such an instance, the relevant financial institution should submit to the FIU an initial SAR/STR, annotated as a “complex investigation,” within 15 days of determining that the activity is suspicious. Following the initial SAR/STR filing, the financial institution has an additional 30 days to obtain all necessary information related to the complex investigation and to submit to the FIU a follow-up SAR/STR. The guidance provided a non-exhaustive list of factors to be considered when determining whether activities/transactions that have been investigated qualify as complex: employee-related investigations; significant investigations involving multiple customers, multiple jurisdictions, multiple accounts, multiple transactions and/or multiple subpoena requests; and legal referred investigations.

In light of this new guidance, UAE financial institutions should ensure they have clear policies, procedures and training programs governing the identification of suspicious activity or transactions, including attempted transactions, as well as the degree and extent of investigation that is appropriate prior to reporting.

Central Bank Cautions Against Defensive SAR/STR Filings

Importantly, however, the new guidance cautions UAE financial institutions that defensive filings could result in the imposition of supervisory measures by the Central Bank, including administrative sanctions or a temporary limitation on certain business activities. According to the Central Bank, it will view defensive SARs/STRs, filed by UAE financial institutions in order to reduce the risk of regulatory penalties for non-filing rather than to report on activities or transactions that are considered truly suspicious, as indicative of inefficient transaction monitoring systems and weak internal controls.

Recommended Post-SAR/STR Filing Processes

The new guidance also explains that, following submission of a SAR/STR, the FIU may or may not revert to the UAE financial institution with specific instructions, requests for additional information, feedback or further guidance related to the SAR/STR or to the business relationship more generally. Regardless of whether the FIU contacts the UAE financial institution, that institution is expected to (1) “identify all related/associated accounts or relationship of STR or SAR customers and conduct a review on those accounts/relationship to check whether any suspicious transaction(s) has taken place. If yes, appropriate risk-based Enhanced Due Diligence (“EDD”) and ongoing monitoring procedures should be implemented”; and (2) “the customer or business relationship, including the related/associated accounts and relationship to the SAR or STR customers, should immediately be classified as a high-risk customer and appropriate risk-based EDD and ongoing monitoring procedures should be implemented in order to mitigate the associated money laundering and the financing of terrorism and illegal organizations risks.” In instances where the FIU does not revert substantively, and subject to the requirement not to “tip off” a customer or any other person, whether directly or indirectly, that a SAR/STR has been filed or will be filed, or that an investigation is underway concerning an activity or transaction, a UAE financial institution must come to its own decision regarding whether to retain or exit the relevant customer relationship, or to maintain or restrict an account, product or service, based on its internal policies and procedures and its risk appetite. A UAE financial institution could help inform its decision by conducting enhanced due diligence, engaging an external party to render third-party professional advice, and reassessing the customer risk profile and the business relationship risk.

Additionally, UAE financial institutions that decide to maintain a relationship after filing a SAR/STR would be well served by documenting the process by which the decision was released, the rationale for the decision, and the implementation of any additional control measures to manage and mitigate the money laundering/terror financing risk, such as requiring additional data, information or documents from the customer in order to carry out transactions or restricting the customer’s use of certain products or services.

Mandatory Document Retention Period

UAE financial institutions are reminded that, under [Cabinet Decision No. 10 of 2019 Concerning the Implementing Regulation for the AML-CFT Law](#), they are required to retain all records and documents pertaining to SARs/STRs and the results of all related internal analyses or investigations for a period of at least five years from the date of completion of the activities/transaction or termination of the business relationship.

Common UAE Typologies and Red Flag Indicators

Finally, the new guidance includes common typologies and red flag indicators of money laundering or terror financing in the UAE, as identified by the FIU. There are general indicators, including transactions involving locations with poor AML/CFT regimes or high exposure to corruption; significant and/or frequent transactions in contrast to known or expected business activity or employment status; ambiguous or inconsistent explanations as to the source and/or purpose of funds; and, where relevant, nervous or uncooperative customer behavior. There are also possible indicators with respect to more specific activities/transactions, including wire transfers; dealing in valuable assets or commodities; offshore companies; nominees and trustees; trade-based money laundering; cancellation of credits or overpayments; commingling of funds; cash dealings; check dealings; structuring; smurfing; underground banking and alternative remittance services; and currency conversion and cash exchanges. UAE financial institutions should review these typologies and red flag indicators carefully and consider whether updates are necessary to policies, procedures and detection scenarios.

Contacts

Benjamin D. Wood

Partner, Washington DC
T +1 202 457 6685
E benjamin.wood@squirepb.com

Kevin P. McCart

Partner, Washington DC
T +1 202 457 6457
E kevin.mccart@squirepb.com

Claiborne W. Porter

Partner, New York
T +1 212 872 9839
E claiborne.porter@squirepb.com

Richard J. Gibbon

Partner, Abu Dhabi and Dubai
T +971 2 651 5900 and +971 4 447 8700
E richard.gibbon@squirepb.com