Financial crime systems and controls during coronavirus situation

Discover our expectations on how firms should apply their systems and controls to combat and prevent financial crime during this crisis.

Maintaining the integrity of the financial market is a key objective for the FCA. In the current climate, it is important for firms to maintain effective systems and controls to prevent money laundering and terrorist financing.

Criminals are already taking advantage of the coronavirus (Covid-19) pandemic to carry out fraud and exploitation scams through a variety of methods, including cyber-enabled fraud. Those seeking to launder criminal proceeds or finance terrorism are likely to also exploit any weaknesses in firms' systems.

We are already working with partners in law enforcement such as the National Economic Crime Centre (NECC) to share information on Covid-19 related financial crime, and will continue to do so as new risks emerge or as criminals change their approach.

It is important that firms remain vigilant to new types of fraud and amend their control environment where necessary to respond to new threats. This should include the timely reporting of Suspicious Activity Reports (SARs) of any new threats.

Operational challenges

While we recognise that the current climate may give rise to operational challenges in relation to financial crime systems and controls, firms should not seek to address operational issues by changing their risk appetite. For example, firms should not change or switch-off, current transaction monitoring triggers/thresholds, or sanctions screening systems, for the sole purpose of reducing the number of alerts generated to address operational issues.

However, we do recognise that, while continuing to operate within the legislative framework for anti-money laundering and counter terrorist financing, firms may need to re-prioritise or reasonably delay some activities. These could include ongoing customer due diligence reviews, or reviews of transaction monitoring alerts.

We would consider such delays reasonable as long as:

- the firm does so on a risk basis (for example, reviews for high risk customers should not be delayed unless absolutely necessary)
- there is a clear plan to return to the business as usual review process as soon as reasonably possible

The challenges of detecting terrorist financing remain, and firms must not weaken their controls to detect such high-risk activity.

Where a firm is collecting information from an existing customer, Regulation 31 of the Money Laundering Regulations (MLRs) requires the account to be closed where the information is not provided. However, in the current situation, we expect firms to make reasonable efforts to collect this information or consider whether there are other ways of being reasonably satisfied with the customer's identity, before taking a decision to close the account.

Where firms need to amend their controls in response to the current circumstances, decisions should be clearly risk assessed, documented and go through appropriate governance.

We expect firms to notify us of any material issues that are impacting the effectiveness of their financial crime controls or causing significant delays to remediation plans.

Client identity verification – flexibility within existing requirements

Restrictions on non-essential travel have affected firms' abilities to use traditional methods to verify a customer's identity.

During this period, we expect firms to continue to comply with their obligations on client identity verification. The MLRs and Joint Money Laundering Steering Group guidance already provide for client identity verification to be carried out remotely and give indications of appropriate safeguards and additional checks which firms can use to assist with verification.

For example, firms can already use a combination of the following (where appropriate):

- accept scanned documentation sent by e-mail, preferably as a PDF
- seek third-party verification of identity to corroborate that provided by the client, e.g. from their lawyer or accountant
- ask clients to submit digital photos or videos for comparison with other forms of identification gathered as part of the onboarding process
- place reliance on due diligence carried out by others, such as the client's primary bank account provider, where appropriate agreements are in place to provide access to data
- use commercial providers who triangulate data sources to verify documentation provided
- use digital identity solutions to identify customers where a firm considers that the solution provides an appropriate level of assurance as to a person's identity
- gather and analyse additional data to triangulate the evidence provided by the client, such as geolocation, IP addresses, verifiable phone numbers
- verify phone numbers, emails and/or physical addresses by sending codes to the client's address to validate access to accounts, and
- seek additional verification once restrictions on movement are lifted for the relevant client group

The examples provided do not represent a relaxation of requirements, or suggest that taking one of the measures in isolation would be appropriate or sufficient verification. Any steps firms take to verify identity must be in line with their overall risk assessment, and the risk profile of the customer.

SM&CR

The FCA and PRA issued a joint statement [1] on arrangements for senior management in dual regulated firms, and we have also published a statement [2] for solo-regulated firms. These statements said that individuals performing required functions (including the Money Laundering Reporting Officer (SMF17)) should only be furloughed as a last resort.

UK Coronavirus Business Interruption Loan Scheme (CBILS) and the Bounce Back Loan Scheme (BBLS)

We have set out our approach to the application of Customer Due Diligence (CDD) measures [3] where businesses apply under the UK Coronavirus Business Interruption Loan Scheme (CBILS) and the Bounce Back Loan Scheme (BBLS).

Changes to regulatory reporting

We have introduced some temporary measures for firms submitting regulatory returns. Please refer to this statement [4] for further detail.

Source URL: https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation
First published: 06/05/2020 | Last updated: 06/05/2020

Links

- [1] https://www.fca.org.uk/news/statements/joint-fca-pra-statement-smcr-coronavirus-covid-19
- [2] https://www.fca.org.uk/news/statements/smcr-coronavirus-our-expectations-solo-regulated-firms
- [3] https://www.fca.org.uk/news/statements/uk-coronavirus-business-interruption-loan-scheme-cbils-and-new-bounce-back-loan-scheme-bbl

- [4] https://www.fca.org.uk/firms/regulatory-reporting/changes-regulatory-reporting-during-covid-19
- [5] https://www.fca.org.uk/print/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation
- [7] https://www.fca.org.uk/firms/financial-crime
- [8] https://www.fca.org.uk/firms/financial-crime/bribery-corruption
- [9] https://www.fca.org.uk/firms/financial-crime/cryptoassets-aml-ctf-regime
- [10] https://www.fca.org.uk/firms/financial-crime/data-security
- [11] https://www.fca.org.uk/firms/financial-crime/fraud
- [12] https://www.fca.org.uk/firms/financial-crime/money-laundering-regulations
- [13] https://www.fca.org.uk/firms/financial-crime/payment-service-providers-repeatedly-fail-provide-information
- [14] https://www.fca.org.uk/firms/financial-crime/financial-sanctions
- [15] https://www.fca.org.uk/firms/financial-crime/financial-crime-systems-controls-during-coronavirus-situation
- [16] https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing
- [17] https://www.fca.org.uk/firms/money-laundering/derisking-managing-risk
- [18] https://www.fca.org.uk/firms/money-laundering-terrorist-financing/registration
- [19] https://www.fca.org.uk/firms/money-laundering-terrorist-financing/high-risk-customers-politically-exposed-persons
- [20] https://www.fca.org.uk/firms/money-laundering/safe-custody-services