GIBSON DUNN

May 11, 2020

COVID-19: UK FINANCIAL CONDUCT AUTHORITY EXPECTATIONS ON FINANCIAL CRIME AND INFORMATION SECURITY

To Our Clients and Friends:

The UK Financial Conduct Authority ("**FCA**") has issued statements to financial services firms outlining its expectations on: (i) financial crime systems and controls; and (ii) information security, during the COVID-19 pandemic. These are further examples of the FCA requiring firms to take steps to prevent and/or limit harm to consumers and the market more generally in this challenging period. This client alert summaries these two statements and the steps that financial services firms should be taking to ensure continued compliance with their regulatory obligations.

Financial crime systems and controls

In its statement to firms, the FCA noted that criminals are already taking advantage of the COVID-19 pandemic to conduct fraud and exploitation scams through a variety of methods (including cyber-enabled fraud). The FCA flagged the importance of firms remaining vigilant to new types of fraud and amending their control environment where necessary to respond to new threats (including ensuring the timely reporting of suspicious activity reports).

Risk appetite

Firms should not address any current operational issues faced during the COVID-19 crisis 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.

Flexibility relating to ongoing customer due diligence reviews

The FCA does, however, acknowledge that firms may need to prioritise or reasonably delay some activities, whilst still operating within the anti-money laundering legislative framework. For example, this may involve, in some cases, delaying ongoing customer due diligence ("**CDD**") reviews. This is subject to two important caveats:

- when there are delays, the firm has accepted these on a "risk basis" (such as delaying CDD reviews of customers posing a lower risk); and

- a clear plan is in place to return to the "business as usual" review process as soon as possible.

The FCA specifically flags that challenges of detecting terrorist financing still exist and firms must not, therefore, weaken their controls to detect such high-risk activity.

Decisions to amend controls to take account of the current circumstances should be clearly risk-assessed, documented and go through the appropriate governance process.

Client identity verification

Firms are still expected to comply with their obligations under money laundering legislation relating to client identity verification. They are reminded, in light of current travel restrictions, that such legislation, together with the Joint Money Laundering Steering Group guidance, allows for client identity verification to be carried out remotely. They also give indications of certain safeguards and additional checks which can help with verification. For example, firms can ask clients to submit digital photos or videos for comparison with other forms of identification gathered as part of the onboarding process

The FCA is, however, keen to point out that this does not constitute flexibility of the requirements – this is something already provided for under the anti-money laundering legislative framework and associated guidance.

Information security

Linked to the FCA's concerns prompting the above statement on financial crime, the FCA has also issued a statement with respect to firms' information security.

Changes to the "threat landscape"

The unprecedented circumstances caused by coronavirus have required firms to change their ways of working at some speed and have changed the threat landscape faced by many financial services firms. As more people are working from home, online systems are becoming increasingly mission-critical and cyber criminals are taking advantage of the situation for their own gain.

Managing the increased risk

Firms are expected to prioritise information security and ensure that adequate controls are in place to manage cyber threats and respond to major incidents. This may include implementing enhanced monitoring to protect end points, information and firm critical processes (including, but not limited to, video conferencing software).

Firms should "*proactively manage the increased risks*". Amongst other things, they should be:

- vigilant to the potential increase in security breaches or cyber-attacks;
- ensuring that they continue to have appropriate governance and oversight arrangements in place; and
- ensuring that necessary regulatory notifications are made.

Ongoing areas of regulatory focus

Information security and financial crime are two areas on which the FCA has focused for some time prior to the COVID-19 pandemic. For example, there is an ongoing FCA consultation on operational resilience (published in December 2019), under which cyber security is a key theme.

Further, there are no indications of the FCA's interests in these area waning. For example, the FCA Business Plan 2020/2021 provides that the FCA will start to implement changes to how it reduces financial crime. These include making greater use of data to identify firms or areas that are potentially vulnerable. It warns that it will continue to take enforcement action where it uncovers serious misconduct, particularly where there is a high risk of money laundering.

Gibson Dunn's lawyers are available to assist with any questions you may have regarding developments related to the COVID-19 outbreak. For additional information, please contact your usual contacts or any member of the Firm's Coronavirus (COVID-19) Response Team, or the following authors:

Authors: *Michelle Kirschner, Martin Coombes and Chris Hickey*