ISLE OF MAN
FINANCIAL SERVICES AUTHORITY
Lught-Reill Shirveishyn Argidoil Ellan Vannin

BY EMAIL ONLY

Contact: Mr Andrew Kermode / Mr Marc Barlow
Ref: FSA/Dear CEO/Banks
Date: 13 July 2022

Dear CEO

Please act: ensure that you have appropriate and effective financial crime systems and controls in relation to account warnings and blocks.

Introduction

This letter is issued by the Isle of Man Financial Services Authority ("FSA") following consultation with, and input from, the Isle of Man Financial Intelligence Unit ("FIU"). It is intended to assist banks to fulfil their regulatory obligations. As it contains a number of related issues that are within the scope of the Proceeds of Crime Act 2008 ("POCA") and/or the remit of the FIU, please also refer to the FIU's '*Guidance for Making SARs and Other Disclosures*'[1].

When it comes to reporting suspicions of money laundering via Suspicious Activity Reports ("SAR") to the FIU, banks generally follow a similar process. However, the FSA, liaising with the FIU, has noted some deviation in how different banks handle the blocking of customer bank accounts, and the effectiveness of the systems and controls that are in place.

We therefore consider it is helpful to inform and remind banks, given their unique role in financial services, of observed examples of effective control frameworks, good practice and other key considerations.

[1] https://www.fiu.im/news/guidance-for-making-sars-and-other-disclosures-to-the-fiu/

The information contained in this "Dear CEO" letter may also be of relevance to other firms operating in the Isle of Man that are subject to the Island's AML/CFT framework.

Account Blocking

Banks may find it necessary to apply a block, lock or warning on an account for a variety of different reasons, some of which may relate to financial crime considerations.

Accounts do not need to be automatically blocked when suspicious activity is detected, however failure to do so may result in the relevant person (i.e. the bank) committing an offence under POCA or not being able to avail themselves of a defence against money laundering by seeking consent. Further information about consent and Court Orders is contained below.

The FSA, in consultation with the FIU, has observed a number of different approaches being taken by banks, ranging from 'hard' account blocks that prevent any transactions taking place without the block being removed by an appropriately authorised individual(s), through to warning messages that rely on a member of staff to take some appropriate action.

The most appropriate approach will depend on the specific circumstances, banks' risk appetites and the policies and procedures that are in place. Banks are encouraged to continue to take a risk-based approach to ensure that they:-

"Establish and maintain appropriate internal and operational controls, systems, policies and procedures relating to all aspects of its business to ensure appropriate safeguards to prevent and detect any abuse of the licenceholder's services for money laundering, financial crime, the financing of terrorism, or the proliferation of weapons of mass destruction"[2].

Consent

The FSA has observed a number of different approaches, with some banks taking a risk-based approach and choosing not to seek consent for transactions, others seeking consent concerning all individual transactions above certain thresholds, and others seeking consent for the minimum £250 threshold to be increased to an amount that represents a specified series of transactions.

Consent requests must be submitted via Themis to the FIU and in accordance with the Proceeds of Crime (Prescribed Disclosures) Order 2015. Until consent is received (or the

[2] Rule 8.3(2)(f) Financial Services Rule Book 2016

relevant period under POCA has expired without notice from the FIU that consent is refused) it is in the requesting bank's interests to ensure that appropriate systems and controls are in place to guard against transactions taking place in relation to relevant accounts. If such transactions do occur, they may amount to money laundering offences to which (in the absence of consent or expiry of the relevant period) the bank will not have a defence under Part 3 of POCA.

Where banks look to make use of the consent regime, the FSA has typically observed that the banks use account warnings instead of hard account blocks to try to prevent transactions taking place prior to the bank obtaining the appropriate consent (or until expiry of the relevant period) from the FIU.

It is for each bank to decide on its approach to obtaining consent(s); however, where a bank has documented that this is part of its processes and procedures, the FSA has an expectation that the systems and controls must be adequate and effective to prevent funds being paid away until the consent has been issued (or until expiry of the relevant period).

Court Orders

Receipt of a Court Order made under POCA, or a request under section 18 of the Financial Intelligence Unit Act 2016, should be a 'red flag'. It may immediately give rise to suspicion under POCA and/or trigger a review by the bank of the relevant client's activities.

In addition, a Court Order (for example a restraint order made under POCA) may impose restrictions, effectively 'freezing' assets and restraining persons (usually their owner/controller **and** the bank holding the assets) from dealing with them in any way. Failure to observe these restrictions (whether intentionally, or in error due to ineffective systems and controls) can also amount to a criminal offence, and / or result in the FSA commencing an enforcement investigation.

It should be noted that transactions such as payment of restrained funds to suspense accounts, or the closure of accounts with nil balances even if consent has been provided to pay funds away, could amount to a breach of the restrictions imposed by a Court Order.

It is therefore important that banks have an appropriate level of systems and controls in place to reflect the specific risks associated with Court Orders.

If you have any concerns or queries in relation to Court Orders, you should seek legal advice.

Tipping Off / Exiting Client Relationships

The POCA offence of 'tipping off' occurs when a person in the regulated sector divulges that a disclosure has been made to the FIU, or that a money laundering investigation is underway. This may be particularly relevant when banks are considering whether to terminate an existing client relationship.

Consideration of existing restrictions (whether imposed by Court Order or under the consent regime) should be part of the process for exiting client relationships.

The FSA has observed examples where banks have decided to exit relationships once they have raised a SAR. Whilst this approach may be appropriate in some circumstances, banks are reminded that they should not look to restrict business relationships with customers to avoid, rather than manage, ML/FT risk in line with the risk based approach. As per the AML/CFT Handbook July 2021, it is important to note that in doing so *"it can introduce further ML/FT risk and opacity into the financial system. Terminating business relationships potentially forces entities and persons underground which creates financial exclusion and reduces transparency meaning transactions are less traceable consequently increasing ML/FT risks"*.

If banks choose to exit a relationship they should consider their policy regarding obtaining the prior consent of the FIU. Extra care should be taken where Compliance staff / MLROs have taken the decision to exit a relationship to ensure that any account warnings or blocks are still considered and that the appropriate referral/sign off is still obtained prior to a transaction taking place.

No Longer Having a Suspicion (Negated Suspicion)

As part of a bank's ongoing investigations it is possible that additional information is supplied or discovered after a SAR has been raised that results in the bank no longer having knowledge or suspicion of money laundering.

In such cases a further disclosure should be submitted to the FIU (via Themis) setting out the new information, and why it has resulted in there no longer being suspicion of money laundering. This should be submitted under the original Themis submission reference, via the "further information" tab.

Other Considerations

Banks may additionally wish to consider some of the following when considering the use of account blocks or warnings:

- Are your systems and controls designed to effectively manage accounts that are blocked? This includes potential 'internal' (e.g. intra group or to suspense accounts) as well as external payments/transfers, and accounts that have nil balances that may still be subject to a Restraint Order.
- Do you have an overreliance on manual processes/warnings versus technology-based solutions?
- Do you have fully documented policies and procedures that are fit for purpose?
- Do you have appropriate and effective detective controls in place should any preventative controls fail?
- Are front line staff trained on the importance of blocks/warnings and to avoid the risk of tipping off customers that a money laundering investigation is taking place?
- Are compliance / risk teams adequately resourced to provide the appropriate level of oversight and challenge?

When Things Go Wrong

As part of maintaining an open and honest relationship with the FSA, banks are reminded to engage in a timely manner regarding any matters that should be notified under the Rule Book.

When things go wrong the FSA has a number of tools available in the event that the bank or the FSA identifies any regulatory failings. This includes the use of discretionary civil penalties and other enforcement action should the FSA deem it proportionate, reasonable and appropriate, which may be undertaken in parallel with remediation.

What You Need To Do

Banks are not expected to respond to this letter. However, you and your senior management should carefully consider its contents and take the necessary steps to gain assurance that your bank's financial crime systems and controls in relation to account warnings and blocks are commensurate with the risk profile of your bank. They should also meet the requirements of any appropriate legislation or regulatory guidance, including but not limited to POCA, the AML/CFT Code 2019, the AML CFT Handbook 2021 and the FIU's '*Guidance for making SARs (and Other Disclosures) to the FIU*'.

Please be advised that in future engagement with your bank the FSA may ask you to demonstrate the steps you have taken. If the FSA assesses banks' actions in response to this letter to be inadequate, it may consider appropriate regulatory intervention, which may include the use of enforcement powers.

If you have any questions regarding the content of this letter, please contact your usual bank supervisor or myself.

Yours faithfully

Andrew Kermode
Head of Banking, Funds & Investments Division

Anti-Terrorism and Crime Act 2003

Please note that this letter does not cover the Anti-Terrorism and Crime Act 2003 (ATCA). For general guidance in relation to ATCA, please refer to the FIU's 'Guidance for Making SARs and Other Disclosures'. If you have any terrorism financing related concerns regarding any specific clients or transactions, please contact the FIU immediately.