THE TA FORUM
AML Working Group

The TA Forum AML Working Group undertook a review of the Fraud Alert schemes available to firms in our industry. These schemes are a central alert process providing information on fraudulent transactions that may impact a number of our members. The working group considered creating a new scheme for TA Forum members however, after engaging with the Investment Association (IA), we are pleased to support the existing IA scheme that has been running for a number of years.

The IA scheme allows for the Asset Managers and their appointed Transfer Agents to provide and receive information on instances of fraud where the customer may be a customer of other firms, together with understanding the details of how the fraud was discovered. The AML Working Group believes this information can be a vital aid in protecting the victim together with sharing typologies to assist in the understanding of the fraud. Fraud is becoming ever more sophisticated as the criminal develops new ways to commit financial crime and it is imperative, we are as proactive as we can be to address such risks.

The IA revised the Scheme Rules in 2018, such rules and the application process can be located below and referenced in Appendix 1.

If any member of the TA Forum AML Working Group wishes to alert members of a fraud, these should be notified to the IA by completing the Fraud Alert notification as shown in Appendix 2.

Data Protection and information sharing considerations:

Various legislation is available that we can consider when issuing personal data relating to financial crime. Under the Data Protection Act 2018, Schedule 2 Part 1.2(1)(a)[1], there is a listed GDPR provision to reference where needed.

In addition to the foregoing, under the Criminal Finances Act 2017, the sharing of information within the regulated sector under s339ZB-339ZG[2] provides guidance on when and where we may feel it necessary to issue further data to assist in money laundering or, terrorist financing.

[1] https://www.legislation.gov.uk/ukpga/2018/12/schedule/2/enacted

[2] https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/679032/HO_Circular-_Sharing_of_information_within_the_regulated_sector_1.0.pdf

THE TA FORUM
AML Working Group

IA FRAUD ALERT SCHEME RULES

(Version 3.1 – June 2018)

Scope and purpose

1. The purpose of the IA Fraud Alert Scheme ("the Scheme") is to provide information to participating IA members relating to frauds (actual or attempted) that might affect multiple firms - a typical example would be applications to purchase fund units using false or stolen debit card details.

2. Details of the alert procedure may be found in paragraphs 18 - 22 below.

3. It is not intended that the Scheme should be used to distribute information relating to frauds that are clearly isolated to a single firm (e.g. frauds by a member of staff), nor is the Scheme intended to be used in cases where there is little other firms can do with the information (e.g. postal cheque interception). Instead, firms are encouraged to share their experience of such cases through the regular IA Financial Crime Discussion Group.

4. While the Scheme is not intended to be used in cases where there is little other firms can do with the information, where there is information that other firms could act on, this should be shared. For instance, details of a client who is being attacked by fraudsters, as they may be a client of other firms. Especially useful may be details of how the fraud was identified.

Participation

5. Participation is voluntary but is restricted to full IA members plus affiliates that are fund supermarkets. Whilst all full members are able to participate, the Scheme is likely to be of most interest to retail product providers.

6. Third party administrators are able to submit alerts to the Scheme where they are acting on behalf of their client management companies who are members of the Scheme.

7. Registration to participate must come from the firm's Money Laundering Reporting Officer (MLRO) who is approved by the FCA to fulfil Senior Management Function 17, using the form in Appendix 1.

8. The MLRO may permit others within their own organisation and/or their third-party administrator (where appropriate) to issue alerts on their behalf. However, they may nominate only one person (including themselves) to receive alerts.

9. The MLRO is able to nominate a group email address (e.g. Fraud.Alert@XYZ.com) to receive alerts. As the alerts are always sent with a formulaic subject line (see paragraph 19) it is possible to set up auto-forwards, should the normal recipient be unavailable.

10. Exceptionally, where the firm employs a third-party administrator (TPA), the MLRO may wish to agree with the TPA that they should receive alerts on the firm's behalf; in such instances, this may be in addition to someone at the firm. TPAs are not, however, eligible to participate in the Scheme in their own right. TPAs so nominated must be an IA affiliate member.

11. Whoever may be permitted or nominated to issue/receive alerts, the participating firm's MLRO will remain responsible for the proper use or disclosure of any facts or personal information.

Relevant information, data protection and tipping off

12. The information circulated in relation to an alert will vary according to the circumstances but, needs to be sufficient for other firms to identify potentially related activity. It is recommended that details include all relevant names, address and other details (e.g. bank/card), as well as a description of the circumstances. TPAs who submit alerts on behalf of their client firms should identify the firm(s) concerned.

13. The IA does not provide a central repository for this information - it is for member firms to retain any information as appropriate for their own needs. Requests for further details or clarification should be directed to the originator of the alert.

14. Professional advice received by the IA is that the proper use of personal data for the purposes of the Scheme is exempt from the "non-disclosure provisions" of the Data Protection Act 2018, by virtue of Schedule 2 Part 1.2 of the Act. Although it is not a legal requirement, the following statement should be included in all alerts by the submitting firm:

    "***This message is circulated solely for the attention of IA members and those carrying out relevant functions on their behalf. The information is provided under the provisions of Schedule 2 Part 1.2 (Crime and taxation: general) of the Data Protection Act 2018 (i.e. it is personal data that is exempted from the non-disclosure provisions of the Act). Its content should only be used for the prevention and detection of crime and the apprehension or prosecution of offenders."***

15. Information should be submitted for circulation only where there are good reasons to suspect that the activity concerned is fraudulent. As such, the firm involved will have good reasons to believe that the activity is fraudulent; mere suspicion would not be enough. Firms should consider reporting the matter to National Fraud Intelligence Bureau/Action Fraud, or to the police and, if so, may wish to discuss with them whether or not circulating an alert to the Scheme is likely to prejudice an enquiry.

16. The IA will, on receipt of an alert, take a view as to whether it is appropriate to forward it on, e.g. via Association of Payment and Clearing Services (APACS) and the Dedicated Cheque and Plastic Crime Unit (DCPCU) system, to the fraud expert of the relevant bank. Appropriate alerts would be those containing details of bank accounts that were being used for fraudulent purposes. The permission of the originator is required for the IA to do this.

Procedure

17. The originating firm should send an e-mail containing the completed IA Fraud Alert template (see Appendix 2) and the Schedule 2 Part 1.2 caveat (see paragraph 14 above) to fraud.alert@theia.org

18. The IA will add a unique reference (e.g. "IA Fraud Alert 20/0001") to the subject line of the e-mail, and top right-hand-side of the template and forward it to all those nominated to receive alerts at participating firms. Inclusion of the originator in the distribution of the alert will provide them with acknowledgement of their submission.

19. The e-mail addresses of all recipients of the forwarded e-mail will be visible, so that firms will be able to see who has received an alert. Recipients may wish to forward the e-mails automatically to someone else (e.g. during their temporary absence), which they should be able to do by reference to the standard text that will be included in the subject line.

20. If a firm, having received an alert, wishes to seek further information or clarification, they should contact the originating firm direct, not the IA.

21. If a firm wishes to add information to a previous alert, they should reply to the IA, using the original alert, with the new information for circulation. They should not 'reply all'. If the firm is not sure whether the information relates to a previous alert, a new alert should be submitted

THE TA FORUM
AML Working Group

Appendix 1

To: Investment Association
From: [Insert name of MLRO]

being the Money Laundering Reporting Officer and person approved by the Financial Conduct Authority to fulfil the SMF17 controlled function for:

[Insert name of firm] ("the Firm")

APPLICATION TO PARTICIPATE IN THE IA FRAUD ALERT SCHEME

Please register the person(s)* named below as authorised to receive fraud alerts on behalf of the Firm.

I understand that the Scheme operates as described in the "IA Fraud Alert Scheme Rules" and give the following undertakings:

1. that the Firm will participate in the Scheme by initiating alerts in relation to any fraud activity it detects that contains new information, that may reasonably be assumed might also impact on other IA members, subject to any request for secrecy by law enforcement or other authorities;

2. to ensure that any personal data and other information disclosed by the Firm or its administrators in the course of its participation in the Scheme will be that which is appropriate for the purposes of enabling other IA members to detect and prevent fraud that may be attempted against them, having regard for the provisions of the Data Protection Act 2018;

3. that the Firm will co-operate with any reasonable request for further information from another firm that believes it may have been similarly targeted, to the extent that such information is available and the Firm is not restrained by any requirement (e.g. from law enforcement) to maintain secrecy;

4. to ensure that I, and anyone who may from time to time be nominated by me to receive alerts from other firms via the IA Fraud Alert Scheme, will exercise all due diligence in the handling, including onward communication, of any personal data and other information that may be provided, having regard for the provisions of the Data Protection Act 2018 and the potential for tipping off under UK anti-money laundering legislation;

5. to notify the IA without delay of any changes to the contact details provided below of the person nominated to receive alerts:

	At the firm	**At [insert name of TPA*]**
Contact name:		
E-mail:		
Telephone:		

Signature: **Name:** **Date:**

Firm:

* A second contact will be accepted only where the Firm's client administration functions are outsourced to a third-party administrator, and that TPA is an IA affiliate member

THE TA FORUM
AML Working Group

Appendix 2

IA FRAUD ALERT

Reference	IA USE
Date	ONLY

This alert is circulated solely for the attention of IA members and those carrying out relevant functions on their behalf. The information is provided under the provisions of Schedule 2 Part 1.2(1)(a) of the Data Protection Act 2018 (i.e. it is personal data that is exempted from the non-disclosure provisions of the Act). Its content should only be used for the prevention and detection of crime and the apprehension and prosecution of offenders.

Type of fraud:		For account takeover fraud, the victim is…:	
Victim name(s)			**Optional but encouraged - complete only where this intelligence will be relevant to other firms.**
Victim address (from firm's records)			
	Postcode:		
Subject name(s):			**Enter the name(s) (where appropriate) and/or address provided by fraudster. Do not enter the victim's details here. Include phone numbers, email etc. if provided by the fraudster.**
Subject address (only include if different to above):			
	Postcode:		
Bank/branch name:			
Sort Code (or BIC):			**Enter any details provided/ obtained re account take-over or from cheque or card used for subscription (i.e. details from fraudster, not of victim).**
Account Number (or IBAN):			
Card Number:			
Details of incident (method of attack, cause of suspicion etc.)			
Contact Name:			
Position:			
Firm:			
Telephone:			
E-Mail:			
I consent to details of the alert being submitted to the DCPCU			☐Please tick box