National Strategic Assessment 2021

Money Laundering Chapter Collection Questionnaire

- Please provide responses to the questions below, based on your perspective of the threat area.

- The collection period for the 2021 NSA is January–December 2020. If you have information outside of this period which you believe is relevant please mark this accordingly.

- Responses should be returned to charlotte.grace@nca.gov.uk and helen.morgan@nca.gov.uk by **30th October 2020**.

1.	**How has the money laundering threat changed since the last NSA?** Please detail where possible: • Changes in or new/emerging methodologies • The drivers and enablers of these changes • Any changes in key nationalities and jurisdictions of risk • If you have not seen a change in the threat please provide any reasons why.
	Cryptocurrency: One trend that is emerging in EMA member firms is that the transaction monitoring associated with cryptocurrency transactions and accounts is improving through the intervention of more efficient investigative tools and services. We feel improvements in this area and the ability to blacklist suspicious accounts has served to reduce risk of money laundering through cryptocurrency as identified in the last NSA. Improvements in this area are being driven by greater familiarity and understanding of the cryptocurrency landscape and improved technical developments in the tracking and identification of transactions. **Fraud as predicate offence – money laundering:** EMA member firms see money laundering associated to fraud scams as very common typology where successful fraudsters launder the proceeds of their own scams through the E-Money sector. The underlying frauds in these cases often involve an element of social engineering through social media and online dating sites to recruit victims. The firms are picking up these cases through velocity rules in transaction monitoring systems generally and where they do they seek clarification on source of funds for the transaction are told it is unknown as the customer is helping a friend. The EMA feels more could be done by the NCA and the government to improve training and awareness of such scams – particularly with older people vulnerable. The EMA feels that the enablers of such scams are the social media sites where victims are recruited and the drivers are the fact that potentially controls around

authentication in the payment transaction have improved and thus scammers need to have the customer make the transaction and therefor dupe them using social engineering.

COVID-19:

Covid-19 is a driving factor in the current UK landscape and its advent has seen exponential growth in transaction volumes for online purchases of goods. Greater use of online market places inevitably leads to greater exposure to fraud for consumers especially those who are less tech savvy.

As previously stated, the use of social engineering in all fraud types is on the increase and is used by criminals to lauder the proceeds of crime and also commit fraud.

The common types of underlying scams noted by EMA members are often targeted at less tech savvy victims –traditional scams where the victim is offered a fake prize or reward and then is duped to give personal details and pay a fee to receive the gift.

Another prevalent typology under Covid-19 is the sale of goods online not being supplied or delivered after payment. Again, given the increase is online transactions an increase in this type of scam is inevitable and this acts as driver and enabler.

2.	**What has been the impact of that change?** • Has this reduced, increased or displaced the threat? • How has this impacted the overall threat level?
	   In overall terms the money laundering threat for traditional cash-based systems has not increased according to our members. Most firms in the payments sector have very strict controls around the use of cash and how it can be loaded onto cards and wallets. This serves to mitigate significantly the threat of cash-based money laundering. However as previously stated the threat of money-laundering linked to funds from fraud as the predicate offence has increased. The drivers and enablers of these types of fraud and associated money-laundering are the online market places themselves who could potentially do more to investigate and block fraudulent merchants.
3.	**How is the threat likely to develop over the next 3 years?** • Please indicate any key drivers of this change.
	Will any threats identified increase or decrease?

	Given the greater use of the internet by consumers and greater numbers of online transactions the EMA believes it is likely that this threat will continue to increase over the next three years.
	However, there is likely to be some mitigation possible as those less tech savvy consumers who often become victim may learn from their experiences and also with a campaign to increase public awareness of such scams being rolled it would also likely have a beneficial impact.
4.	**Are you able to provide or signpost to any data that can be used to articulate;** a) **The scale of the threat;** b) **The threat trajectory (ideally from January–December 2020).**
	We do not have any data to support the trends and themes we have identified in this report.
5.	**The OFFICIAL NSA includes a section on what the public can do to protect themselves from being a victim of money laundering (previous focus on money mules).** **What area(s) do you think the section should focus on this year and what should be the key public message(s)?**
	The EMA feels that warning the public around fraudulent scams particularly where social engineering is used to encourage them to be the victim of fraud and/or use their account to assist criminals to launder the proceeds of crime is an emerging threat. The best mitigation of such threats is a widespread advertising campaign to warn consumers against these risks using mainstream media sources and public adverts. Given many of the victims are vulnerable greater focus on targeting these consumer groups to help protect them would be beneficial using methods that will have the greatest impact in terms of advertising and education.
6.	**Please provide any other information that you believe would be useful for this year's NSA Money Laundering chapter (optional).**
	Not applicable.