Written evidence submitted by the Financial Conduct Authority

RE: Economic Impact of Coronavirus: Reducing the risk of fraud

''What are the financial regulators and the financial sector doing to reduce the risk of people being taken advantage of by fraud at this time, in particular with regard to vulnerable groups?''

The FCA's remit in relation to fraud

Protecting consumers is at the heart of what we do as a regulator. The Financial Conduct Authority (FCA), as the conduct regulator and money laundering supervisor for the financial sector, has a keen interest in reducing frauds being committed, especially those that may be facilitated by firms we regulate, use the appearance of FCA authorisation to deceive victims or otherwise occur within the financial system.

Our general approach recognises not all frauds can be stopped before they happen, we are not able to restore all victims to the position they were in beforehand and most frauds and scams operate outside the FCA's formal regulatory jurisdiction. For these reasons, the FCA devotes considerable efforts to the prevention of fraud by requiring regulated firms to maintain high standards of conduct and diligence to ensure they do not facilitate fraud (either by permitting their systems to be used by fraudsters, by laundering proceeds of crime or otherwise) and by providing consumers with information about how to identify fraudsters through our successful Scamsmart campaigns.

In addition to prevention, we also pursue fraudsters, especially those who operate on the perimeter of our jurisdiction, either conducting regulated activities without our permission (which often involves fraud) or those who make unrealistic 'too good to be true' promises to consumers. We also maintain a robust approach to market abuse which the courts view as a species of fraud.

Given the incidence of fraud goes beyond the formal reach of our jurisdiction, we also work closely with other agencies. The FCA is a member of the National Economic Crime Centre (NECC), which has a broad coordinating role across UK agencies. We have provided resources to the NECC through a secondment programme and work closely with fellow members, the National Crime Agency (NCA), Serious Fraud Office (SFO), City of London Police and HM Revenue and Customs (HMRC). The problem of fraud, especially volume fraud, is a complex one, spanning responsibilities across UK law enforcement, which is why the FCA is a keen supporter of the establishment of the NECC.

With those general observations in mind, I want to turn to some of the specifics of our prevention and pursuit programmes.

Prevention: Our expectations regarding financial services firms

Under our rules, regulated firms are required to establish and maintain systems and controls to counter the risks that they may be used for financial crime. We supervise firms in respect of these obligations, act when these requirements are not met and issue guidance to assist firms about tackling financial crime and protecting consumers from frauds and scams.

For example, we have recently advised firms that Covid-19 and the current public health measures are likely to make consumers more vulnerable to scams and we are working closely with banks and building societies to ensure they have additional measures in place to help vulnerable consumers make payments safely during the crisis. Banks and building societies are proactively contacting their vulnerable customers to give them clear information on how they can make payments through trusted people. This is particularly important for consumers who

are self-isolating and rely heavily on in-person payments.

This builds on a number of recent reforms designed to tackle Authorised Push Payment (APP) frauds (when a fraudster tricks a payer into making a payment to an account controlled by the fraudster):

- To help prevent APP fraud, the industry has developed the Contingent Reimbursement Model Code: https://www.lendingstandardsboard.org.uk/contingent-reimbursement-model-code/. This Code covers 9 UK banking groups and 85 per cent of UK personal current accounts. It sets out the standards expected from firms to control fraud, the circumstances in which they must reimburse customers, and best practice for firms to follow when investigating APP fraud. The best practice standards also protect consumers through complaint handling procedures and ensuring access to resolution through the Financial Ombudsman Service if necessary.

- A further safeguard against APP fraud is Confirmation of Payee (CoP). This is the account name-checking service, which the Payment Systems Regulator has directed 6 of the UK's largest banking groups to implement by 30 June 2020. CoP checks that the name of the account that a payer is sending money to matches their payment instructions. Anybody setting up a payment will be alerted if the name on the recipient account does not match, meaning it can be stopped or corrected before the payment is made. CoP is designed to cover at least 90 per cent of UK payment transfers made by Faster Payments or CHAPS.

- In May this year, we published guidance for firms on our rules and principles relevant to countering financial crime risks. It sets out examples of good and bad practice in preventing fraud.[1]

More generally, our Principles for Businesses require all the firms we regulate to treat their customers fairly and we expect firms to exercise particular care with consumers in vulnerable circumstances.

Building on our Principles, in July 2019, we issued a first consultation on draft guidance on the fair treatment of vulnerable customers. The draft guidance sets out our proposals for how firms should approach the treatment of vulnerable customers, embedding this in their culture, practices and processes throughout the whole consumer journey, from product design to customer service. This includes consumers whose characteristics or circumstances mean they are especially vulnerable to scams. Due to the wider demands of the Covid-19 pandemic we delayed publication of the detailed final Guidance Consultation planned for Q1 2020. However, we continue to make clear to firms that preventing harm to vulnerable consumers is even more important than ever at this challenging time.

Similarly, on 14 March 2020, we introduced rules for banks to implement Strong Customer Authentication (SCA) for e-commerce. While we have given the industry an additional 6 months to implement these measures (the revised date is 14 September 2021), these rules require banks to obtain identification for customers accessing online banking through at least two different categories, e.g. through something the customer knows (such as a password), something the customer has (such as a mobile phone), and something inherent to the customer (such as a fingerprint). The deadline for implementation has been extended to avoid significant disruption for consumers who are likely to be more heavily reliant on e-commerce at this time. However, this is only if the firm sufficiently mitigates the risk of unauthorised transactions and fraud by having the necessary fraud monitoring tools and systems in place and taking swift action where appropriate.

[1] https://www.handbook.fca.org.uk/handbook/FCG.pdf

We are also talking to credit card firms about the interaction of their anti-fraud arrangements and the purchase of essential goods.

Prevention: Protecting retirement income

Given the difficult choices faced by consumers, it is as critical now as ever that consumers have access to appropriate pension products; they are supported to make well-informed retirement income decisions and have information and appropriate warnings to avoid frauds and scams when considering transferring their pension.

We recognised the potential risks here at the outset of the Covid-19 crisis and issued a joint statement with The Pensions Regulator and The Money and Pensions Service to highlight the risk of fraud at this time and to signpost the support available to individuals.[2]

We have issued guidance to firms to support them in having meaningful conversations with their customers about the risks and implications of actions they might be considering – for example, crystallising losses caused by the current market downturn. As always, providers should signpost the availability of free and impartial pensions guidance from Pension Wise and encourage consumers to seek advice from an FCA-authorised financial adviser.

Prevention: Scamsmart

The FCA also protects consumers through a broad range of consumer education initiatives designed to prevent consumers from being susceptible to scams. We do this by actively warning them about both specific scams and the general risks of falling victim to scams and frauds. These warnings are published on our website and we heavily market the existence of this site and its utility in our consumer campaigns.

Scamsmart is a broad, multi-year campaign to educate consumers about how to avoid becoming a victim of scams. It provides basic information, consumer tips and is supported by professional research that identifies particularly vulnerable groups or behaviours that fraudsters tend to exploit. Our campaign uses television, radio and press to market our messages and Scamsmart has its own pages on our website with access to all our data as well as our warning list of firms which we advise consumers to avoid. We regularly update our Scamsmart website and have launched 9 multi-media campaigns over the last 5 years in relation to investment scams focussing on retirees, pension transfers and other sources of harm for vulnerable groups.

We have stepped up our work in relation to the prevention of frauds and scams with warnings posted to our warning list increasing by 160% since last year.

We are currently planning additional Scamsmart campaigns to be launched in the next month. In addition, in our 2020/21 Business Plan we stated that we are particularly concerned at the moment about retail investments and the harm caused by fraudulent and high risk illiquid investments and this year we will prioritise helping consumers make better investment decisions. Through our Fees Consultation Paper, we are consulting on our proposal to undertake this campaign and the basis of recovering the 2020/21 costs of £2.3m from fee-payers.

In addition to Scamsmart, we also pay Google to flag warnings to consumers searching for investment opportunities through Google's search engine.

[2] https://www.thepensionsregulator.gov.uk/en/media-hub/press-releases/2020-press-releases/covid-19-savers-stay-calm-and-dont-rush-financial-decisions

Pursuit: Investigation and Prosecution

We have a dedicated function focused on detection, investigation and prosecution of fraudsters (our pursuit of offenders or pursuit function). This is focused primarily on the remit we have under the Financial Services & Markets Act 2000 (FSMA) and the Financial Services Act 2012. We pursue regulated or passported firms who commit misconduct, including regulated firms who may facilitate financial crime, such as those with poor anti-money laundering systems and controls); those who pretend to be regulated by the FCA (inducing victims on that basis); those who carry on regulated activities without our permission and those who use false or misleading statements to induce investors to invest in regulated investments.

The FCA has a broad range of powers which it uses including using the full range of our sanctioning powers to impose financial penalties, suspend and prohibit firms and individuals, seek injunctions and commence civil or criminal proceedings.

Most recently, for example, last week we acted to stop four Cypriot firms from selling contracts for difference using UK celebrities as a marketing tool. We allege those celebrities had not endorsed or otherwise associated themselves with the product, thus misleading consumers.

We have conducted many major criminal prosecutions in which significant jail terms have been imposed in which we have also secured compensation for victims and we have a healthy pipeline of cases under preparation now.

Given the limits of our jurisdiction, we also collaborate with other agencies to disrupt frauds and scams, providing intelligence, expert assistance and referring cases that are more appropriate for other agencies to pursue, including the NCA, SFO, City of London Police and HMRC.

Recent trends in frauds and scams

At the outset of the Covid-19 crisis we were concerned there might be an increase in frauds and scams and we issued alerts and joined with the NECC in its campaign.[3] Whilst there has been an uptick in general scams related to Covid-19 (including in areas like trading standards), those scams specifically related to financial services have remained relatively stable, although we have seen some specific Covid-19 variants.

We are also exchanging information with the NCA and the NECC on a weekly basis, and engaging with the Information Commissioners Office (ICO), the Insolvency Service and Trading Standards. On 26 March, we co-signed a joint statement with members of the NECC to highlight the types of fraud to be aware of and advice for individuals.[4] The FCA advises anyone who wishes to report frauds and scams to contact Action Fraud, which is the UK's national reporting centre for fraud and cyber-crime, and takes crime and information reports on behalf of the police.

As of 19 May, we had received 41 scam reports since the beginning of 1 February that directly reference coronavirus. Of these, 23 appear to be related to regulated financial services. In terms of overall numbers of scams, this is relatively low, but the possible reason is that fraudsters are seeking to exploit the public's fears caused by the pandemic, such as economic downturn, but are not referencing the pandemic directly in their communications. For instance, promotion of scams may place significant emphasis on a promised high rate of return. While not directly linked to coronavirus, such scams pray on concerns caused by low interest rates.

Over the last quarter, we have noticed the following trends:

[3] https://nationalcrimeagency.gov.uk/news/fraud-scams-covid19
[4] https://www.nationalcrimeagency.gov.uk/news/fraud-scams-covid19

- Clones: These are clones of authorised firms which market themselves through social media sites and often have an overseas source. The number of clone reports we receive continues to grow. Wealthy clients appear to be targeted in particular and some banks have found themselves targeted repeatedly by different clones. The sums involved can be substantial so we expect this type of scam to continue to appeal to scammers. We are working closely with the banks involved and are increasing our efforts to remind consumers to always check contact details against the FCA public register before transferring funds.
- Scams involving foreign exchange/contracts for difference/binary option trading: These scams target consumers using social media at the other end of the spectrum, usually younger, less wealthy individuals who are willing to take greater risks in order to make greater profits. We have seen evidence of these scams on Instagram, Facebook, Twitter and even dating sites, such as Tinder. Scammers will commonly approach consumers on these sites, but then invite them to engage with them directly on WhatsApp or Snapchat so that they can provide them with details about the investment. One notable feature of this kind of scam is the pervasive use of minor celebrities to promote the activities of the scammer. These celebrities may unwittingly promote a scam, but we are concerned with the potential breach of our financial promotion rules by those posting these videos.
- Cryptoasset scams: We have noticed an increasing number of websites offering a variety of investments or services involving cryptoassets or services. It has attracted scammers who pretend to offer legitimate opportunities in the crypto-market, which are either non-existent or offered at highly inflated prices. Social media is widely used to promote these opportunities and the use of professional looking websites and promises of high returns can prove to be an effective way to entice investors.
- Recovery rooms: This is where fraudsters approach investors who have been scammed or had failed investments, offering to help them get their money back for an upfront fee. The sums can be relatively small but the activity is high volume and the scammers therefore depend on targeting large volumes of those investors who may be particularly vulnerable as they have already experienced financial loss.
- Debt services: We continue to see firms offering debt services in a misleading way and charging substantial fees for their services even though those same services can be obtained for free (such as, for example, from the well-recognised charity StepChange). These firms may use ruthless marketing campaigns that can be misleading. For example, we see some who claim they are government backed or that they offer services for free but go on to make charges. Given the vulnerability of the consumers seeking these services, we are concerned by the growing number of firms inhabiting this space.

I hope this is helpful. I would of course be happy to discuss this further.

Christopher Woolard
Interim Chief Executive

June 2020