If you remain unsure, report your concern to a colleague in Compliance as soon as you can. When you make your report avoid jumping to conclusions - just explain what you have observed that worries you.

DO remember your financial crime awareness training! You have a duty to report *any* suspicions that someone might be using us or a customer's account for criminal purposes, via a Suspicious Activity Report. This is a simple process; you just need to send a short email to the MLRO's email address you have been given explaining the facts that you have seen that worry you. Again, avoid expressing any conclusions about what you think might be behind the facts you see. The Compliance team will make whatever investigations that need to be made. **But in the situation where you are worried about a vulnerable customer you should not delay in telling someone about your worries. Your promptness could make a huge difference in our ability to protect the customer.**

More Information

Office of the Public Guardian Safeguarding Team: https://www.gov.uk/report-concern-about-attorney-deputy

Action Fraud: https://www.actionfraud.police.uk/news

ABI Vulnerability Guide:

https://www.abi.org.uk/products-and-issues/lts-public/issues-in-long-term-savings/vulnerability-guide/

Citizens Advice Bureau https://www.citizensadvice.org.uk/

About TISA

TISA is a unique industry-wide membership organisation. Our mission is to bring the UK financial services savings industry together to promote collective engagement, to deliver solutions and to champion innovation for the benefit of citizens, our industry and the nation. www.tisa.uk.com

Disclaimer

The information is provided free and is current at December 2018, based on TISA's understanding of current law and guidance. Whilst every care has been taken to ensure the accuracy of this information TISA cannot accept any responsibility for any inconvenience, loss, damage, or liability nor for any legal fees and costs incurred or caused as a result of any information provided.

tisa
Leading on Investments and Savings

Vulnerable Customers and Financial Crime

Advice to front-line colleagues in financial services

Introduction

Criminals love the vulnerable because they are an easier target. All financial services firms have a duty to safeguard the vulnerable, and as a front-line (customer-facing) colleague you have a special role to play in ensuring that our customers are protected. *You* are the person who is most likely to see signs that a customer is being exploited, or scammed, or ripped-off, or simply robbed. It is important that you know what those signs are, and know what to do when you recognise them.

What do we mean by 'vulnerable'?

There isn't a typical 'vulnerable' person - and people who others see as vulnerable might not view themselves in that way! The FCA defines a vulnerable consumer as *"someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care".* There are many circumstances that might cause vulnerability, such as:

- The elderly (although just being an older person does not necessarily make one vulnerable);
- The young – particularly people with no experience of making financial decisions for themselves;
- Recent bereavement;
- Learning / decision-making difficulties;
- Poor reading skills, or dyslexia or dyscalculia;
- Mental health issues, either inherent or triggered by events such as relationship issues and/or divorce, job loss, family problems, etc;
- Debt / financial difficulties causing stress;
- Language difficulties – people with limited or no English;
- Physical health problems or disabilities.

These are just examples of situations you should be alert to. There will be others! But as a front-line colleague, whether you are meeting the customer face-to-face or talking to him or her on the phone, you might see warning signs of vulnerability such as:

Indicators that an individual may be in 'vulnerable circumstances'

The individual:

- Asking irrelevant and unrelated questions, or displaying signs of forgetfulness;
- Struggling to read or understand the information they are provided with, or asking for it to be continually repeated;
- Responding in an irrational way to straightforward questions;
- Saying 'yes' or 'no' in a way that suggests they haven't understood;
- Taking a long time or displaying difficulty in responding to simple questions or requests for information;
- Saying they do not understand or cannot use the technology;
- Repeating simple questions such as 'who are you?', 'what investment is it?' and 'what do you want?';
- Wandering off the subject at hand and making incongruous statements;
- Saying that they are not well or not in the mood to continue;
- Displaying signs of ill-health like breathlessness or making signs of exasperation or discontent;
- Giving a statement such as *'I don't usually do things like this, my husband/wife/son/daughter takes care of it for me'*
- Indicating in any way that they are feeling rushed, flustered, or experiencing a stressful situation;
- Having trouble remembering relevant information, for example that they are already a client or have recently made an investment.

Of course, just because someone is showing potential signs of vulnerability - or is indeed vulnerable - it does not necessarily mean that he or she is, or is going to become, the victim of crime. As a front-line colleague you are trained to recognise the obvious signs that a criminal might be trying to access a customer's account, such as callers who struggle to remember IDV responses, but there are more subtle warning signs to watch out for in connection with potentially vulnerable customers:

Indicators of potential criminal activity

- Any unusual increase in account activity, particularly when payment is being requested to a third party account and/or a Power of Attorney has recently been appointed;
- The customer asking to make a large withdrawal in cash;
- An instruction to make an unusually large payment or transfer;
- A large payment to a web-based investment business;
- The customer is accompanied by family, staff or others who appear to speak for, coax, or otherwise pressure, the customer into making decisions;
- When on the phone the customer appears to be prompted by another person;
- The customer complains about not having access to her/his own money;
- Calls are received on an account where the caller profile doesn't match, such as sounding too young or old, or with an accent that doesn't match the customer's profile;
- A series of cash withdrawals to the maximum daily limit;
- Account instructions being received via a third party with no PoA and only a weak level of third-party authorisation, such as a typed letter;
- Unconvincing signatures on cheques or third party authorisation letters;
- A family member or anyone else showing unusual interest in the assets of the customer, or asking for confidential information about the account (which obviously should not be given!);
- Attempts to 'blag' information about an account with a story, no matter how convincing, about why the customer cannot act for him or herself;
- The caller getting angry when he or she is asked to provide corroborative IDV information, or simply hanging up;
- Transactions that just seem odd and out of character, such as for example an elderly person with plenty of spare cash taking out a short-term loan for no obvious purpose, or sending a significant sum of money abroad.

What matters here is your commonsense. Don't just ignore something that worries you! You don't need to (and you should **not**) play the detective but there are some simple steps you can take to help make sure our customers don't fall victim to criminals:

What to do if you see something that worries you

- Don't be frightened of asking the customer if everything is alright? No genuine customer will normally resent being asked in a friendly way if there is anything worrying them;

- If the customer is asking for a large payment, transfer or cash withdrawal, ask them if they would mind sharing with you the purpose of the transaction? If they refuse you should obviously not pester the customer but the right tone of enquiry is unlikely to be resented. The key here is to avoid using phrases like *'Could you tell me / explain the purpose of the transaction?"* – that sounds too much like an interrogation. *"Would you mind sharing with me…"* or *"do you mind me asking…"* are softer approaches. Importantly, if you are face-to-face with the customer you should make sure your discussion is confidential and not capable of being overheard. If you can, invite the customer to a quiet area;

- If your concern relates to a situation in which you are being given instructions from the customer via a third party, do not be afraid to ask the third party for permission to contact the customer for verification of the instruction;

- Do bear in mind that if the customer is being manipulated by a criminal or unfairly coerced by a third party he or she might have been instructed to refuse to answer questions. Be alert to the customer saying something like *"I've been told not to tell you that"*.