



The UK's Fraud Prevention Service

# Best Practice Guide: Protecting the Vulnerable

[www.cifas.org.uk](http://www.cifas.org.uk)



# Contents

- What is this guide about? 1
- What should we consider? 2
- What makes us at risk? 2
- How do fraudsters select their targets? 3
  - 'Phishing' and 'Grooming' 3
  - 'Fronting' and 'Fooling' 3
  - Staff Fraud and Corruption 4
- What can be done to tackle these problems? 5
  - Know Your Customer 5
  - Know Your Staff 5
  - Customer-Staff Interaction 5
  - Lines of Communication 5
  - Taking Action Against Fraud 6



Best Practice Guides are produced by CIFAS for CIFAS Members on subjects related to fraud prevention, not just pertaining to CIFAS systems but also in associated areas. They are intended to inform Members - they are not mandatory instructions.

CIFAS is a not-for-profit organisation, concerned solely with the prevention of fraud and funded by subscription. CIFAS Members are drawn primarily from the UK financial services industry, but also from telecommunications, insurance and other business sectors and soon from the public sector.

Website: [www.cifas.org.uk](http://www.cifas.org.uk) [www.identityfraud.org.uk](http://www.identityfraud.org.uk)

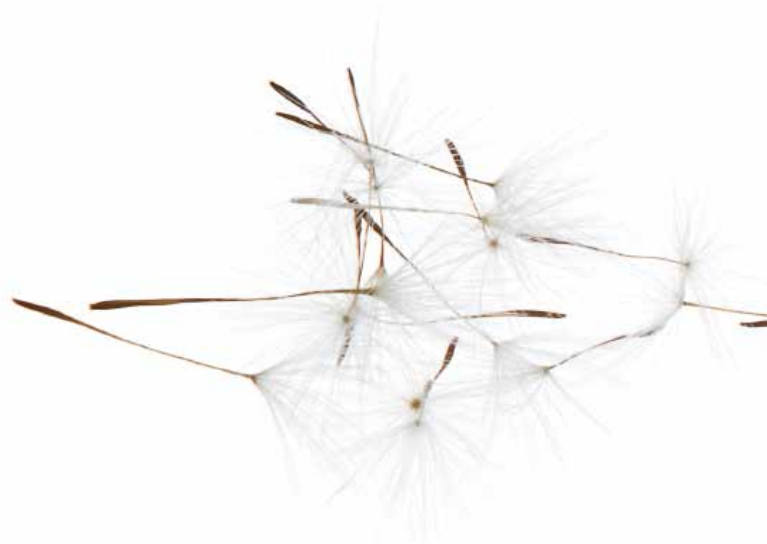


# What is this guide about?

Members have approached CIFAS with increasing evidence that fraudsters are targeting and exploiting people who are perceived as being vulnerable in such a way that they can be bribed, corrupted or coerced into committing fraud against CIFAS Members, individuals and other organisations to obtain funds. These criminals may also be involved in other types of organised crime.

This guide:

- seeks to raise awareness at all levels amongst CIFAS Members that fraudsters are becoming more expert at targeting individuals who put their trust in, or rely on, third parties.
- outlines the methods that fraudsters are using to take advantage of people based on the experience of CIFAS Members, other fraud prevention professionals and law enforcement officers who attend the CIFAS Organised Fraud and Intelligence Working Group meetings.
- compiles national best practice guidelines produced by the Building Societies Association, The Trading Standards Institute, the British Bankers' Association and Operation Liberal (the national distraction burglary intelligence unit) together with current best practice used across the CIFAS Membership.



## What should you consider?

When it comes to abuse of trust, any trusting person can be deceived or intimidated. Fraudsters will target anyone they believe could be a potential asset, whom they can deceive and of whom they can take advantage.

The determined fraudster has the knowledge, skills and experience to make him or her adept at spotting and exploiting any perceived vulnerability.

The financial loss from a fraud may fall to the financial organisation involved, or it may fall to the victim of a scam. The emotional cost to a victim who is abused in this way is unquantifiable.

## What makes us at risk?

Everyone is at risk from fraud at different times in their lives as individual circumstances can lead them to being targeted by fraudsters in different ways. For example:

1. Anyone who is new to the UK financial market or who lacks specialist knowledge of the UK financial systems and associated fraud risks; for example, young people.
2. Elderly people, people with physical disabilities; or people with special needs may be emotionally susceptible to blackmail, intimidation or coercion. This could be from strangers or from people they know.
3. The UK remains a popular destination for migrants seeking work, seeking to study or attracted by the promise of a new start for themselves or their families. Language barriers and the sometimes desperate circumstances of these individuals can make them targets for organised criminals, who may exploit them to open genuine accounts for subsequent fraudulent use, or to sell or obtain documents and otherwise facilitate other types of crime. Illegal immigrants may be particularly susceptible to blackmail, corruption or exploitation.

# How do fraudsters select their targets?

## ‘Phishing’ and ‘Grooming’

The object of ‘phishing’ is for a fraudster to persuade individuals to give out their personal information to them voluntarily. Fraudsters may set up genuine-looking websites, or hijack existing websites and online profiles, to ‘hook’ their victims. Once diverted to the fraudulent website, individuals are often unaware that they are passing their details to criminals. Some of these websites can look very convincing. Someone who lacks technological knowledge, or who is not fully aware of the risks associated with online security, for example the very young, or the elderly, can be particularly vulnerable to these types of scams.

Online dating sites are a common route by which fraudsters may establish rapport with their victims. After a period of time, once trust has been established and the victim has been ‘hooked’, the fraudster pretends to have had an urgent change in financial circumstances and persuades the victim to send money abroad to them. In ‘romance frauds’ the fraudster will often exploit sympathetic victims, requesting money from them to help with a fictional family crisis or serious accident. Where a victim gives out their personal or financial details, in any situation, these may then be used by the fraudster to commit further crime.

Fraudsters are not selective in their approach. They may use a variety of recruitment methods, including spam emails, adverts on genuine recruitment web sites or in newspapers, or on instant messaging and social networking sites, to find and recruit individuals who can be duped into acting as ‘money mules’. These individuals are recruited by fraudsters to receive fraudulent funds into their accounts, and withdraw the money to send it overseas by wire transfer service. A

fraudster may pretend to sell an article or asset to a victim, such as a car or property, and may ‘groom’ them to lull them into a false sense of security about the nature of the purchase arrangements. Once the victim has paid out, the fraudster vanishes and the purchased item is never delivered.

## ‘Fronting’ and ‘Fooling’

In order to evade detection, some fraudsters will target individuals and persuade them to permit their details to be used to ‘front’ new applications for facilities on the fraudsters’ behalf. Fraudsters may also persuade individuals to allow them to use their existing facilities for fraudulent purposes. ‘Persuasion’ could take the form of bribery, intimidation or coercion.

For example, some fraudsters will approach young students, who may or may not also be international students, and persuade them to receive fraudulently obtained funds, or to pay stolen cheques or false travellers cheques into their account and withdraw the funds before the payment is returned unpaid. Sometimes the fraudster will create a cover story to disguise or ‘legitimise’ why they need to use the victim’s account.

During 2009, Members reported an increase in the number of individuals who were complicit in this type of fraud, which suggests that this type of fraud in particular is becoming more organised. However it can often be difficult for Members to confirm whether an individual is complicit in such frauds, or if they have been fooled.

>

about their activities and the individual may be offered a form of payment, or 'commission' for the use of the account. Where a Member can prove that the customer is complicit in the fraud, a Misuse of Facility case could be filed to CIFAS. However in other situations, the individual may not be fully aware of the implications of their actions and may have been conned into allowing their account to be used in this way in the first place. Such individuals may be susceptible to further blackmail or intimidation if the fraudster thinks they could be useful again.

In a case study reported to CIFAS, a student working in the call centre of a financial institution developed a gambling addiction and lost substantial funds at local casinos. Criminal customers at the casino were aware of his employment and recognised that he was in financial difficulties. The student was approached and offered payment in return for customer profile details which he provided. Monies were transferred fraudulently out of multiple customer accounts into third party accounts and withdrawn in cash to the tune of around £850,000.

## Staff Fraud and Corruption

Members of staff may be at risk of being targeted by a fraudster by virtue of their position. For example, any worker with access to personal/commercial/sensitive data could be targeted by organised criminals as a potential 'asset'. Members have reported instances where front line staff have been planted or 'turned' by criminals in order to facilitate exploitation of other individuals who are at risk of being targeted by fraudsters. This could include setting up accounts for individuals who have been trafficked into the UK by organised criminal groups or manipulating genuine accounts belonging to vulnerable customers.

# What can be done to tackle these problems?

## Know your Customer

Members will have standard compliance and 'Know Your Customer' checks at the point of opening the account or facility. Guidance given to staff, and particularly to sales teams, may include advice on the fraud risks when taking on clients and customers who may be considered worthwhile targets by fraudsters.

For example, Members may wish to consider what fraud prevention advice they already give to young customers or students, when an account or facility is opened. For example, the website [www.banksafeonline.org.uk](http://www.banksafeonline.org.uk) hosted by UK Payments Administration offers comprehensive guidance and advice on 'money mules'. Members may wish to consult or refer customers to [www.getsafeonline.org.uk](http://www.getsafeonline.org.uk). This website offers further advice on internet security and protecting identity online.

The British Bankers' Association (BBA) have also produced a leaflet for consumers on the importance of proving one's identity which highlights how criminals seek to use bank accounts for money laundering to hide and disguise the money they make from crime. This leaflet is available from the BBA website at [www.bba.org.uk](http://www.bba.org.uk).

## Know your Staff

CIFAS and the Chartered Institute of Personnel and Development (CIPD) have produced guidance on *Tackling Staff Fraud and Dishonesty: Managing and Mitigating the Risks* which can be obtained by contacting the CIFAS office. SOCA has also produced an Alert product on 'Counter Corruption – Managing Insider Threats' which is available for download from the SOCA section of the Secure Members' Area of the CIFAS website.

## Customer-Staff Interaction

National best practice guidance was circulated as part of Operation Liberal, the national police operation into 'doorstep crime' (including distraction burglary, bogus callers and rogue traders). The guidance was drawn up in 2004 by the Trading Standards Institute, the Building Societies Association (BSA) and the British Bankers' Association (BBA), and refers to the protection of vulnerable people in a face-to-face environment, such as a branch. It may be that the customer has been the victim of a mass marketing fraud, or is responding to a '419' lottery scam. An example is when an elderly, or other potentially vulnerable customer wishes to make a withdrawal which is outside their normal routine, (e.g. unusually large and/or especially when they are accompanied by an unknown person).

The cashier should tactfully enquire why the cash is needed; point out the dangers of carrying large cash amounts; discourage the customer from drawing out cash, especially by pointing out the other means of payment available. Such advice, where possible, should be communicated to the customer in a private area. Some Members have a separate interview room in branches for front line staff to handle cases where persons have been accompanied by an unknown third party or wish to make unusual transactions.

Where it is suspected that the customer may be a potential victim of financial crime, the consent of the customer should be sought to inform the police or Trading Standards.

Where suspicious circumstances arise, every effort should be made to record the customer and any accompanying person(s) on the CCTV security system.



Where possible, an attempt should be made to identify any vehicle being used by the customer.

## Lines of Communication

Having a clear and direct line of communication between front line staff and fraud teams can be essential to ensure an efficient and timely response when an individual is potentially at risk from being defrauded. Some Members encourage staff to use a central 'hotline' number to report incidents of suspicious behaviour involving vulnerable people.

Many CIFAS Members have systems or procedures in place to monitor unusual account activity or to spot suspicious spending behaviour which could pose a fraud risk to the organisation. For example, some of these processes will flag large transactions being made in the early hours of the morning across an account. However these processes may not necessarily flag that an individual account holder is particularly at risk of being defrauded or conned out of their life savings.

Members may wish to evaluate how their existing policies protect against the exploitation of vulnerable people and consider using some of the ideas in this guide to introduce additional policies or procedures where possible.

## Taking Action Against Fraud

People at risk, particularly the elderly, can be targeted over the telephone by 'cold callers', some of whom may in fact be fraudsters phishing for information. When dealing with 'cold calls', advice from Trading Standards and Operation Liberal is to join the free Telephone Preference Service (TPS) by calling **0845 070 0707**. This

removes people from marketing lists within 28 days and should stop the majority of legitimate, though unwanted, telesales calls, including 'silent calls' where the phone rings but nobody is there when the phone is picked up. Registering with the service should prevent legitimate organisations from contacting an individual, and therefore it may help individuals to distinguish more easily when an unsolicited call is suspicious and should be treated with extra caution. Further information on the TPS can be found at [www.mpsonline.org.uk/tps](http://www.mpsonline.org.uk/tps). Further information on the extensive work of Operation Liberal can be obtained by emailing [opl Liberal@leicestershire.pnn.police.uk](mailto:opl Liberal@leicestershire.pnn.police.uk).

It is not uncommon for fraudsters to target the elderly through '419' mass mailing scams, whereby elderly individuals can be conned out of their life savings in response to unsolicited phone calls and other phishing methods. Further information for Members on phishing scams and how to report phishing websites can be found in the CIFAS Best Practice Guide 2009/28. Useful information and thought-provoking case studies on mass marketing fraud scams can be found on the 'Think Jessica' website at [www.thinkjessica.com](http://www.thinkjessica.com). The Office of Fair Trading has also produced a guide for carers and care professionals on how to prevent someone they are caring for from being defrauded. This is available from the Consumer Advice section of the OFT website at [www.of.gov.uk](http://www.of.gov.uk)

Additional guidance and advice on how to identify and report scams may be obtained from Consumer Direct at [www.consumerdirect.gov.uk/watch\\_out/](http://www.consumerdirect.gov.uk/watch_out/). Individuals who believe they have been the victim of a scam may wish to contact Consumer Direct on 08454 04 05 06 for advice.



CIFAS - The UK's Fraud Prevention Service  
6th Floor, Lynton House  
7-12 Tavistock Square  
London  
WC1H 9LT

[www.cifas.org.uk](http://www.cifas.org.uk)