

PAS 17271:2017

Protecting customers from financial harm
as a result of fraud or financial abuse –
Code of practice



Publishing and copyright information

The BSI copyright notice displayed in this document indicates when the document was last issued.

© The British Standards Institution 2017. Published by BSI Standards Limited 2017.

ISBN 978 0 580 91671 7

ICS 03.060, 03.080.30, 13.310

No copying without BSI permission except as permitted by copyright law.

Publication history

First published 2017

Contents

Foreword	ii
Introduction	iv
1 Scope	1
2 Terms, definitions and abbreviations	2
3 Organizational principles, culture and strategy	5
4 Service planning and design	7
5 Systems and tools for the prevention and detection of fraud and financial abuse	13
6 Helping customers to make informed decisions	17
7 Identifying customers at risk from financial harm	19
8 Taking action to prevent or reduce financial harm	22
9 Service evaluation	27
Bibliography	29
List of figures	
Figure 1 – Factors that can contribute to financial harm	iv
Figure 2 – Organizational key steps to minimizing financial harm to customers	5
List of tables	
Table 1 – Factors which can place individuals in vulnerable circumstances	19
Table 2 – Potential indicators of individuals in vulnerable circumstances	20
Table 3 – Possible organizational response to customers in vulnerable circumstances	26

Foreword

This PAS was sponsored by NatWest. Its development was facilitated by BSI Standards Limited and it was published under licence from The British Standards Institution. It came into effect on 31 October 2017.

Acknowledgement is given to the following organizations that were involved in the development of this PAS as members of the steering group:

- Barclays
- Building Societies Association
- Consumer & Public Interest Network
- Financial Fraud Action UK*
- Home Office Joint Fraud Task Force
- KMB Telemarketing Ltd
- Metropolitan Police
- National Trading Standards
- NatWest
- Office of the Public Guardian
- Santander UK plc
- Scottish Business Resilience Centre
- The Co-Operative Bank plc

Acknowledgement is also given to the members of a wider review panel who were consulted in the development of this PAS.

The British Standards Institution retains ownership and copyright of this PAS. BSI Standards Limited as the publisher of the PAS reserves the right to withdraw or amend this PAS on receipt of authoritative advice that it is appropriate to do so. This PAS will be reviewed at intervals not exceeding two years, and any amendments arising from the review will be published as an amended PAS and publicized in *Update Standards*.

This PAS is not to be regarded as a British Standard. It will be withdrawn upon publication of its content in, or as, a British Standard.

**Financial Fraud Action UK (FFA UK) is responsible for leading the collective fight against financial fraud. On 1 July 2017, FFA UK joined with the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Payments UK and The UK Cards Association to form UK Finance, representing around 300 firms in the UK providing credit, banking, markets and payment-related services. FFA UK will continue to facilitate collaborative activity between industry participants and with other partners committed to fighting fraud.*

The PAS process enables a code of practice to be rapidly developed in order to fulfil an immediate need in industry. A PAS can be considered for further development as a British Standard, or constitute part of the UK input into the development of a European or International Standard.

Use of this document

As a code of practice, this PAS takes the form of guidance and recommendations. It should not be quoted as if it were a specification and particular care should be taken to ensure that claims of compliance are not misleading.

Any user claiming compliance with this PAS is expected to be able to justify any course of action that deviates from its recommendations.

It has been assumed in the preparation of this PAS that the execution of its provisions will be entrusted to appropriately qualified and experienced people, for whose use it has been produced.

Presentational conventions

The guidance in this standard is presented in roman (i.e. upright) type. Its recommendations are expressed in sentences in which the principal auxiliary verb is "should". The word "may" is used in the text to express permissibility, e.g. as an alternative to the primary recommendation of the clause. The word "can" is used to express possibility, e.g. a consequence of an action or an event.

Commentary, explanation and general informative material is presented in smaller italic type, and does not constitute a normative element.

Where words have alternative spellings, the preferred spelling of the Shorter Oxford English Dictionary is used (e.g. "organization" rather than "organisation").

Contractual and legal considerations

This publication does not purport to include all the necessary provisions of a contract. Users are responsible for its correct application.

Compliance with this PAS cannot confer immunity from legal obligations.

Particular attention is drawn to the following regulations, and their equivalents in the different countries of the UK:

- Equality Act 2010 [1];
- Payment Services Regulations 2009 [2];
- Second Payment Services Directive 2016 [3];
- Money Laundering Regulations 2007 [4];
- Proceeds of Crime Act 2002 [5];
- Mental Capacity Act 2005 [6];
- Criminal Finances Act 2017 [7];
- Fraud Act 2006 [8];
- Adults with Incapacity (Scotland) Act 2000 [9];
- Adult Support and Protection (Scotland) Act 2007 [10].

Introduction

Financial harm is the loss of an individual's money or other assets that occurs as a result of fraud or financial abuse perpetrated by a third-party. Fraud is a criminal act involving deception or omission intended to result in financial or personal gain, or to cause loss to another party. Fraud can be carried out by individuals or organized crime groups, who constantly devise new and sophisticated methods to: deceive individuals; stay a step ahead of organizational fraud prevention measures; and evade enforcement agencies. Financial abuse is the criminal act of controlling a person's property, money, pension book or other valuables intended to result in the financial or personal gain of the abuser. It is carried out by people in a position of trust, such as partners, relatives, friends or carers.

Fraud and financial abuse are both illegal acts.

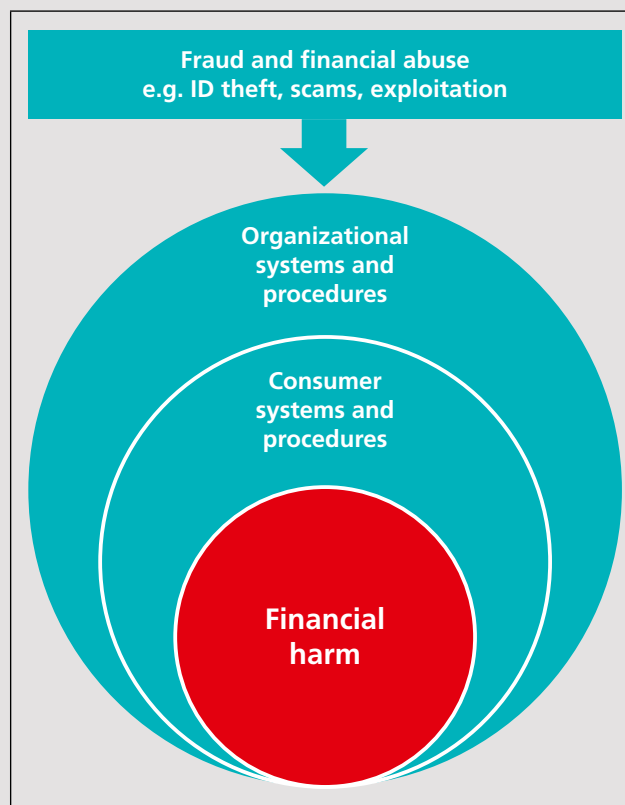
Cases of fraud and financial abuse are widespread. In 2016, there were a total of 1,857,506 cases of financial fraud in the UK, according to Financial Fraud Action UK [11]. During 2016, financial fraud losses across payment cards, remote banking and cheques totalled £768.8 million, an increase of 2% compared to 2015 [11]. Certain types of fraud, such as mobile banking, and scams directly targeting customers, are on the rise [11].

However, experts believe that only a fraction of all fraud cases are reported [12]. Consumers might not realise that a crime has taken place; they might not know where to report incidents; or might be too scared or embarrassed to tell anyone what has happened.

Anyone can be a target of fraud or financial abuse, but there are a number of factors that can contribute to financial harm (see Figure 1). Some individuals are more susceptible to fraud and financial abuse, or more likely to suffer financial harm. This can include individuals in vulnerable circumstances, either temporarily or permanently, which can affect their ability to communicate, understand, make decisions or take actions that are in their best interests.

The way that organizations treat customers can also contribute to levels of financial harm. Inadequate systems and procedures that fail to inform, protect and support customers can exacerbate existing consumer vulnerabilities, making it more likely that fraud or financial abuse will result in financial harm.

Figure 1 – Factors that can contribute to financial harm



This PAS aims to help organizations protect customers from financial harm, by identifying good practice in systems and procedures to prevent and detect fraud and financial abuse, recognizing customers who might be susceptible to risk, and advising on the best way to respond to certain situations. This PAS provides detailed recommendations, guidance and a comprehensive checklist to organizations that want to implement change, to achieve or maintain levels of good practice.

Working together has many benefits for financial service providers, as well as fraud prevention organizations, enforcement agencies, and consumers. Sharing knowledge, experience and intelligence, within the limits of current legislation, can help to build stronger defences against fraud and financial abuse and reduce the impact of financial harm. Organizations that comply with this PAS are encouraged to explore opportunities for collaborative working, at both a local and national level, to ensure consistent messaging and effective protection for consumers.

1 Scope

This PAS gives recommendations to organizations for protecting customers from financial harm that might occur as a result of fraud or financial abuse.

The PAS also gives guidance on how to recognize customers who might be at risk from fraud and financial abuse, how to assess the potential risks to the individual and how to take the necessary actions to prevent or minimize financial harm.

In cases where fraud or financial abuse has already occurred, the PAS gives guidance on how to help and support customers, and how to minimize future risks.

This PAS does not cover financial services provided to businesses, organizations that only hold, manage or process personal data, or the sale of products and services by retail organizations. It does not cover financial service providers operating outside the UK, even if they are providing services to UK consumers.

The PAS is applicable to any size or type of organization, operating in the UK, that manages the money or other financial assets of UK consumers, in particular banks, building societies, credit card providers, credit unions, and pension providers.

NOTE 1 *This PAS could also be of interest to local authorities across the UK that provide social care services.*

NOTE 2 *This PAS cannot help organizations to prevent fraud or financial abuse from external threats, but aims to help them minimize or prevent the financial harm experienced by customers as a result of these activities.*

NOTE 3 *Fraud or financial abuse can involve transactions which are not authorized by the customer, or are authorized by a customer who has been deceived or socially engineered by a criminal.*

2 Terms, definitions and abbreviations

2.1 Terms and definitions

For the purposes of this PAS, the following terms and definitions apply.

2.1.1 accessibility

usability and availability of a product, service, environment or facility by people with the widest range of capabilities

NOTE The concept of accessibility addresses the full range of user capabilities and is not limited to users who are recognized as having a disability.

2.1.2 accessible format

method of presenting **information (2.1.16)** that makes it usable by the widest possible range of people, regardless of their different needs and abilities

NOTE For example, accessible formats for those with visual impairments can be audio description, braille or telephone. Accessible formats for people with hearing impairments can be British Sign Language, Makaton, subtitling, textphone or SMS. Accessible formats for those with co-ordination difficulties can be large print, audio, audio description or telephone.

2.1.3 authorized transaction

payment from a **customer's (2.1.5)** account, which has been approved by the **customer (2.1.5)**

*NOTE An authorized transaction might include a payment approved by a **customer (2.1.5)** under duress as a result of financial abuse (2.1.9) or as a result of fraud (2.1.11), where a criminal has maliciously misdirected a payment by substituting their bank details for those of a legitimate person or business.*

2.1.4 complaint

oral or written expression of dissatisfaction made to an organization, whether justified or not, from (or on behalf of) an individual, about the provision of, or failure to provide, a service

2.1.5 customer

person using, or thinking of using, a financial service provided by an organization

NOTE 1 For example, the person might have a current account, savings account, mortgage or insurance policy with the organization.

NOTE 2 For the purposes of this PAS, the term customer includes existing and potential customers of the organization's financial services.

2.1.6 deputy

person appointed by the Court of Protection in England and Wales to make decisions on behalf of another person who lacks mental capacity to make those decisions themselves

NOTE A deputy can be appointed to make decisions about property and financial affairs, or health and welfare, or both.

2.1.7 detriment

negative impact as a result of an action or event

NOTE Detriment to an individual can include financial loss, damaged credit rating or exclusion from essential financial services. It may also include non-financial detriment such as wasted time, inconvenience, stress, anxiety, depression or sleeping problems.

2.1.8 feedback

comment(s), suggestion(s) or formal **complaint(s) (2.1.4)** about an organization from a **customer (2.1.5)**, member of staff or any other interested party

2.1.9 financial abuse

criminal act of controlling a person's property, money, pension book or other valuables intended to result in the financial or personal gain of the abuser, carried out by people in a position of trust, such as partners, relatives, friends or carers

NOTE 1 The abuser might use coercion and exploitation, which can include physical threats or emotional manipulation, pressure in connection with wills, property or inheritance or financial transactions or the misuse or misappropriation of property, possessions or benefits.

NOTE 2 Attention is drawn to the Fraud Act 2006 [8].

2.1.10 financial harm

loss of a **customer's** (2.1.5) money or other financial assets, or harm to a **customer's** (2.1.5) financial condition or reputation, that occurs as a result of **fraud** (2.1.11) or **financial abuse** (2.1.9) committed by a third-party

NOTE In addition to financial loss, financial harm can also include reputational loss or regulatory censure.

2.1.11 fraud

criminal act involving deception or omission intended to result in financial or personal gain, or to cause loss to another party

NOTE 1 Fraud can be committed online, by email, letter, or in person. Methods of fraud can be very sophisticated and are changing all the time. Fraud can involve authorized or non-authorized payments.

*NOTE 2 An occurrence of fraud can be known as a **scam** (2.1.21).*

NOTE 3 Attention is drawn to the Fraud Act 2006 [9].

2.1.12 frontline staff

staff that have direct contact with **customers** (2.1.5) across all contact channels

NOTE Contact with customers can be face-to-face, over the telephone, via emails, social media or online chat.

2.1.13 guidance

free, impartial service to help **customers** (2.1.5) or their **third-party representatives** (2.1.24) identify their options and narrow down choices to make decisions that are in their best interests

*NOTE For example, by giving **information** (2.1.16) that is relevant to the individual's circumstance, explaining options and benefits and identifying further action that can be taken.*

2.1.14 guardian

person appointed by the Sheriff Court in Scotland to make decisions on behalf of another person who lacks mental capacity to make those decisions themselves

NOTE A guardian can be appointed to make decisions about property and financial affairs, or health and welfare, or both.

2.1.15 inclusivity

availability, usability and **accessibility** (2.1.1) of a product or service to all **customers** (2.1.5) equally, regardless of their personal circumstances, needs and abilities

2.1.16 information

communication of items of knowledge, facts and data about certain topics that can be used to inform choice

NOTE Information can be given in response to an enquiry, or suggested to someone that might benefit from the information. The recipient is responsible for interpreting information and deciding how to proceed.

2.1.17 outcome

end result or impact

*NOTE Desired outcomes can be set out in an organization's objectives. An outcome can affect **customers** (2.1.5), staff or the organization itself. An outcome can be positive or negative. A positive outcome could be detecting **financial abuse** (2.1.9) before **financial harm** (2.1.10) has taken place, preventing the loss of a **customer's** (2.1.5) personal data or money from their bank account, or reimbursement of a **customer's** (2.1.5) financial losses.*

2.1.18 power of attorney (POA)

legal document that lets an individual appoint one or more persons (the "attorney(s)") to help them make decisions, or to make decisions on their behalf

NOTE There are different types of Power of Attorney in England and Wales, Scotland and Northern Ireland: see <https://www.gov.uk/power-of-attorney/overview>.

2.1.19 referral

re-direction of a **customer** (2.1.5) for the purpose of receiving more **information** (2.1.16), specialized advice or further action

2.1.20 safeguarding

measures put in place to protect **customers** (2.1.5) and staff from harm

2.1.21 scam

transaction or proposition based on false information, which encourages the victim to reveal security information or pay away funds on the basis that there will be a benefit to them as a result

2.1.22 signposting

giving **information** (2.1.16) about other organizations providing products or services that might be relevant and appropriate to a **customer's** (2.1.5) needs

*NOTE The **customer** (2.1.5) has responsibility for taking further action and making contact.*

2.1.23 suspicious transaction

financial transaction or activity which raises concerns, or can suggest, that a **customer (2.1.5)** is at risk from **fraud (2.1.11)** or **financial abuse (2.1.9)** that could result in **financial harm (2.1.10)**

***NOTE** A suspicious transaction can be a payment, or series of payments, for an unusually large amount or to a new payee. A transaction may also raise suspicions if it matches a known method of fraud.*

2.1.24 third-party representative

person acting legitimately on behalf of a **customer (2.1.5)**

***NOTE** For example, a third-party representative might be a relative or friend acting on behalf of another person. They might have a power of attorney (POA), guardianship or a court order in place to act formally, and make decisions, on that person's behalf.*

2.1.25 unauthorized transaction

payment where money is debited from a **customer's (2.1.5)** account without their approval or consent

***NOTE** For example, an unauthorized transaction can include a payment made using a stolen debit or credit card.*

2.1.26 vulnerable circumstance

long or short-term situation that can make an individual more susceptible to **fraud (2.1.11)** or **financial abuse (2.1.9)**, placing them at increased risk of **detriment (2.1.7)** or **financial harm (2.1.10)**

***NOTE** Anyone can find themselves in vulnerable circumstances at any time, depending on their personal situation. There are a variety of factors that can place an individual in vulnerable circumstances such as: age related issues; low literacy, numeracy or financial capability; physical or mental illness; or a change in circumstances (e.g. job loss, bereavement or divorce). See 7.1.3.2 for further information about factors that can cause vulnerability.*

2.2 Abbreviations

For the purposes of this PAS, the following abbreviations apply.

BIBA	British Insurance Brokers Association
FCA	Financial Conduct Authority
FFA UK	Financial Fraud Action UK
FOS	Financial Ombudsman Service
NFIB	National Fraud Intelligence Bureau
POA	Power of Attorney

3 Organizational principles, culture and strategy

3.1 General principles

The organization should deliver a service that:

- offers a person-centred approach that responds to the needs of each customer;

NOTE Further information on identifying and responding to customers' needs is given in BS 18477.

- takes a proactive approach to minimizing risks, impact and incidences of financial harm;

- treats all customers fairly (see 4.2.1);

NOTE Further information on how to treat customers fairly is given in BS 18477 Inclusive service provision.

- provides a consistent level of customer service that meets or exceeds reasonable customer expectations;

NOTE Further information on how to meet or exceed customer expectations is given in BS 18477.

- empowers customers to make informed choices;
- is responsive to feedback and newly emerging threats.

3.2 Organizational culture

The organization should develop behaviour and responsibilities that demonstrate commitment to the general principles identified in 3.1. This commitment should be led by the executive team and embedded across the organization through on-going engagement and communication with all members of staff.

3.3 Customer fraud prevention strategy

3.3.1 Documented strategy

To ensure that all members of staff adopt a consistent approach, and are aware of key processes, the organization should have a documented customer fraud prevention strategy.

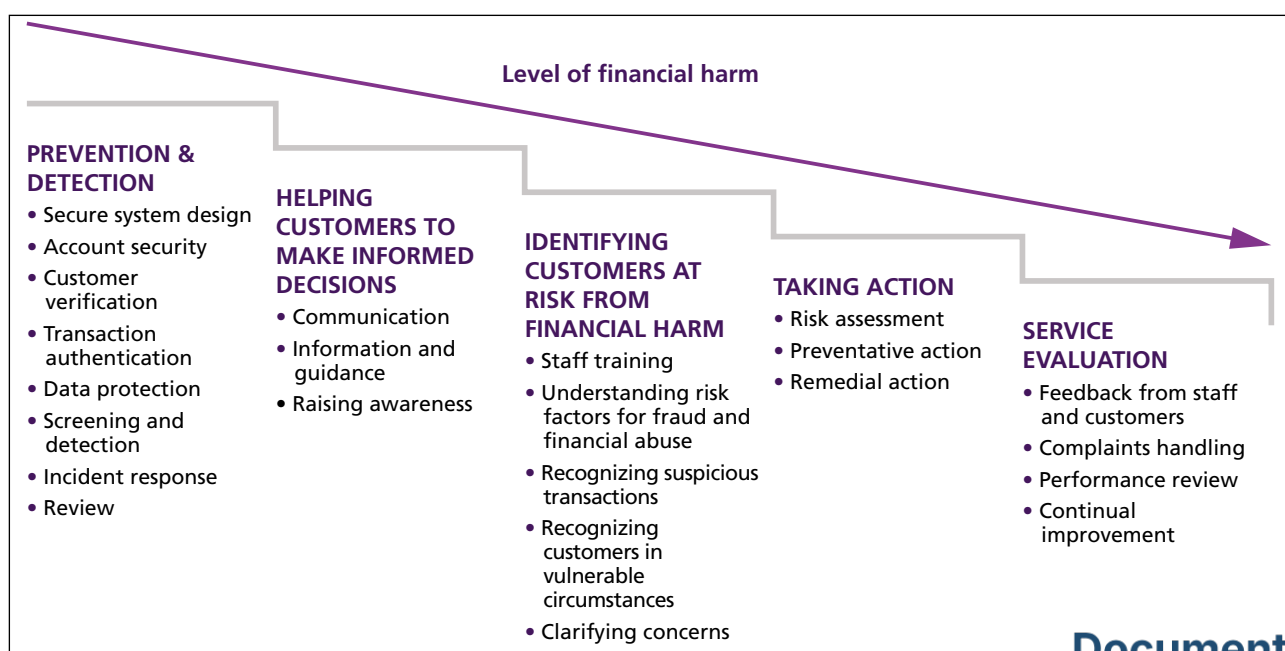
NOTE The organization may use a different name for this strategy, but it is important that the content, consultation and staff awareness follow the requirements below.

3.3.2 Key stages of service delivery

The customer fraud prevention strategy should include information about how the organization plans to protect its customers from financial harm by implementing the five key stages of service delivery detailed in this PAS (see Figure 2):

- systems and tools for the prevention and detection of fraud and financial abuse (see Clause 5);
- helping customers to make informed decisions (see Clause 6);
- identification of customers at risk from financial harm (see Clause 7);
- taking action to prevent or reduce financial harm (see Clause 8); and
- service evaluation (see Clause 9).

Figure 2 – Organizational key steps to minimizing financial harm to customers



3.3.3 Leadership responsibility

The organization should appoint a specific senior member of staff who, irrespective of other responsibilities, should have the defined role, responsibility and authority to implement and manage the customer fraud prevention strategy.

3.3.4 Specialist staff

The organization should appoint specific fraud prevention staff, that have specialist knowledge of fraud or financial abuse and can deal with customers, or frontline staff, who need expert guidance on issues related to financial harm.

NOTE Customer fraud prevention staff may refer to an individual, or a specialist team, whose specific role is to provide help and support to customers who are at risk from, or have suffered financial harm as a result of, fraud or financial abuse.

3.3.5 Awareness of the customer fraud prevention strategy

The organization should create a defined, documented procedure, communicated and accessible to all frontline staff, that details:

- a) who in the organization is responsible for implementing and managing the customer fraud prevention strategy;
- b) where to go within the organization for further information and advice on related matters;
- c) how to identify customers who might be at risk from financial harm, and when to refer these customers to specialist staff or team within the organization;
- d) the referral process for customers who require specialist help and support from external agencies; and
- e) the Banking Protocol¹, and other industry guidance, where in operation.

The organization should ensure that all members of staff are reminded of the customer fraud prevention strategy at key stages throughout their employment. These stages should include, as a minimum:

- a) when staff begin their employment with the organization;

- b) when staff move to a new role within the organization;
- c) when the customer fraud prevention strategy is revised or updated;
- d) after an incident which resulted in, or had the potential to lead to, financial harm; and
- e) whenever the organization introduces new products, services or distribution channels.

The customer fraud prevention strategy document should be accessible to all relevant members of staff so that they can reference the full text when necessary.

NOTE The above list is not exhaustive and there might be other occasions on which it is useful for the organization to remind staff of the customer fraud prevention strategy.

3.3.6 Strategy consultation

When developing the customer fraud prevention strategy the organization should consult with those who have knowledge and experience of the subject to ensure that policies, systems and procedures are relevant and effective.

NOTE Those that have knowledge and experience of the subject can include organizations that represent vulnerable groups, customers who have experienced financial harm and experts working to protect consumers from fraud and financial abuse.

¹⁾ The Banking Protocol is a collaboration between police forces, trading standards departments and financial organization branch staff set up to prevent fraud. Information and relevant documentation regarding the Banking Protocol is available from Financial Fraud Action UK upon request: <https://www.financialfraudaction.org.uk>.