fair4all finance

Good Practice Lending Guide

RM06 Customer Verification and Fraud Prevention

May 2024

Disclaimer

This Guide is provided purely for informational purposes, has been prepared for general use only, and does not constitute legal, financial or other professional advice.

All information contained in this Guide is based on the laws and regulations applicable to England and Wales and which are current as of the date of publication. This guide is not maintained regularly, but we will endeavour to update it when relevant laws or regulations are amended, varied, or supplemented. At a minimum, the Guide will be reviewed annually to ensure compliance with any legal or regulatory changes.

Fair4All Finance Limited make no representations or warranties of any kind, express or implied, about the accuracy, completeness, suitability, or reliability of the information contained herein. Fair4All Finance Limited shall not be liable for any loss or damage arising from the use of, or reliance on, this Guide. This Guide does not create an advisor-client relationship between you and Fair4All Finance Limited.

You are advised to consult with suitably qualified legal, financial or professional advisors to obtain advice tailored to your specific circumstances. You should not rely on the content of this Guide and any reliance on any information provided in this Guide is done at your own risk.

By accessing and using this Guide, you acknowledge and agree to the terms of this disclaimer.

This Guide must not be amended, copied, reproduced, distributed or passed on at any time without the prior written consent of Fair4All Finance Limited.

Contents

1 Introduction

1.1 Why are customer verification and fraud prevention important?

Money laundering and fraud are rife in financial services. Every year more than a billion pounds are written-off due to fraud[1] and the scale of Money Laundering in the UK potentially runs to hundreds of billions of pounds a year[2]. The nature of these activities is also changing rapidly and there has been an increase in the frequency of fraud attempts as lending moves increasingly online, with customers no longer needing to be physically present to make loan applications.

To prevent money laundering and minimise fraud loses, prudent lenders undertake several customer verification and fraud prevention measures before agreeing to advance funds to customers. These measures cover four main areas:

1. **Customer Verification.** This is to confirm that the person is who they say they are, resident at their stated address and that the information they provide is correct
2. **Sanctions Checks and PEP checks.** These are to check the individuals are not on the UK government's official sanctions list, and are not classified as Politically Important People (PEPs)
3. **Fraud Screening.** This identifies people who have previously been identified as fraudsters, people who have been the subject of fraud in the past and who believe they might be targets of fraud in the future
4. **Fraud Prediction.** This utilises predictive modelling and statistical analysis to identify potential fraudsters based on unusual patterns in their data compared to normal customers

Customer Verification, Sanctions and PEPs checks are primarily intended to comply with Know Your Customer (KYC) due diligence requirements to prevent money laundering and related activities as required by UK Law. However, they are also powerful fraud prevention tools that can prevent significant fraud losses being incurred. This is because by confirming that the applicant's details are correct, they prevent fraudsters using fictious personal details to acquire a loan. Likewise, tools designed to specifically to identify and prevent fraud also reduce the incidence of other types of illegal activity,

[1] UK Finance 2023. ANNUAL FRAUD REPORT 2023

[2] https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance, accessed 06/06/2023.

including money laundering.

Consequently, lenders who apply appropriate measures across all 4 of these areas have the most robust defences against both money laundering and fraud losses.

1.2 Why has Fair4All Finance commissioned this guide?

In our work with community finance lenders, those we have made significant investments into, and those we have funded through grants and capability support, we have come across a range of approaches to credit risk and provided consulting support to enhance them in many instances. This guide reflects our intention to document what good practice looks like on customer verification and fraud prevention, to share the insight that has been developed for specific lenders more broadly.

1.3 Purpose of this document

This document is intended to support Community Finance lenders in undertaking appropriate customer due diligence when processing loan applications. Specifically, this covers customer verification, Know Your Customer and fraud checks when deciding to lend to customers, and the different measures and tools that can be used to support these processes.

Every lender has their own approach to customer verification and fraud. However, it is important that firms clearly define and comprehensively document their policies and set up governance and oversight processes, to ensure regulatory compliance and that their fraud losses are kept to a minimum, in line with their stated business objectives and risk appetite.

This guide is not prescriptive. It is not intended to provide the definitive view as to how organisations should undertake customer verification and fraud prevention. However, it describes industry standard good practice approaches that are widely used across the credit industry.

The approach to customer verification and fraud prevention is generally applicable to all UK lenders, but it is primarily intended for small to medium sized organisations who are working to provide fair and affordable credit to sectors of the community who may otherwise struggle to obtain it. For example, not-for-profit community lenders and credit unions. Therefore, it adopts a proportionate approach suitable for these types of organisations.

Organisations can use the Guide in one of two ways:

1 As a reference manual, to help them enhance their own lending policies and to provide assurance that there are no gaps or shortcoming

2 To support new organisations in setting up appropriate customer verification and fraud prevention policies

The focus of this document are customer verification and fraud prevention. However, there are clear overlaps with other areas of lending, such as Credit Risk, Affordability, Management Information, Governance etc. These are signposted within the relevant sections throughout this guide.

2 Scope

The scope of this document, as part of the Good Practice Lending Guide, is:

1. Customer verification that occurs when a customer applies for a new loan ie the Know Your Customer due diligence checks that lenders are required to undertake to reduce the incidence of money laundering in line with their requirements under UK Law
2. The different types of fraud that can occur when a loan is applied for, and the tools that can be used to prevent losses being incurred when fraud is attempted

How customer verification and fraud detection align with other parts of the loan application process, such as credit risk and affordability, is described in the Application Process component of the Guide.

2.1 Legislation and regulatory guidance

The main legislation covering money laundering and how organisations should deal with it is The Money Laundering, Terrorist Financing and Transfer of Funds Regulations 2017[3] (MLRs) which were enacted under the Financial Services and Marketing Act 2000. As such, enforcement of the MLRs falls to the FCA, and applies to all regulated providers of financial services including banks, building societies and credit unions.

The FCA's Financial Crime Guide (FCG) provides comprehensive guidance to firms on the systems and controls they should have in place to prevent financial crime, including money laundering and fraud. The regulations require organisations to deploy appropriate due diligence to prevent its services being used for money laundering or terrorist financing.

The FCG also specifies that firms must assign responsibility for its anti-money-laundering strategy and operational activities to a suitably knowledgeable director or senior manager who can ensure that the organisation takes appropriate steps to mitigate the risks that money laundering (and other financial crime) presents to the organisation and wider society.

Although not a regulatory body, practical guidance as to how to prevent money laundering and combating terrorist financing is provided by the Joint Money Laundering Steering Group (JMLSG)[4].

[3] Amended in 2019.

[4] JMLSG – Joint Money Laundering Steering Group

3 Customer verification

In this section we describe the ways lenders can verify a customer's identity, and that the information they provide is correct. As part of standard due diligence requirements for KYC checks, two aspects of someone's persona need to be verified:

- Their identify, ie confirmation of the name and date of birth
- Where they live, ie their residential address

Traditionally, these would have been obtained by examining physical documents (as discussed later in this section) but these days verification can usually be established electronically by matching the applicant's details to on-line data sources.

3.1 Open banking data

Open Banking is a mechanism whereby an individual gives an organisation permission to view details of their current accounts (including credit cards) electronically. Using Open Banking provides customer verification because the details that a customer provides during their application, including their name, date of birth, address, income, and expenditure, can all be verified via their bank account. In effect, open banking allows the lender to piggyback the verification process that the bank undertook when opening and maintaining the customer's bank account.

A fuller description of Open Banking is provided in the appendix of the Affordability component of the Guide.

3.2 Third party verification tools

A range of organisations, including the three main UK credit reference agencies[5], provide customer verification tools that can be linked to an organisation's systems to automatically provide customer verification as part of the loan application process. Offline versions of these tools also exist to allow loan assessors to perform verification on a case-by-case basis as part of a manual underwriting process where required.

[5] Equifax, Experian, and TransUnion

Most verification tools are based on matching the customer's details provided during the loan application to other information the CRA's hold about them[6]. For example, if a customer:

- Is confirmed as having been registered on the Electoral Roll at their current address for many years
- Is paying utility bills from their current address
- Has several active and previous credit agreements recorded at that address

Then that provides a high degree of assurance that the person is a real person living at that address. In general, there needs to be at least two confirmed utility and two credit accounts for an account to pass verification.

Rather than providing a simple pass/fail indicator, many verification tools provide a score or grading system that rates customer based on the amount of information found. If, in the above example, a customer had been registered for 20 years on the Electoral Roll and had 10 active or previous credit agreements and utility bills, this would result in a higher verification score than someone who had only lived there for a couple of years and had say, 3 credit agreements/bills.

See the Credit Reference Agency component of the Guide for more information about the fraud and verification tools provided by specific Credit Reference Agencies. ￼

3.3 Documentary evidence

Automatic on-line customer verification methods, such as Open Banking and the tools provided by CRAs, are the easiest, quickest, and most efficient tools for verifying an individual's identity. However, there will be a proportion of cases where online verification is not possible, or the customer fails to pass the online check. Examples of when this can occur are:

- Someone has recently moved to the UK. Therefore, they are not registered on the Electoral Roll and no data about them is held by the CRAs
- Someone does not have an established credit record. It may be the first time that they have applied for a loan or several years since their last loan. This is a common issue for young people without much financial history
- The customer is actually a fraudster. If they have falsified data on the application form such as their date or birth, then no record of them will be found

To comply with anti-money laundering regulations, in these cases physical proof of identify are required

[6] This is almost identical to the process that occurs when a credit search is performed but the data is being used for verification rather than to provide a historic record of the customers credit history as provided on their credit report

before a loan can be granted. In some cases, organisations still insist on seeing these when engaging with new customers that they have not dealt with before even if on-line checks have been passed[7]

The UK Government[8] defines acceptable documentation as that shown in Table 1:

Table 1. Acceptable Forms of Identify & Proof of Address

Identify	Proof of Address
Current signed passport	Utility bill (gas, electric, satellite television, landline phone bill) issued within the last three months
Original birth certificate	council tax bill for the current council tax year
EEA member state identity card	Current UK driving licence (but only if not used for the name evidence)
Current UK or EEA photocard driving licence	Bank, Building Society or Credit Union statement or passbook dated within the last three months
Photographic registration cards for self-employed individuals in the construction industry -CIS4	Original mortgage statement from a recognised lender issued for the last full year
Benefit book or original notification letter from Benefits Agency	Solicitors letter within the last three months confirming recent house purchase or land registry confirmation of address
Firearms or shotgun certificate	Council or housing association rent card or tenancy agreement for the current year
Residence permit issued by the Home Office to EEA nationals on sight of own country passport	Benefit book or original notification letter from Benefits Agency (but not if used as proof of name)
National identity card bearing a photograph of the applicant	HMRC self-assessment letters or tax demand dated within the current financial year
	Electoral Register entry, OR NHS Medical card or letter of confirmation from GP's practice of registration with the surgery

[7] Often this will be traditional banks when open a bank account for a new customer.
[8] Proof of identity checklist - GOV.UK (www.gov.uk)

A lender can specify that they only accept some of these forms of identification. For example, a lender may not accept a firearms certificate because these are relatively rare, and staff are not trained to recognise what a real certificate looks like. However, they must ensure that they accept at least one item from each section in Table 1.

Documents that are not acceptable (but which customers sometimes mistakenly think are acceptable) are:

- Provisional driving licence
- Mobile phone bills
- Credit card statements

For cases where enhanced due diligence is required (such as someone appears on a PEP list or fraud is suspected) then a lender may ask for these proofs in addition to online verification to provide additional assurance of the customers identify.

For existing customers, there is no requirement to provide these documents again when they request a new product or service. However, if can be useful to repeat verification (ideally electronically) and fraud checks to identify third party fraud such as account takeover, or to identify any customers who have subsequently registered with CIFAS or have been added to PEPs and Sanctions lists.

4 PEP and sanctions lists

4.1 Politically Exposed Persons (PEPs)

A Politically Exposed Person (PEP) is an individual who holds, or has held, a prominent public position or role that may make them susceptible to corruption or involvement in money laundering activities. PEPs are considered higher risk by financial institutions due to their potential to abuse their position for personal gain. In the United Kingdom, the concept of PEPs is primarily governed by the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017.

A PEP can include individuals holding positions such as heads of state, government ministers, members of parliaments, senior judicial or military officials, or executives of state-owned enterprises. PEPs can also extend to their immediate family members and close associates who may benefit from their position or influence. There is no singular definition of what defines someone as a PEP, but most countries base their definitions on the recommendations of The Financial Action Task Force (FATF)[9].

When dealing with a loan application from a PEP, financial institutions are obligated to conduct enhanced due diligence measures to mitigate the potential risks associated with money laundering and corruption. These measures aim to ensure that the funds being transacted are legitimate and not derived from illicit activities.

The FCA's guidance to financial institutions on how to handle loan applications from PEPs includes the following steps:

- **Identification:** Financial institutions should implement robust processes to identify and verify if an applicant is a PEP or a close associate or immediate family member of a PEP. This may involve gathering information from credible sources such as public records, media reports, or specialized databases. Practically, this may mean screening loan applicants against lists collated by third party vendors, such as credit reference agencies and may be

[9] https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Peps-r12-r22.html#:~:text=FATF%20Guidance%3A%20Politically%20Exposed%20Persons%20(Rec%2012%20and%2022)&text=A%20politically%20exposed%20person%20(PEP,such%20as%20corruption%20or%20bribery.

included as part of a credit search.

- **Risk Assessment:** Once identified as a PEP, the financial institution should assess the level of risk associated with the applicant based on factors such as their position, the country's corruption index, and other relevant information. This risk assessment helps determine the appropriate level of due diligence measures required. It is not illegal to lend to a PEP, but it is important that lenders carry out sufficient due diligence to ensure that in providing a loan they are not supporting illegal activities such as money laundering and sponsoring terrorism. This may involve seeking additional information about the applicant's source of wealth, the purpose of the loan, and the intended use of the funds. It may also include verifying the applicant's financial background, business activities, and conducting ongoing monitoring of the account
- **Escalation**. In certain cases, a loan assessor may need to seek approval from senior management before proceeding with a loan application from a PEP. This ensures that decision-making is subjected to higher levels of scrutiny

It's important to note dealing with a PEP is riskier than dealing with an average customer, but it does not automatically mean that the loan application should be rejected. Financial institutions must consider the overall risk and make an informed decision based on their assessment and enhanced due diligence findings. It is likely that PEPs from the within the UK are probably less risky than those from elsewhere, and this should be considered within the overall review.

It should also be noted that concerns were raised in 2023 about the number of PEP related accounts being closed by banks and building societies without adequate justification. The FCA subsequently began an investigation in August 2023 as to the reasons for account closures[10].

4.2 Sanctions

The financial sanctions list in the United Kingdom is a database maintained by the government to enforce economic restrictions against individuals, entities, and countries deemed to pose a threat to national security, international peace, or human rights. Once a person is added to the list, their UK assets are frozen, and specific prohibitions and restrictions are placed on financial dealings with them. If an individual is on the sanctions list, then this means that a lender should not advance funds to them, and any application for credit should be declined.

Financial institutions, including banks, building societies, credit unions and other lenders, are required by law to screen their customers against the financial sanctions list. If a match is found during screening, the

[10] https://www.fca.org.uk/publication/correspondence/fca-chancellor-freedom-expression-provision-banking-services.pdf Note that at the time of writing (August 2023), the FCA's investigation is on-going.

financial institution must freeze the assets and report the findings to the OFSI.

The UK's financial sanctions regime derives from the Sanctions and Anti-Money Laundering Act 2018, which provides the legal framework for imposing and implementing sanctions. The primary responsibility for enforcing sanctions lies with the Office of Financial Sanctions Implementation (OFSI) with is a department within the Treasury.

The consequences of violating the financial sanctions list can be severe. In addition to reputational damage, criminal and civil penalties may be imposed on both individuals and firms.

The sanctions list contains multiple pieces of information about sanctioned individuals. This includes name, address, DOB, aliases, nationality, and passport details. Therefore, lenders should be careful not reject applications just because there is a name match or just an address match. If a lender is confident that the individual they are dealing with is not the person on the sanctions list (even though they have the same name or address) then they can proceed to grant the loan and taken no further action.

If a lender is unsure if a case is a match to the sanctions list, then they are advised to contact the OFSI for further guidance.

5 Fraud detection

In this section we describe the data and tools that can be used to identify fraudulent loan applications.

Whereas customer verification is a legal requirement to address money laundering, lenders are not obliged to have specific fraud prevention measures. However, having a robust fraud prevention process is important because, from a business perspective, fraudsters often target those institutions with the weakest defences. Once it becomes known that an organisation is an easy target, the incidence of fraud increases as fraudsters seek to maximise the amount they can extract before the organisation reacts to close the losses, and the fraudsters move on to their next target.

5.1 The types of loan application fraud

There are lots of different forms of financial fraud. In this section we discuss the types of fraud that can occur during a loan application.

5.1.1 First party fraud

First party fraud is when someone deliberately provides incorrect information to improve their changes of obtaining credit, or more credit on better terms than they would otherwise get. Personal details such as name and address are correct, but other aspects of the credit application are falsified. In most cases the applicant intends to repay what they borrow but provides misleading information, so they appear more creditworthy.

Typical, first party fraud will involve someone stating they are older than they are, providing inflated salary details, lying about their employment status, how long they have lived at their current address or failing to declare their full address history to conceal adverse history registered at previous addresses.

5.1.2 Identity theft (third party fraud)

Identify theft is when a fraudster obtains sufficient information about someone that they can impersonate them when making a credit application. Information allowing identity theft to occur may come from a variety of sources including:

- Online accounts and social media. Fraudsters capture information that people have made publicly available
- Bank statements, utility bills, payslips or other documents that have not been securely destroyed. For example, put out with the rubbish or stolen from someone's home or car
- The theft of items that contain personal information such as a credit card, someone's phone,

passport, or driver's licence

- Obtaining data directly from an organization. Data may be supplied by a member of staff who sells data for money, or an external hacker that obtains data by illegally accessing the organisations systems
- Phishing. This is where someone is persuaded to provide information about themselves. Usually this is via email or text from someone impersonating an organization or somebody that the person trusts, such as their bank or phone provider, who persuades them to provide personal details such as, their name, address, date of birth, bank account details and security information such as pin numbers and passwords

A widespread practice is for the fraudster to begin by using the information they have obtained to set up a bank account. Any funds they obtain can be paid into this account and then withdrawn. As the account has been set up using someone else's name and address it is very difficult to trace the fraudster should the authorities decide to investigate. Alternatively, the fake details may be used to obtain a revolving credit product or to obtain a phone or other credit facility.

5.1.3 Synthetic identify fraud

An advanced form of identity theft is synthetic identify fraud. Often a fraudster will be able to obtain some personal information about an individual but not enough to complete a loan application process fully. They will therefore create artificial data to fill in the gaps.

In some cases, information from multiple individuals will be blended to create a customer profile that appears very realistic, and at first sight is indistinguishable from a real individual. In extreme cases the entire application could be artificial with no real information used at all.

5.1.4 Sleeper fraud

Sleeper Fraud is when a fraudster initially obtains a credit facility that they use normally at first to improve their credit rating. They then use this "good" account as a steppingstone to additional credit. Once they have obtained as much credit as they can, they stop making payments to the accounts.

An example of sleeper fraud may be when someone initially opens a savings account, depositing a relatively small amount. After a few months they then apply for a low limit credit card with the same organisation. This is followed by loan applications, requests for credit limit increases and so on. They then withdraw their savings, max out their credit cards and stop paying their loan.

5.1.5 Account takeover

Account takeover is where a fraudster obtains information that allows them to access someone's account, such as their password or pin number. Once the fraudster has access to the account, they can change the details on their account to enable them to access funds.

An example of account takeover is where a fraudster obtains access to a credit union members account, and they then change the bank details on the account to match their own account. Once this has been done, they apply for a loan that is paid into this new bank account. This is one reason why it is important to carryout verification and fraud checks for existing customers as well as new customers when they apply for an additional lending facility.

5.2 Fraud detection and prevention tools

In this section we discuss the different tools that lenders can employ to detect fraudulent loan applications.

Although some organisations develop their own in-house fraud prevention tools, the most widely used tools for fraud prevention are provided by third party vendors. During the loan application process, access to the relevant tool(s) is via an appropriate Application Interface (API) between the lenders application processing system and the vendor's systems. Standalone versions of the tools also exist, to single cases to be reviewed outside of the standard application process.

All the major credit reference agencies provide a variety of verification and fraud prevention tools. Many of these can be supplied as an extension to a standard credit report, supplied as part of a credit search.

5.2.1 CIFAS

The Credit Industry Fraud Avoidance Scheme (CIFAS) is a not-for-profit subscription services which maintains the National Fraud Database of proven and suspected cases of fraud. Over 600 organisations in the UK are members of CIFAS including most banks and building societies, and many credit unions.

CIFAS operates by allowing lenders to screen new loan applications against their database of fraud cases. In return, members provide CIFAS with details of known or suspected fraud cases. Consequently, not all cases on the CIFAS database will be actual fraud. This means that lenders should not automatically decline applications based on a CIFAS record being found, but rather that it should prompt a referral to an appropriately trained member of staff to investigate the case further become a final decision to accept or decline the loan is arrived at.

CIFAS members can access the National Fraud Database directly from CIFAS as a batch service or on a case-by-case basis. Alternatively, CIFAS data can be accessed via a range of anti-fraud tools provided by third party suppliers. This includes the option to receive a CIFAS warning flag via a standard credit search with one of the three main UK credit reference agencies. If the CIFAS flag is set on the customer's credit report, then this drives a more detailed investigation into the case.

CIFAS also maintains a “Protective Register” of individuals who have been the victims of fraud or think that they may be more at risk. For example, they have had documents stolen, or they know that an institution that holds their personal data was hacked and therefore the hackers could have their personal details. Anyone who thinks they may be at risk of financial fraud can (for a small fee) provider their details to the register. This means that when a credit application is made in their name, lenders will undertake additional checks to ensure that the application is not fraudulent.

CIFAS also maintains a staff fraud database, to allow new staff to be vetted for previous fraudulent behaviour. ￼

5.2.2 National SIRA

Like the National Fraud Database maintained by CIFAS, National SIRA is a database of fraudulent cases provided by its members, that loan applications can be screened against, but is run on a commercial basis. SIRA is one service provided by Synectics Solutions Ltd.

In addition to maintaining SIRA, Synectics Solutions also provides fraud scoring and a range of bespoke solutions tailored to the needs of specific clients.

5.2.3 National Hunter

National Hunter is another not-for-profit member-based fraud prevention agency. Hunter works a little differently from CIFAS and SIRA in that it generates fraud alerts based on matching information between a current loan application and previous loan applications.

Members of Hunter upload details of all new loan applications that they receive. When a customer makes a new loan application, their details are compared to other loan applications that the customer has made in the past and any significant discrepancies are reported. This will include things like their income, employment status, time living at current address and so on. For example, if a customer says that have lived at their current address for 10 years, but on a previous loan application they made a few weeks ago they said they had only lived there 3 years, this might trigger an alert.

5.2.4 Internal data (previous fraud cases)

Where a lender has identified previous cases of suspected fraud, good practice is to maintain these as a list against which new applications can be screened against. Good practice is to automatically decline repeat cases of attempted fraud.

Lenders should also screen new applications against current and previous applications to prevent a single individual obtaining many loans in a short period of time (velocity checking).

5.2.5 Predictive models & fraud scoring

Screening approaches such as CIFAS and SIRA are very useful fraud prevention tools. However, they rely on there being previous incidences of fraud relating to the loan applicant. Therefore, they will not prevent fraud the first time it occurs in relation to a specific individual. Consequently, best practice in fraud prevention is to combine screening methods with predictive methods that aim to identify high risk cases with no existing fraud indicators which can then be investigated more fully.

In the Lending Policy (Credit Risk) Component of the Good Practice Lending Guide, credit scoring was described as a way of representing the default risk of a customer as a credit score. The credit score then forms one of the key pieces of information that lenders use when deciding to accept/decline a loan application. Fraud scoring follows the same principles as credit scoring. Only in this case, the score predicts how likely a loan application is to be fraudulent.

Fraud models are constructed using much of the same type of data as credit scoring models, but also incorporate data about customer behaviours that are unusual or lie outside the normal range, particularly certain combinations of data. For example, it's not unheard of for some people to have salaries exceeding £150,000. Likewise, it's not unusual for people to live in deprived areas in northern towns. However, these two things together are unlikely[11]. Therefore, this is a potential indicator that would contribute to someone receiving a high fraud score. Similarly, someone who is relatively young (say <25) earning this type of salary would also be potentially fraudulent.

Like credit scores, fraud scores don't provide a concrete outcome. Only a measure of likelihood. Therefore, if someone receives a high fraud score, good practice to ensure good customer outcomes is to refer the case and conduct further investigation as part of an enhanced due diligence process.

When implementing a fraud score, a lender will need decide on the relevant thresholds to apply based on the trade-offs that different thresholds yield. If the fraud score thresholds are extremely strict, resulting in a high proportion of loan applications being referred for investigation, then nearly all cases of fraud will be detected. However, this will be very resource intensive, and a substantial proportion of case will turn out not to be fraudulent. At the other end of the spectrum, if very few cases are referred for investigation, then a high proportion of these will be fraudulent, but a lot of fraud cases will be missed because they don't score highly enough.

For all except the very largest organisations, most lenders don't have enough cases of proven fraud to be able to construct reliable fraud models themselves. Instead, most fraud models are developed by Credit Reference Agencies or the custodians of national fraud databases who have tens of thousands of fraud cases to work with. Lenders then obtain fraud scores via a suitable API that links to their application

[11] ie this is probably first party fraud, with the customer inflating their real earnings on their application form.

processing system. If a fraud score is being provided by a Credit Reference Agency, then the fraud score may be supplied as part of the credit search undertaken during the application.

Fraud scores can be very effective on their own, but lenders will usually use them in conjunction with fraud screening services, such as those provided by CIFAS or Synetics Solutions.

6 Dealing with cases of suspected fraud

6.1 Processing of fraud cases

There is no right to credit. A lender can decide to decline a customer's loan application for any reason they like as long it this doesn't breach equality and anti-discrimination laws[12]. Therefore, if any indicators of fraud exist, a lender is within their rights to decline the customer's loan application based on those indicators alone.

However, many cases of suspected fraud are just that, suspected. They are not proven, and it can't be taken for granted that an application is fraudulent simply due to a match with an external fraud database such as CIFAS or because the customer has a high fraud score. Consequently, when fraud is suspected, good practice, which supports good customer outcomes, is for the case to be subject to further investigation (enhanced due diligence) before a final decision is made. This is particularly relevant where the customer has raised a fraud warning themselves, such as by registering themselves with the CIFAS database.

This means that fraud investigation expertise needs to be maintained within the underwriting function, or as a separate standalone fraud investigation team. Typically, fraud investigation will involve obtaining additional information from the customer to be able to confirm their identity and that the information they provided on their application is correct. Sometimes this may involve speaking to the customer directly on the phone or asking them to come into branch and bringing additional documentation with them. For example, seeking character or employer references to confirm employment, or undertaking obtaining further verification checks from a third-party provider.

[12] For example, declining based on gender or race, or characteristics that act as proxies for these characteristics.

6.2 Oversight, monitoring and reporting

6.2.1 Oversight

As specified in the FCA's Financial Crime Guide, lenders should appoint a Money Laundering Reporting Officer (MLRO) who is responsible for the oversight of the organisation's anti-money laundering operations. This includes ensuring that robust customer verification and KYC procedures are in place.

KYC checks are required when a customer applies for new products, but also on an ongoing basis to identify and manage unusual financial transactions. For examples, multiple large deposits and withdrawals from a customer's account in a short space of time is a common indicator of money laundering activity. Similarly, a customer may not be on a PEP or sanctions list when they first enter a relationship with the lender but may be added later, requiring appropriate action to be taken at that time.

The MLRO should also have responsibility for reporting the status of the organisation's AML activities through to the appropriate management forum (such as the Board or a delegated sub-committee such as risk committee) and the regulatory authorities.

The MLRO should be sufficiently experienced and independent to be able challenge the business when appropriate to do so and should report directly into the board or senior management (a board member).

6.2.2 Reporting to the police and national crime agencies

Money-laundering is a criminal act. Where a firm detects or suspects a case of money laundering, they are required[13] to file a Suspicious Activity Report (SAR) with the National Crime Agency.

Fraudulently obtaining a loan is also a crime. However, there is no legal requirement for organisations to report individual fraud cases to the police or other authorities and many organisations do not report loan application fraud unless it is part of a larger organised criminal undertaking[14]. This is because of the cost of pursuing cases, low conviction rates and the limited recoveries when someone is convicted means it's not worth their while. Where organisations do undertake legal action, it is usually civil action through the courts to recover funds via a court judgement. This is in similar a manner to the way that normal debts are recovered through the courts if a customer becomes seriously delinquent.

[13] This is a requirement of the Proceeds of Crime Act (2002) and the FCA (Financial Crime Guide, Section 3.2.10)
[14] For example, if several hundred fraudulent loan applications were all made as part of a single coordinated fraud attempt.

6.2.3 Regulatory reporting to the FCA

The FCA requires regulated firms to submit an Annual Financial Crime Report[15] detailing instances of financial crime that relate to money-laundering. This includes the reporting of PEPs and Sanctions cases.

Credit unions are exempt from this requirement.

[15] FCA Handbook SUP 16.23

7 Appendices

7.1 Appendix A: Glossary of terms used in this document

Term	Description
CIFAS	CIFAS is the Credit Industry Fraud Avoidance Scheme. It is a not-for-profit organisation that maintains the National Fraud Database of known or suspected fraud cases. Members of CIFAS can then screen their customers against the CIFAS databases to identify potential fraud.
Credit Reference Agency (also known as a Credit Bureau)	An organisation, licensed under the Consumer Credit Act 1974, to hold information about individuals' repayment behaviour when using credit products such as mortgages, loans, and credit cards. Nearly all UK-based Lending institutions provide details of the balances and arrears status of their customer accounts to one or more of the UK credit reference agencies each month. When a new customer applies for a loan, a lender will purchase a copy of the customer's credit report from the CRA, which details the balances and arrears status of the customers current and previous loan agreements with other lenders. The 3 main credit reference agencies in the UK are Experian, Equifax, and TransUnion (formally CallCredit).
Credit Score	A credit score is a number which provides a holistic view of a customer's creditworthiness based on several different features (characteristics). Typically, these are a mixture of geo-demographics (eg age, occupation, residential status) and financial history (eg number of existing credit agreements, credit card utilisation, defaults, and court judgements). Credit Reference Agencies each provide their own credit scores and the scores differ between agencies due to the different data and methodologies used to create them. Individual lenders often develop their own Credit Score(s), which are tailored to their

Term	Description
	customer base and may incorporate additional data sources that they have available.
Credit Scoring	An algorithm (mathematical formula) that creates a credit score for an individual by assigning weights to the different pieces of information that is known about them.
Financial Conduct Authority (FCA)	This is the regulatory body responsible for the functioning of the UK financial markets. This includes the regulation of firms providing consumer credit products and services.
Fraud Scoring	Similar in principle to credit scoring, A fraud sore is a number which provides a holistic view of a customer's propensity to be a fraudster or to be the victim of fraud (ie a fraudster is using another person's identity. The scores are based on factors that are shown to correlate to fraudulent behaviour such as large or unusual financial transactions that are out of keeping with the normal behaviours exhibited by the customer.
Joint Money Laundering Steering Group (JMLSG)	The JMLSG produces guidance (JMLSG Guidance) to assist those in financial industry to comply with their obligations in terms of UK anti money laundering (AML) and counter terrorist financing (CTF) legislation and the regulations prescribed pursuant to legislation.
Know Your Customer (KYC)	Know your customer checks cover the due diligence that financial (and other) organisations must undertake to ensure that they know who their customers are. KYC processes are primarily required to comply with UK's anti-money laundering laws. Having good KYC practices in place also supports fraud prevention but creating barriers to fraudsters using false names and other fictitious information.
Money Laundering	The act of passing money gained by illegal means through the financial system to generate "clean" money that appears to have come from a legitimate source.
Money Laundering Reporting Officer (MRLO)	An individual appointed by a firm to oversee its anti-money laundering processes and procedures. All FCA regulated firms are required to have an MRLO.

Term	Description
Open Banking	Open Banking refers to customers who have given permission for lenders to review the transactions that occur in relation to their bank account(s). This enables the lender to verify the customer's income and expenditure patterns.
Politically Exposed Person (PEP)	This is a prominent figure, sometimes but not always in the public eye. Examples in the UK are senior politicians and heads of prominent institutions, and potentially their associates. PEPs are deemed to be high risk due to the nature of the roles they undertake, making them potential targets for bribery, corruption, and fraud. Dealing with PEPs requires a higher level of due diligence than for standard customers. For example, confirming that their assets come from legitimate sources. There is no singular definition of what defines someone as a PEP, but most countries base their definitions on the recommendations of The Financial Action Task Force (FATF).
Principles of Reciprocity	These are the rules that are determined by the Standing Committee on Reciprocity (SCOR) as to how lenders share and use data via a credit reference agency.
Prudential Regulatory Authority (PRA)	The PRA is a part of the Bank of England and is regulatory body responsible for ensuring the soundness of the UK financial system. For example, ensuring that companies hold enough capital reserves and have sufficient liquidity to remain solvent.
Policy Rule	A clear statement of a lenders criteria for lending. Usually, a set of clear Policy decline rules are used within the lending policy to identify specific high-risk cases, such as bankrupts of those with serious arrears, which should never normally be granted a loan.