SAFECAPITAL

Open Banking for AML and Fraud Prevention in Law Firms

Reducing the dual threats of money laundering and payment fraud with open banking

www.safecapital.co.uk

v1.1 - May 2024

Table of Contents

CONTENTS

p1.
INTRODUCTION

p2.
FRAUD RISKS FOR LAW FIRMS

p5.
MONEY LAUNDERING RISKS

p6.
CLIENT MONEY RISKS

p8.
OPEN BANKING

INTRODUCTION

Open banking is a new and innovative way for individuals and businesses to securely make payments and share bank account information. For law firms, open banking can help reduce the risks of payment fraud and money laundering as well as reduce friction when taking and making payments.

In addition, open banking provides an opportunity for law firms to streamline, better secure and simplify the payment process for their clients - making life easier for the accounts team and also helping with regulatory compliance around client money.

In this white paper, we discuss the current risks facing law firms around fraud and money laundering, before looking at how open banking can help.

FRAUD RISKS

FRAUD RISKS FOR LAW FIRMS

> *"Cybercrime is now the most prevalent crime in the UK ... law firms are an obvious target. It is the job of firms to take steps to protect themselves and their clients' money."*
>
> SRA - Cybercrime Risk

In recent years, there has been a significant increase in fraudulent financial activities, especially when it comes to Authorised Push Payment (APP) fraud - when a criminal tricks someone into sending money directly from their bank account to an account which the criminal controls.

UK Finance recorded over 230,000 incidents of APP fraud last year^, with losses totalling £459.7 million. Law firms are an obvious target for criminals, due to the large sums of money that are often moved into and out of a firm's client account - especially in property transactions.

PAYMENT FRAUD IN CONVEYANCING

> *"High-value transactions, such as conveyancing, are more likely to be targeted by means such as email modification fraud."*
>
> SRA - Risk Outlook

Conveyancing matters are seen as a particularly lucrative target for fraudsters, due to the time pressures to complete a property transaction on a given day. This has led to multiple incidents of Friday Afternoon Fraud occurring - whereby criminals try to divert deposits or completion monies when conveyancing transactions are completing, often on Friday afternoons.

^ UK Finance Annual Fraud Report 2024

FRAUD RISKS

PAYMENT FRAUD IN OTHER SERVICES

"Although conveyancing remains a frequent target, due to the large funds involved, criminals are broadening their attacks to other fields as well."

SRA - Risk Outlook report: information security and cybercrime in a new normal

Whilst conveyancing fraud cases are often the stories that hit the headlines, the Solicitors Regulation Authority (SRA) has highlighted that criminals are broadening their attacks to other fields as well. SRA scam alerts show a range of scam attempts outside of conveyancing, including debt recovery, landlord and tenant, estates/inheritance, immigration, class actions and even offering legal assistance to victims of online fraud.

PAYMENT FRAUD ATTACK VECTORS

In most cases, criminals target the client rather than the firm because they are less likely to be aware of the risk of payment fraud. The most common attack is where the criminal poses as the law firm, and tries to provide clients with a new set of bank details for the firm, which actually belong to the criminal.

There have been incidents of finance teams also being targeted - for example a criminal pretends to be a client pulling out of a property purchase, and asking for their deposit back urgently.

Attacks are most commonly initiated by email, and generally fall into two categories:

- **email modification fraud** - whereby a criminal has gained access to the email account of the client or the law firm, and then uses that access to modify emails and provide a different set of bank details for funds to be sent to.

- **email spoofing** - where an email looks like it came from the law firm but didn't. This can either be because the firm has inadequate safeguards in place to prevent their email address being spoofed, or because a criminal has set up a new email address that looks very similar to the one used by the law firm.

FRAUD RISKS

Historic SRA scam alert data shows that there are over five attempts per month on average, where criminals attempt to supply false bank details to either a firm or their clients. There are likely more attempts that evade detection.

ARTIFICIAL INTELLIGENCE & PAYMENT FRAUD

The rise in the availability of a range of Artificial Intelligence (AI) tools has been a boon for criminals, when it comes to impersonating others and undertaking payment fraud attempts.

The past year has seen a range of AI tools become widely accessible, which criminals are now able to use to make themselves look, sound and write like other people.

Writing Tools

Tools such as ChatGPT make it easier for fraudsters to draft well written letters and emails, which look like they could have come from a law firm. When coupled with the ability to spoof email addresses, recipients can easily be tricked into believing the email contents.

Voice Cloning

There are a wide range of tools available that enable a person to change their voice so they sound like someone else. All that is needed is a few seconds of a recording of someone's voice, in order to create a voice clone.

Deep Fake Video

We are on the cusp of seeing believable video impersonation fraud attempts using deep fake video tools. Leading firms are now rightly concerned about the potential for deep fake video calls targeting their clients and their own teams too.

In a recent risk assessment the SRA also highlighted deepfakes as a risk that law firms need to aware of.

> *"[deepfakes] increases the risk of relying on video calls to identify and verify your client."*
>
> SRA Sectoral Risk Assessment - AML and Terrorist Financing, March 2024

AML RISKS

MONEY LAUNDERING RISKS

"If you display your client account details freely, for example, on your letterhead or a website, the risk of them being abused by criminals is greatly increased. This is something you should avoid."

LSAG: AML Guidance for the Legal Sector 2023: Section 5.6.3.6

Unfortunately, fraud is not the only risk firms face in relation to payments. Money launderers are targeting law firm client accounts as a way to clean up dirty money.

As a result, the SRA advises against including client account information in engagement letters. The Legal Sector Affinity Group (LSAG) suggests that details should not be included on a firm's letterhead or website, and the Law Society of England & Wales advises that circulation of bank details is kept to a minimum.

If the disclosure of bank details is too widespread, it makes it easy for money launderers to obtain a copy of the details and send money to the firm. They then ask for the money back, cleaning it in the process.

CLIENT MONEY

DUTY TO PROTECT CLIENT MONEY

> *"Conveyancing fraud can see people lose their life-savings. We ... want to see firms making sure their clients are aware of the risks."*
>
> SRA - Cybercrime Risk

All law firms have a duty to protect client money. Therefore, understandably, payment fraud resulting in the loss of client funds is a regular feature in the SRA's risk outlook for law firms.

Common themes include firms needing to have a system in place to manage the risk of email modification fraud, as well as making sure their clients are aware of payment fraud risks.

Similarly, the Council for Licensed Conveyancers (CLC) maintains that it is important that practices take all reasonable steps to protect themselves and their clients from fraud.

Thankfully, most law firms are now aware that emails can be intercepted. As a result, most firms follow best practice and proactively warn their clients that bank details will never be shared by email or changed during the course of a transaction.

With email identified as a high risk for sharing bank details, firms have moved to other ways of sharing bank details with their clients. Whilst sharing bank details by SMS or over the phone is an improvement to using email, there is the potential for criminals to mimic that behaviour and share false bank details in the same way too.

For this reason, firms often rely on sharing bank details with their clients at the start of a case, through an initial engagement letter sent by post.

CLIENT MONEY

RETURNING CLIENT MONEY

> *"You ensure that client money is returned promptly to the client, or the third party for whom the money is held, as soon as there is no longer any proper reason to hold those funds."*
>
> SRA Accounts Rules: Part 2 - Client money and client accounts - Rule 2.5

As discussed in the payment fraud section, there is a risk to law firms of criminals contacting the firm whilst posing as their client, and providing bank details for funds to be returned to.

For high value transactions (for example the proceeds of a property sale), the risk is far greater, and as such there is broad consensus between the CLC, Law Society of England & Wales and the Conveyancing Association (CA) that firms should obtain bank account details for their clients at the outset of a transaction. They can then be retained on file for use if and when money needs to be returned.

In addition to the need to return client money promptly, regulators are taking a closer look at what firms are doing to return residual balances to their clients. Due to interest rates now running at over 5%, law firms are going to come under greater pressure from regulators to return client money promptly rather than potentially earn interest on it themselves.

Many firms do not have robust processes in place for obtaining client bank details, which makes it difficult and time consuming to return money easily when needed.

OPEN BANKING

WHAT IS OPEN BANKING?

Open banking allows customers to safely and securely make payments to, or share account information with, third parties - directly from their own bank. The third party does not gain access to the customer's bank login details or passwords.

For account information, the third party is only granted access to the information that the individual has chosen to share. In the case of payments the third party requests an individual to authorise a payment, with the destination account for the payment, along with the payment amount populated automatically.

The user journey that customers go through takes place within the comfort and secure environment of their own bank's mobile or online banking app. Because of this familiarity, customers trust the process taking place.

WHO SUPPORTS OPEN BANKING?

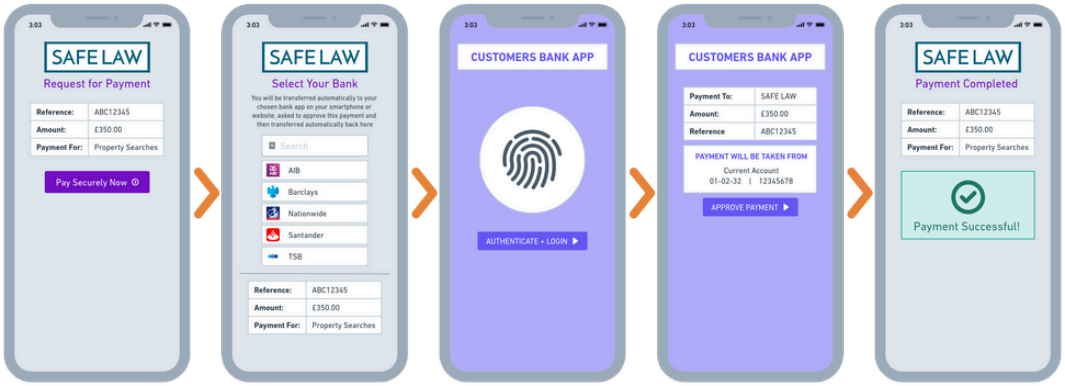
In the UK, implementation of the open banking framework has been overseen by Open Banking Limited, and is supported by the UK's big four banking groups (HSBC, Lloyds, Natwest and Barclays). The vast majority of UK banks are now part of the open banking network, which means that clients of those banks can use open banking services. There are a limited number of banks that do not currently support open banking - e.g. Metro Bank.

OPEN BANKING

WHO CAN USE OPEN BANKING?

Any individual (or business) with online/mobile banking access to a UK bank account should be able to use open banking. With over 93% of the UK population now using online banking, the vast majority of UK adults can now undertake open banking activities.

OPEN BANKING - PAYMENTS



Open banking facilitates direct transfers of funds from one bank account to another, without the need for the individual initiating the payment to manually enter the recipient's bank details or the payment amount.

BENEFITS TO LAW FIRMS

"Avoid disclosing your client account details until you are ready to accept a payment/transfer and discourage clients from passing the details on to third parties."

LSAG: AML Guidance for the Legal Sector 2023: Section 5.6.3.6

Because the bank details used for open banking payments are populated automatically, this removes the need for client account details to be shared before a payment is required.

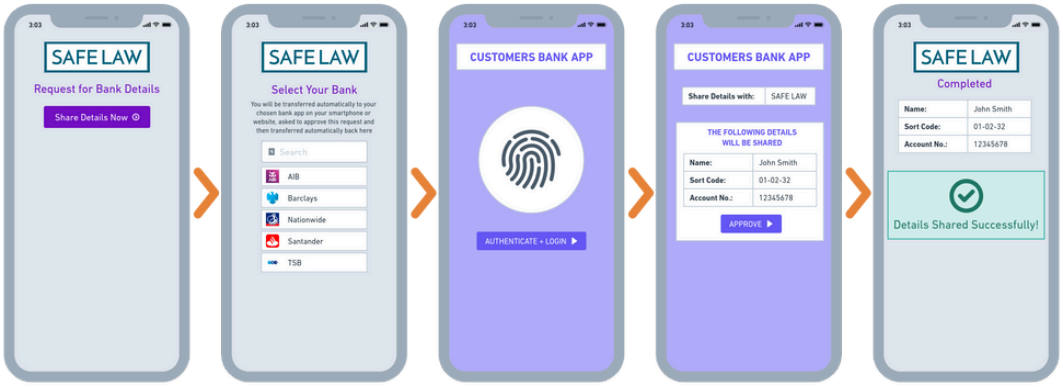
This reduces the risk to clients of accidentally entering the wrong account information (or being tricked by a criminal into doing so). The risk to the firm of their own bank details ending up in the hands of money launderers, or being passed onto third parties is also reduced.

OPEN BANKING

Firms can avoid unexpected payments, as the client cannot transfer any money until the firm initiates a payment request. Once the payment is made, funds usually arrive in the firm's client account within seconds.

When payment is made, the payment reference and amount can also be populated automatically. This makes reconciliation much easier for the accounts team.

OPEN BANKING - ACCOUNT DETAILS



An individual can choose to share bank account information, such as account details and transaction history with a company securely.

For financial services businesses this makes it easier to understand spending patterns and affordability before offering people lending products such as mortgages, loans and credit cards.

Account information can also be used to undertake source of funds checks in order to help combat fraud and money laundering.

BENEFITS TO LAW FIRMS

"Obtain evidence that the bank account is properly constituted as an account conducted by the seller for a period of at least 12 months."

Law Society Conveyancing Protocol - Stage A3 (Instructions - Seller)

OPEN BANKING

Through open banking services, law firms can obtain verified bank account details from their clients which are supplied directly from the client's bank.

By doing so, firms can ensure that the client has access to the account they are providing information for, and the firm can check that the name on the account matches the name of the client (or clients). The transaction history can also be checked, to ensure that the account has been active for at least 12 months, in line with current best practice.

This gives law firms confidence that they have the correct bank details on file for their clients, and enables them to easily make payments back to them. This, in turn, mitigates the risk of payments going to the wrong account through either human error or fraud.

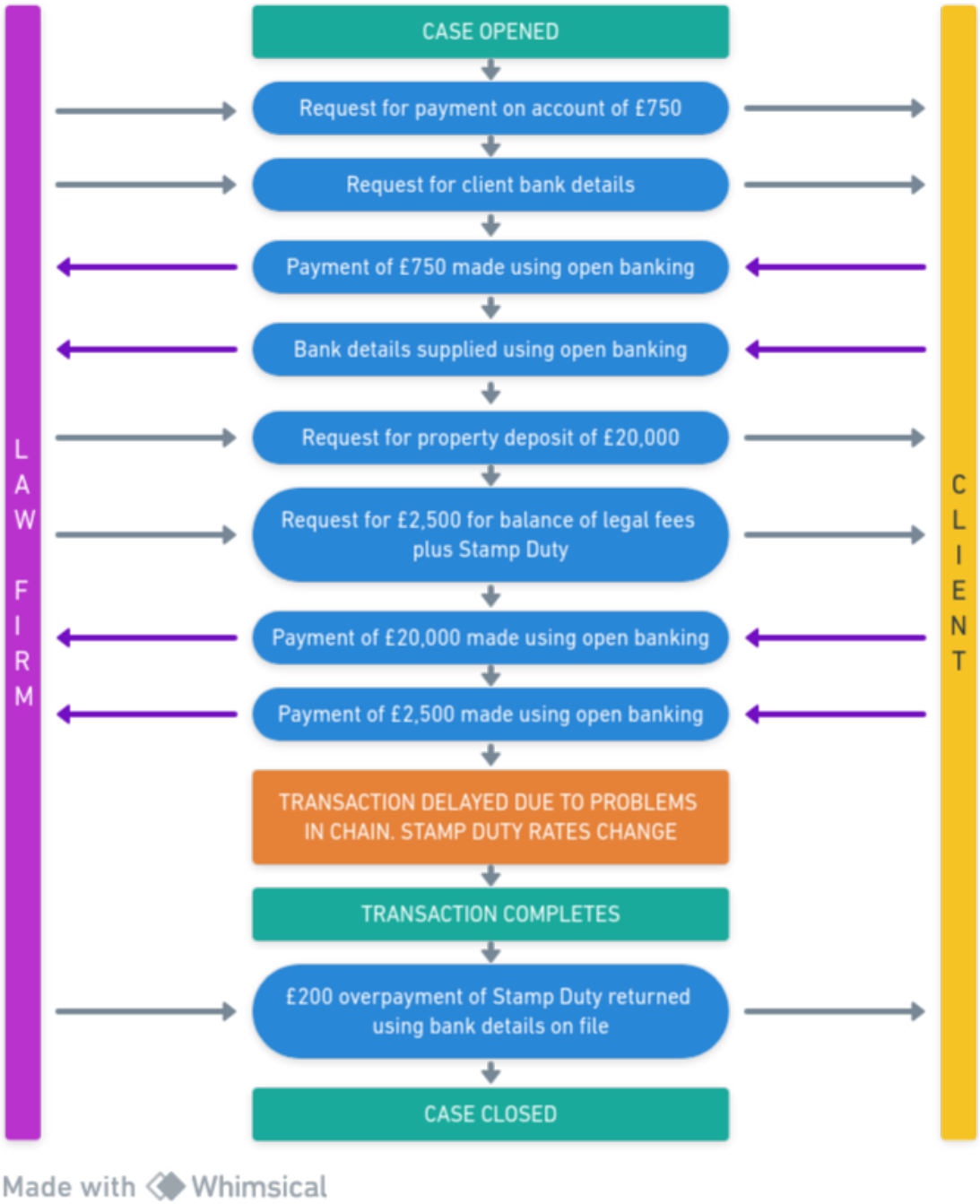
Law firms can use open banking to request bank account details for every client, at the outset of a transaction and in line with industry best practice.

This limits the risk of a criminal introducing false bank details into a transaction further down the line. It also makes it easy for the firm to return client money or any surplus at the end of a transaction, avoiding the build up of residual balances and demonstrating a commitment to their regulators to not hold onto client funds for any longer than needed.

OPEN BANKING

EXAMPLE CASE PAYMENT LIFECYCLE

The example below illustrates how open banking could be used to manage payments over the course of a property purchase transaction.



OPEN BANKING

OPEN BANKING - SUMMARY OF KEY BENEFITS FOR LAW FIRMS

- Payments are taken securely from clients without the need to share bank details upfront by post, phone, email or SMS.
- By explaining to your clients that you do not disclose bank details, the risk of payment fraud to your clients can be reduced.
- Payments can only be made once you request them, and once made are always for the correct amount and include the correct case reference - making life easier for your accounts team.
- By keeping bank details out of engagement letters you can reduce the chances of money launderers obtaining and using them.
- By obtaining bank details for each client upfront, in line with best practice, you can easily return funds or residual balances promptly if needed.

OPEN BANKING & SAFE CAPITAL

> *"Consider using a tool such as 'Safe Capital' to verify bank details before any funds are exchanged."*
> The Law Society Cyber Security Toolkit

Safe Capital enables law firms to obtain client bank account information and receive clients' funds safely, securely and quickly using open banking. Get in touch today to find out more.

Matthew Pennington
Director - Safe Capital
mp@safecapital.co.uk
www.safecapital.co.uk