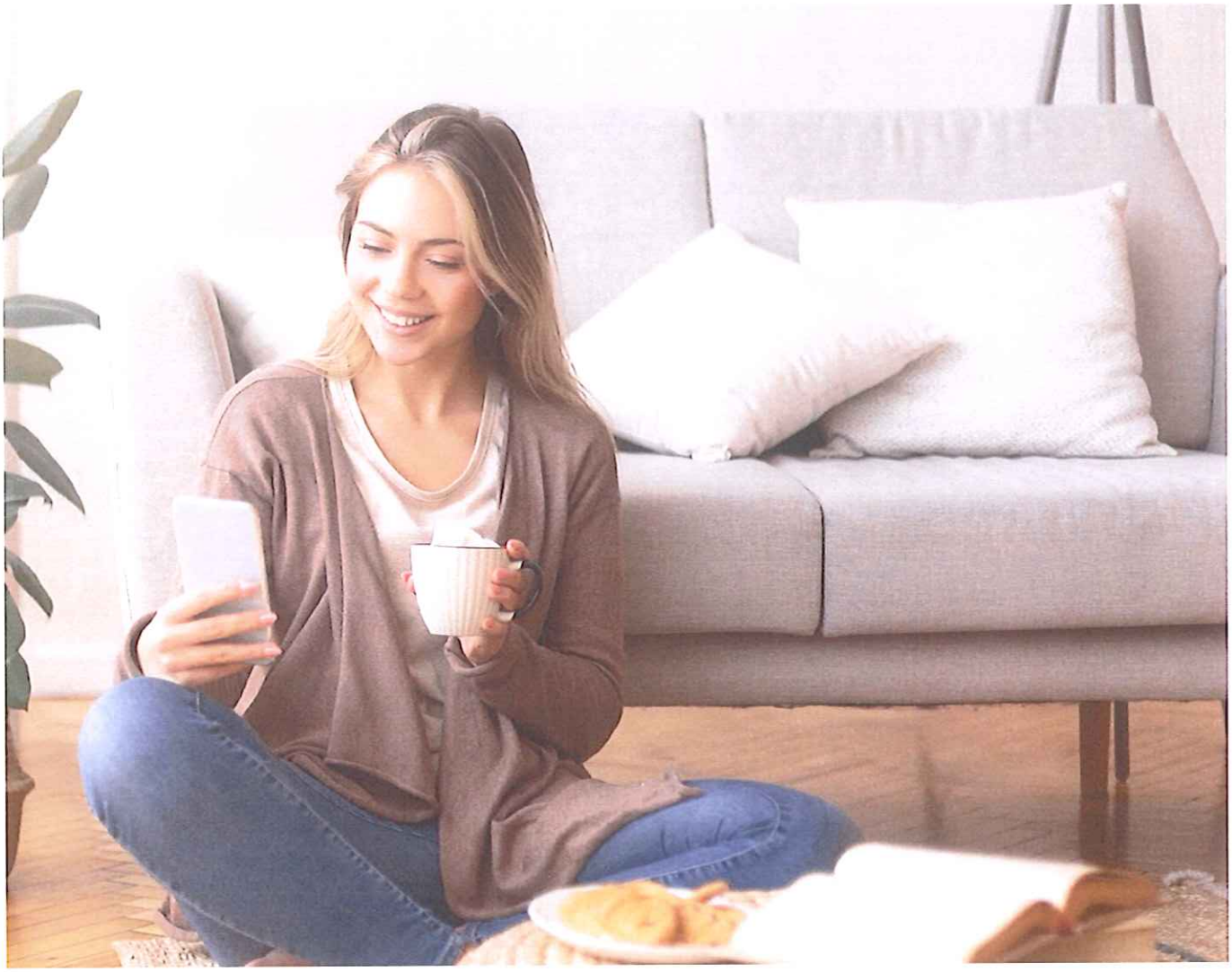
Guide

Your Guide to Using Thirdfort.



thirdfort

Guide to Thirdfort

Introducing Thirdfort

Certain companies are under a regulatory duty to verify your identity before acting on your behalf. This is so they know who you are and helps them combat money laundering to keep everyone's money safe.

Ordinarily, you would be required to take your identity documents to an office or send certified copies.

Thirdfort provides a new, safer way to do this using our ultra-secure app – making life easier for you and keeping your information safe.

Why am I being asked to use Thirdfort?
Companies are under a regulatory duty to make sure every client's identity is verified. Due to an increase in money laundering, providing original identity documents is not always safe or reliable.

Is Thirdfort safe to use?
Security of your information is Thirdfort's number one priority and we are trusted by thousands of people every week. We are regulated by the FCA and use state of the art security measures to keep your data safe. Find out how in the Security section of this leaflet.

How to use the Thirdfort App

To use Thirdfort, you will need your phone and a valid ID. Thirdfort accepts passports, driving licences and national ID cards.

Step 1: Download the Thirdfort app
Wait to receive a text message from Thirdfort with a link to download the app.

Step 2: Follow the instructions to sign up
We'll ask for some information such as your name, date of birth, email, phone number and home address you want to use with your account.

Step 3: Complete your tasks
Your home screen will display the tasks you need to complete in order to verify your identity. This could be all or any of the following depending on your transaction:

- **Identity check** – to help us confirm that you are who you say you are, we ask you to take a photo of your ID and a selfie video. We use this to validate your ID and confirm it belongs to you.
- **Bank statements** – we use Open Banking technology to retrieve digital statements direct from your bank. You can read more about this in the Security section of this leaflet.
- **Purchase funds** – this questionnaire must be completed when purchasing a property to help your professional understand where the funds being used to buy your property originate from.
- **Proof of address** – you may be required to provide photo evidence of your address, such as a utility bill, council tax bill or bank statement.

Tasks will disappear from your home screen once finished and Thirdfort will let you know when all of your tasks are complete. If we need any further information from you, we will notify you through the app.

Have a question?
You can check the FAQ section of the app

Security

Security and data at Thirdfort

We understand that sharing personal information using an app might seem scary. After all, we're usually being told to do the exact opposite! But as we move to a digital world, traditional methods of sharing information are unsafe. We have provided the following information to give guidance and comfort as to how Thirdfort works.

What is digital identity verification?

Digital identity verification lets you confirm who you are using technology. Businesses are increasingly moving processes online and digital identity verification is a natural progression, much like banks moving to 'online banking'. Electronic identity checks are proven to be a much safer way for you to verify your identity and you can use it from the comfort of your own home.

Why does Thirdfort want to access my bank?

When dealing with large transactions, companies are required to investigate the origin of funds under money laundering regulations. To do this, they may ask to see paper bank statements. Thirdfort enables you to provide these digitally using government backed Open Banking technology.

What happens to my data?

At Thirdfort we are serious about security. Thirdfort only temporarily stores your data while we carry out your checks. Once your checks are complete, we pass your data to the professional requesting it and permanently delete it from our database. We only retain your mobile number as a unique identifier of you. This is stored for two years so you can access your account and share data with other professionals in future if you wish. We can delete this on request.

Do you store my data after I complete my checks?

Thirdfort does not store all of your data. Instead, the majority of your data will remain stored locally on your mobile device. All we keep is your mobile number as a unique identifier which allows you to access the app and reuse your locally stored data in the future. If you don't want to store your data locally on your device, you can delete it at any time by deleting the Thirdfort app from your device. For further information, view our Privacy Policy at: www.thirdfort.com/terms/privacy-policy

Bank grade encryption
Thirdfort uses state of the art security measures, including end-to-end 256-bit TLS encryption used by all major banks to encrypt your data and ensure only authorised people are able to view it.

FCA regulated
Thirdfort is registered with the Financial Conduct Authority and adheres to European data protection laws. The FCA have conducted an in depth review of our security policies and we must demonstrate regularly that we protect client data and use state of the art security.

Cyber Essentials Plus
We are certified by the UK government cyber security accreditation scheme, Cyber Essentials Plus, who conduct an annual audit on our systems and processes.

GDPR compliant
We comply with the Data Protection Act 2018 and protect your data under EU law

ICO registered
We are registered with the Information Commissioner's Office under the Data Protection Act. Our registration number is A8225019.

Security at Thirdfort

Open Banking FAQ

Open Banking is the secure way to give regulated Third Party Providers secure access to your financial information. You can find out more at: www.openbanking.org.uk

What is a Third Party Provider?

A Third Party Provider is a regulated organisation that can, with your consent, access your account information in order to help you manage it. Thirdfort is an authorised Third Party Provider and regulated by the Financial Conduct Authority.

Does Thirdfort see my login details?

No. With Open Banking, your login details are safe, as you don't share them with us. The Thirdfort app will always direct you to your mobile banking app or your bank's secure Open Banking website which allows you to enter your credentials without us seeing them.

Is my information safe?

Open Banking uses application programming interfaces (APIs) to allow the software at one company to access information from the software at another company.

Unlike screen scraping, which is dependant on you sharing your login details with an app, APIs allow users to regulate the data they share, with whom and for how long without ever sharing password information. This means you can control what information you share via Thirdfort and you can easily revoke access.

Only Third Party Providers that are highly regulated are permitted access to Open Banking APIs. Thirdfort is regulated by the Financial Conduct Authority. As part of our registration we are obliged to be careful with your data and be open and honest about how we use it. You can visit the FCA website (www.fca.co.uk) to check that we are registered and authorised to carry out relevant activities.

What if Thirdfort gets hacked?

Thirdfort doesn't store any of your banking credentials. This means that your bank account cannot be breached at any time, even if our servers get compromised.

Want to ask us something?

You can contact us at:

help@thirdfort.com

020 3948 1271