Fourthline

The 2025 Fourthline Fraud and Authentication Report

Fourthline surveyed 6000 consumers across six European markets (France, Germany, Italy, the Netherlands, Spain, and the UK), asking them about their experiences and attitudes relating to banks, fraud, KYC, and authentication.

This report explores the survey findings, accompanying them with insights from Fourthline experts to help banks understand consumer sentiment and deliver the best possible KYC and authentication experiences.

Banks: trust and the digital–traditional divide

Digital-only banks experience faster growth, but traditional banks still dominate. A small percentage (8%) of consumers exclusively use digital-only banks, while over a quarter (27%) use both traditional banks and digital-only banks.

Our data shows that older customers tend to prefer traditional banks. 74% of people aged 55 and over use only traditional banks, compared with just 5% using exclusively digital-only banks. It also shows that Europeans have a high level of trust in banks. They trust them to handle finances in a secure way and to have their best interests at heart.

66%

use a traditional bank, compared to 8% who use a digital bank, and 27% who use both

82%

trust their bank to handle finances in a secure way, while only 9% say they distrust banks

69%

trust their bank to have their best interests at heart, while only 15% don't

Trust is earned not given

These positive findings regarding trust in banks reflect years of building relationships and looking after customer finances. They are also a tribute to the work of regulators, who ensure a fair and stable market. However, even the smallest erosion of trust can have severe consequences, both in terms of customer loyalty and regulatory scrutiny. As technology evolves and new threats emerge, banks must stay proactive in how they manage the risks that could affect this trust capital – such as fraud.

Fraud: experiences, attitudes, concerns

A significant percentage of Europeans have been the victim of fraud, and an even greater percentage are worried about the speed at which fraud is evolving. Consumers are also concerned about the newer types of fraud that are emerging with AI.

19%

have been the victim of fraud. This is higher among customers of digital-only banks (27%) than traditional banks (16%).

57%

are worried that fraud is now more sophisticated than ever.

49%

are worried about AI fraud and deepfakes.

26%

trust the EU GDPR to protect their data rights, while 34% in the UK trust the UK GDPR.

Older generations are more concerned about fraud than their younger counterparts. 62% of people aged 55 and over say they are worried about its sophistication, compared to just 46% of people aged 18–34. However, despite their comparative lack of concern, younger people are more likely to have been a victim of fraud (26%) than those aged 55 and over (14%). This counterintuitive difference is also reflected when we compare customers of digital-only banks and traditional banks. Customers of digital-only banks are more likely to have been victims of fraud, but only 47% of digital bank customers are worried about it, compared with 57% of traditional bank customers. The key takeaway here is that fraud is a concern for all age groups and consumer groups.

Fraud is a big threat to customer relationships

In addition to the immediate cost of supporting a customer through an incident of fraud, there is also a risk to the customer–bank relationship. According to a PYMNTS Intelligence report published in October 2024, most victims of fraud at least consider switching financial institutions after the incident is resolved and an estimated 30% actually do so.

"While overall trust in banks remains high, consumers are concerned about how fraud is evolving. It is not enough for banks to ensure that they maintain that level of trust, they must also communicate with their customers about how they are proactively protecting customers against fraud."

Krik Gunning

Co-founder and CEO of Fourthline

KYC and re-KYC: attitudes and preferences

One important way to tackle fraud is through robust customer onboarding and data maintenance processes – i.e. KYC and re-KYC. But there is more than one approach to these processes to consider.

Despite the growing trend for using digital tools for many daily tasks, most survey respondents are wary of online KYC processes. This is likely due to concerns around security and fraud being reinforced by advice not to share sensitive data online. The only KYC method met with the approval of a majority of consumers is in-person verification, which carries its own security challenges since the human eye is not as accurate as AI tools in checking for authenticity.

52%

prefer in-person verification, which rises to 60% among customers of traditional banks, but is only 30% for customers of digital-only banks.

18%

are open to submitting a scanned copy of their ID document through their bank's website or app.

16%

are open to sharing a photo or video holding their ID document.

10%

are open to emailing an electronic image of their ID document.

12%

of German customers are open to having a video call with a bank representative *(see 'About video verification in Germany')*

About video verification in Germany

In 2015, Germany became the first country in Europe to introduce video identification procedures for remote customer identification. The initiative was led by the German Federal Financial Supervisory Authority (BaFin), which introduced comprehensive standards for video identification.

Video identification has become the standard for digital onboarding in the market and has seen widespread adoption. However, as criminals become more technologically savvy, financial institutions need to create more technical controls to counter these risks, something not always easy when a human is involved.

We can draw several conclusions from these statistics.

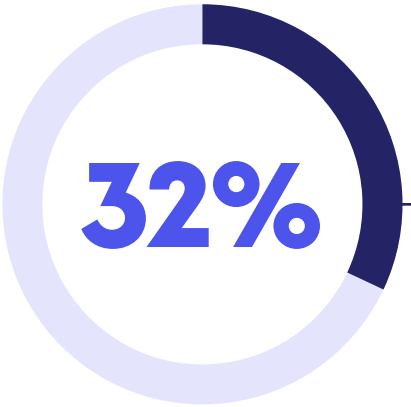
First, there is a clear difference between customers of traditional and digital-only banks. While the former prefer in-person verification, customers of digital-only banks are consistently more open to digital KYC processes.

Second, there is a difference among age groups. Where 60% of respondents aged 55 and over prefer in-person verification, this drops to 46% for those aged 18–34.

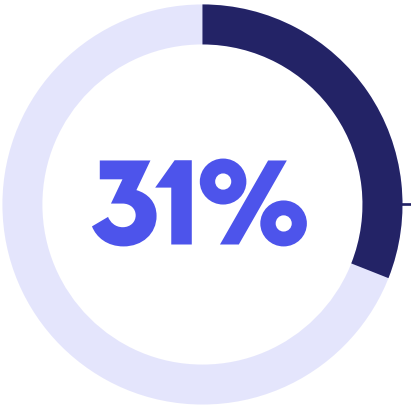
And third, there is a difference among markets. Consumers in the UK tend to be more open to digital KYC processes than their counterparts in mainland Europe, with only 41% of British consumers preferring in-person verification. In addition, British consumers are more open to sharing ID documents digitally, including in video checks. When separating respondents by nationality, we found that German consumers are at the other end of the spectrum. They are consistently least likely to share their ID digitally, be it through submitting a scanned ID document through a bank's app or website, sharing a selfie photo or video holding their ID document, or emailing a photo of their ID.

Attitudes towards re-KYC

Re-KYC is an important part of banks maintaining their legal and regulatory obligations. It's also a tool to mitigate the risk of fraud, though it isn't widely used. Almost an equal number of survey respondents have (42%) and have not (44%) been through a re-KYC flow, and although they tend to view re-KYC as a positive thing overall, respondents were not wholly open to the idea.



have had to repeat the KYC process and say that it made them feel more secure. Only 10% say they found it very annoying.



have not been through a re-KYC process but would be willing to. 13% have not been through re-KYC and say they wouldn't want to.

How to approach KYC and re-KYC

Although many consumers still prefer the in-person experience, digital KYC and re-KYC processes are not nice-to-haves. In a digital-first world where the number of physical bank branches is declining, both traditional and digital-only banks need to adopt digital KYC and re-KYC processes. The question is not 'if', but 'how'.

The data implies two things. First, the tools and processes that banks introduce need to combine trust-building, bank-grade security with a frictionless user experience. This will help ensure that customers who are skeptical about digital verification will embrace it.

Second, banks need to educate their customers on why digital KYC and re-KYC processes are safe. This is particularly true for older customers and those who exclusively use traditional banks in markets such as Germany, where the current preference for in-person verification is even higher. But it's no less important for digital-only banks in markets such as the UK. Although consumers tend to be much more open to digital KYC flows, they may mistake legitimate re-KYC notifications for phishing attempts. Customers of digital-only banks can't turn to face-to-face customer service to verify such notifications. Their banks must therefore invest in educating them about re-verification, including why it is necessary for account security and regulatory compliance.

"While in-person KYC is the most popular and intuitively feels like it should be secure, it is actually less secure than some digital alternatives, where hundreds of real-time checks can be performed to pick up inconsistencies that humans can't."

Ralph Post

CTO of Fourthline

Authentication: attitudes and preferences

Due to concerns around fraud there is strong support for authentication among consumers in all markets. There is also support for the idea that authentication makes them feel in control of their data security.

Biometric authentication is widely regarded as the most secure method. This is true across all markets, and even more pronounced among customers of digital-only banks (68% compared with 61% of traditional banks), younger people (71% of 18–34-year-olds, compared with 59% of those aged 55 and over), and those who trust banks (67% compared with 58% of those who say they distrust banks).

PIN, password, and security questions are viewed as less secure across all markets. For instance, just 36% of people in Italy think security questions are secure, and 40% of people in France feel the same way about PIN. If we accept that younger people and customers of digital-only banks represent the trend for consumers as a whole, then we can see the market is steadily moving in favour of biometrics as the preferred method of authentication.

However, despite widespread belief that authentication processes are easy and that biometric authentication is the most secure option, many consumers would prefer to choose which method to use.

86% agree that they understand why the authentication methods used by their bank are necessary, and only 4% disagree.

73% say authentication makes them feel in control of their data security, while only 7% disagree.

78% would like to be able to choose which authentication method they use, while only 6% wouldn't.

78% say their bank's authentication process is easy to use.

65% say biometric authentication is the most secure method, a figure that rises to 76% in the UK.

59% of respondents don't think biometric authentication is safe because they think it's easy to fake, and a further 50% worry their biometric data might be stolen.

How to approach authentication

Banks need to choose authentication methods that balance security and usability. Not only is this a challenge, but the definition of what is secure can change as new threats emerge.

Multi-factor authentication with a biometric security process is the best approach. However, it remains important for banks to keep a close eye on security protocols and be prepared to adapt in response to new threats. Furthermore, as many consumers have expressed a desire to choose the authentication method they use, providing them with some carefully selected options to tailor their flow can help improve the experience without compromising security.

Not all authentication tools need to be built and managed in-house. In fact, there is a strong case to be made for partnering with proven third-party solutions. These tend to provide superior user experiences and solve edge cases better than in-house solutions can, as they must adapt to emerging fraud trends and solve the same authentication challenges at scale across a wider range of use cases than any single bank. They are also often more cost-effective since no valuable in-house resources are required to build and maintain the solution.

"Fraud is an ongoing game of cat and mouse, where fraudsters have the advantage since they are always able to pick up new technologies and experiment with them immediately without regard for laws or ethics. Banks have a wide range of challenges to think about, so solutions that are laser-focused on solving specific challenges around authentication can help banks stay ahead of emerging fraud threats."

Ralph Post

CTO of Fourthline

How banks should communicate their approach to KYC

Beyond having an effective approach to KYC and fraud management, communicating this approach to customers is key. Most respondents (67%) want to know if their bank outsources fraud or security processes and if they do, to which providers. A similar percentage (66%) would like to know more about how their bank keeps their data safe. However, just over half (55%) say their bank communicates clearly about how they protect their data. An effective communication strategy helps put customers' minds at ease and can help a bank differentiate itself from competitors.

55%

would like to receive written documentation about security.

45%

would like to watch videos about security

28%

would like to receive information about security over the phone.

59% of people aged 55 and over prefer written documentation, as do German consumers (65%), while 50% of people aged 35–54 prefer video. The best approach for banks is to understand the preferences of their customers and use a tailored combination of channels to communicate their approach.

Survey data collected by Fourthline in November, 2024.

About Fourthline

Fourthline is a prominent European fintech specialising in digital identity verification solutions. Founded in 2017, Fourthline is at the forefront of combating financial crime through advanced KYC and AML technology. With a focus on innovation and excellence, Fourthline is dedicated to revolutionising the way financial institutions manage risk and ensure compliance in an increasingly digital world. Find out more at fourthline.com

Fourthline

fourthline.com