NUANCE | WHAT'S NEXT BLOG

Authentication & fraud prevention, Customer engagement

# 101 financial services leaders report on fraud challenges (and biometric solutions)

Nuance Communications

6 June 2022

In a new report by FStech and Nuance Communications, senior decision-makers from the UK's leading banks, building societies, asset management firms, and insurance companies share the biggest threats they face—and how they're responding. The results paint a picture of an industry embracing biometric authentication to comply with Strong Customer Authentication (SCA) and mitigate rising fraud risks on digital and self-service channels.

To truly understand the UK's fraud landscape, you need to talk to the key decision-makers at its leading financial services organizations. This latest survey draws on insights from heads of risk, heads of compliance, CIOs, and more from 101 of the industry's most important players. As well as providing yet more evidence that fraud thrives in times of disruption, the report digs into the growing adoption of AI and biometric solutions to provide stronger customer authentication.

I'll explore some of the headline findings below—to dive deeper, just download the full report.

## The shift to digital has increased fraud risks

Most decision-makers (56%) reported seeing an increase in certain types of fraud attempts, or a sharp rise in fraud attempts overall, during the last two years. A majority (55%) also said that the shift to digital and self-service channels had increased fraud risk for their organisation.

It's further evidence that as customers have adapted to using digital channels, so have professional criminals. Indeed, the report reveals that more respondents are seeing fraud attempts through online banking than through other any other method.

We all remember how, when the pandemic first struck, fraudsters pivoted their operations to capitalise on sudden disruption and fresh anxieties. This report shows that some of the tactics criminals leaned on in those early days remain popular—not least phishing, which is second only to 'online banking fraud' in its prevalence.

Despite the rise in digital threats, the majority of UK financial services organisations say their established remote banking channels (including telephone banking) remain a focus for their anti-fraud and compliance teams. Those in the minority must be careful that as they advance their anti-fraud capabilities on younger channels, the older ones aren't left behind. Fraudsters are quick to find the path of least resistance, and to be robust, a modern fraud prevention strategy needs to be omnichannel.

## The industry is embracing biometric solutions

So, as the fraud landscape changes and digital risks increase, how are UK financial services organisations evolving their customer authentication capabilities? To find out, respondents were asked which authentication technologies they are implementing right now. And biometric technologies top the list.

This is bad news for fraudsters. The many weaknesses of knowledge-based authentication have been well-documented, and criminals are increasingly adept at using malware and SIM swaps to circumvent alternative authentication factors such as one-time passwords.

Biometric solutions enable stronger customer authentication by empowering financial services organisations to verify who a customer is, rather than what they know (like a password that can be stolen) or what they own (like a device that can be compromised).

But making life harder for criminals won't be the only motivation for many brands rethinking their authentication strategies. Some will be looking to keep pace with industry innovators and make life easier for their customers. Almost half (49%) said their customers were frustrated with the PIN and password login experiences that technologies like voice biometrics can replace.

## The barriers to (and business case for) biometrics

The survey also explores why some organisations might hesitate to implement biometric technologies such as AI-assisted authentication, despite the impressive results they're delivering for more and more of their industry peers.

The primary concern is 'cost of deployment', which was chosen by 81% of respondents. This indicates there's still work to be done to communicate the broad and compelling business case for biometric authentication.

Using Nuance biometric solutions, brands have been able to reduce fraud losses (by as much as 92%) and unlock new contact centre efficiencies. The switch away from slow, knowledge-based processes helps them reduce average handle times by as much as 89 seconds.

As leading technologies increasingly become available in the cloud, the upfront costs and time commitment involved in getting started with biometrics are also coming down. Nuance Gatekeeper, for example, is a unified solution that can provide cloud-native biometric authentication and intelligent fraud prevention across all channels, layering multiple biometric and non-biometric factors into a central AI risk engine.

## Questions of compliance, inclusivity, and more—get the insights

There's much more to dissect and debate in the full report, which also explores:

- The challenges UK financial services organisations face as they prepare for SCA compliance
- How much importance they're placing on inclusivity when rethinking customer verification
- How they are (and aren't) using their authentication strategy to improve customer experience

**Tags:** Nuance Gatekeeper, Financial services

## More Information

### Read the report

Download "The fraud risk challenge" to explore the threats that UK financial services organisations currently face, and how they're working to address them.

Download