proov

Deepfakes: The Threat to Financial Services

What are deepfakes?

Deepfakes are videos, images or audio recordings that have been distorted to present an individual saying or doing something that they didn't say or do.

If you think of the thing that you are least likely to ever say, and then imagine your friends, family or employer being shown a (convincing) video of you saying it, it is easy to see the potential for malicious misuse.

Deepfakes are created using artificial neural networks, which means that they can be produced increasingly easily to look authentic and convincing, thus opening up opportunities for abuse.

Both government and commercial enterprises have been called upon to address the threat of deepfakes.

Although deepfakes have been used for social sharing and entertainment, they have also been employed in hoaxes, revenge porn, and increasingly, fraud and impersonation.

Both government and commercial enterprises have been called upon to address the threat of deepfakes, particularly with the US election coming in November 2020. Facebook announced in January 2020 that it would ban the use of deepfakes.

How do deepfakes affect the financial services industry?

The financial services industry could be affected by deepfakes in a number of ways, including:

- Onboarding processes could be subverted and fraudulent accounts created to facilitate money-laundering.
- Payments or transfers could be authorised fraudulently.
- Accounts belonging to high net worth or high profile individuals could be hijacked.
- Synthetic identities could be created, whereby criminals take elements of a real identity and attach them to a non-existent individual.
- CEOs can be impersonated, leading to employees being tricked into unauthorised payment transfers or divulging sensitive information.
- Insider trading and market manipulation could be facilitated.

How can you prevent deepfake fraud?

iProov's biometric authentication technology allows organizations to protect themselves and their customers against deepfake fraud.

iProov technology has been built specifically with anti-spoofing capabilities that establish the 'genuine presence' of a customer. This means that enterprises can put facial biometric authentication technology in place that actively detects and prevents fraudulent attacks using deepfakes.

The benefits to financial services providers are enormous: customers can be authenticated remotely using the customer's smartphone or desktop, allowing them to be onboarded as a customer, to authorize transactions, or to access other services safely and securely.

Summary of findings

- Deepfakes are viewed as a serious threat to the financial sector – the majority (77%) of cyber security decision makers in the finance sector are concerned about deepfakes being used fraudulently in the industry and most expect the threat to worsen in the future.
- Online payment/transfers and online personal banking are most at risk – most decision-makers believe that online payments/transfers and online personal banking are most at risk of criminal deepfake activity.
- Only a quarter have implemented measures to combat deepfakes – 28% say they are prepared to protect themselves and their customers against deepfake fraud, with 41% planning to put measure in place within the next 2 years.

Methodology

The survey was conducted in November 2019 with 105 cyber security decision-makers in financial organisations in the UK.

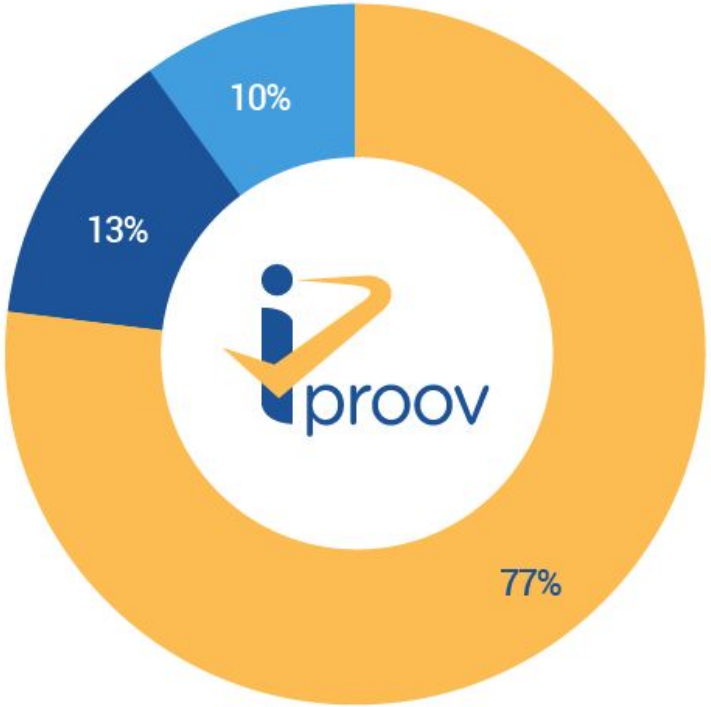
proov

Are you concerned about deepfakes being used fraudulently in the financial services industry?

77% of cybersecurity experts in financial services say they are concerned about fraudulent use of deepfakes

13% had never heard of a deepfake

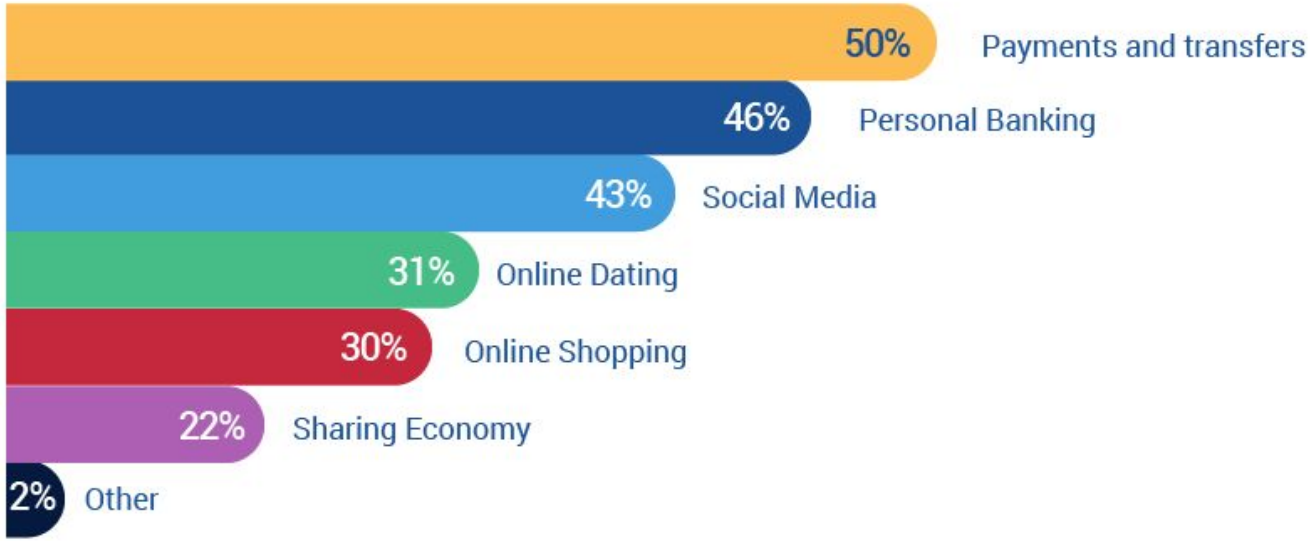
Only 10% did not see deepfakes as a concern



proov

Which services are most at risk of deepfake fraud?

Personal banking and payments were considered to be most at risk of deepfake fraud, underlining that the financial services industry will need to lead the charge in protecting consumers.

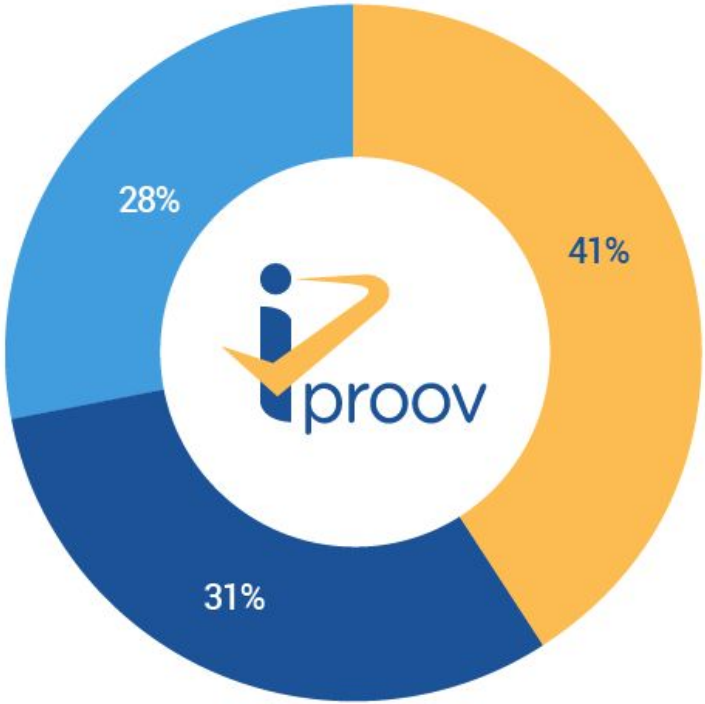


Do you or your organisation plan to put measures in place to combat deepfakes?

41% plan to do so in the next two years

31% have no plans or were not sure

28% have already implemented measures to combat deepfake fraud

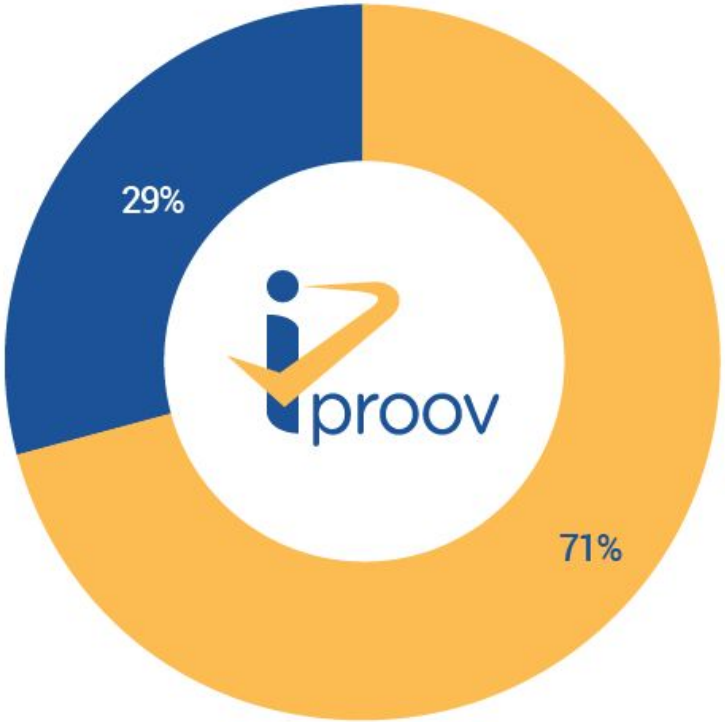


proov

Do you think your customers are concerned by the threat of deepfakes?

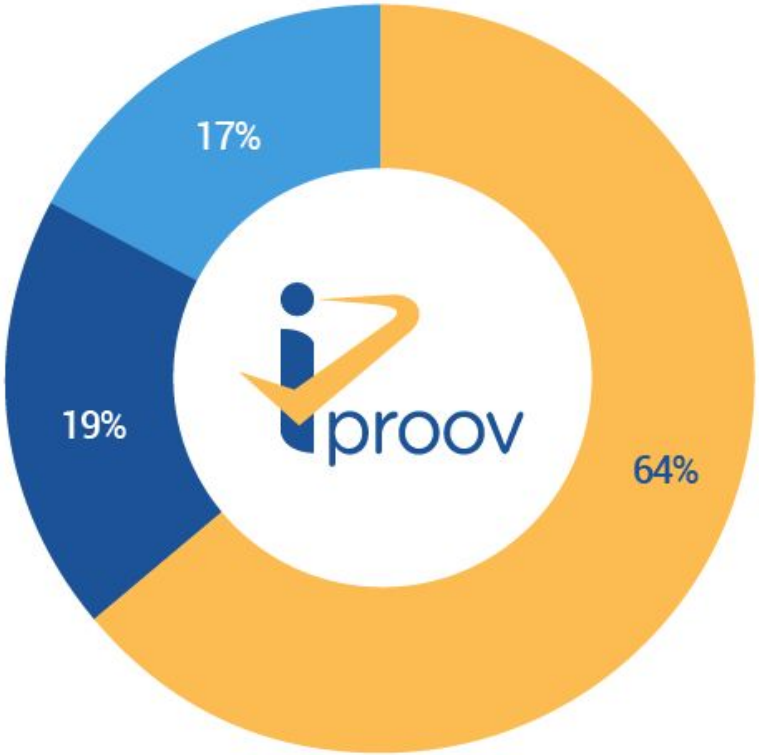
71% felt that their customers were “very concerned” or “somewhat concerned” by the threat of deepfakes

29% felt that their customers were not worried by deepfakes



Do you think the deepfake threat will continue to grow?

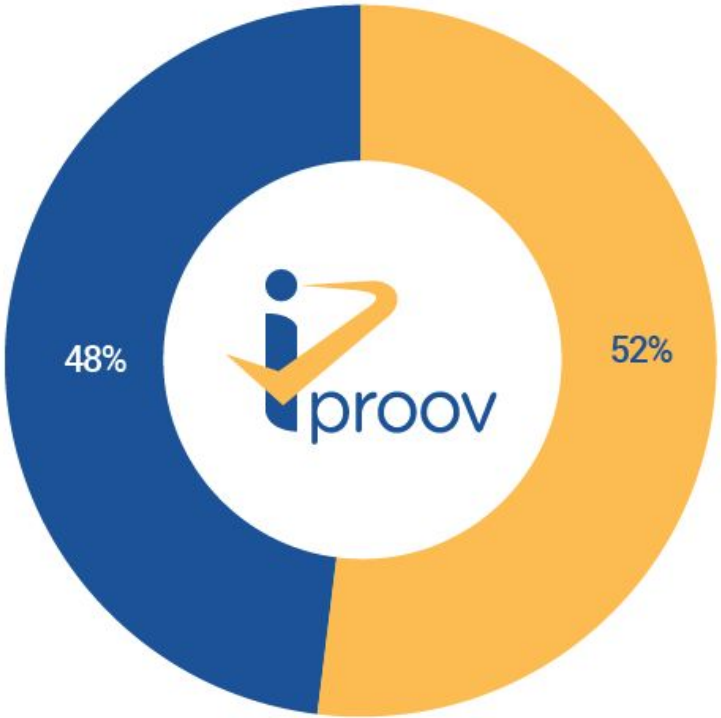
- 64% felt that the threat of deepfakes on the financial services sector is set to get worse
- 19% felt that the impact of deepfakes had got as bad as it is going to get
- 17% were unsure if the threat would continue to grow



Do you feel you know enough about deepfakes to adequately put measures into place to combat them in your organisation?

52% felt they either needed more information or were not clear on the potential impact of deepfakes

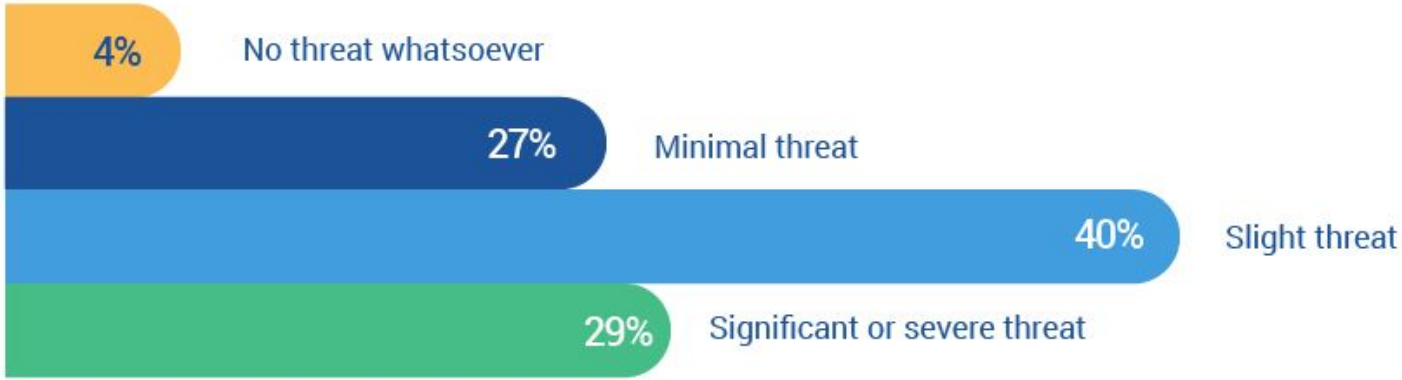
48% felt they understood how deepfakes might impact their organisation and can plan effectively to combat them



proov

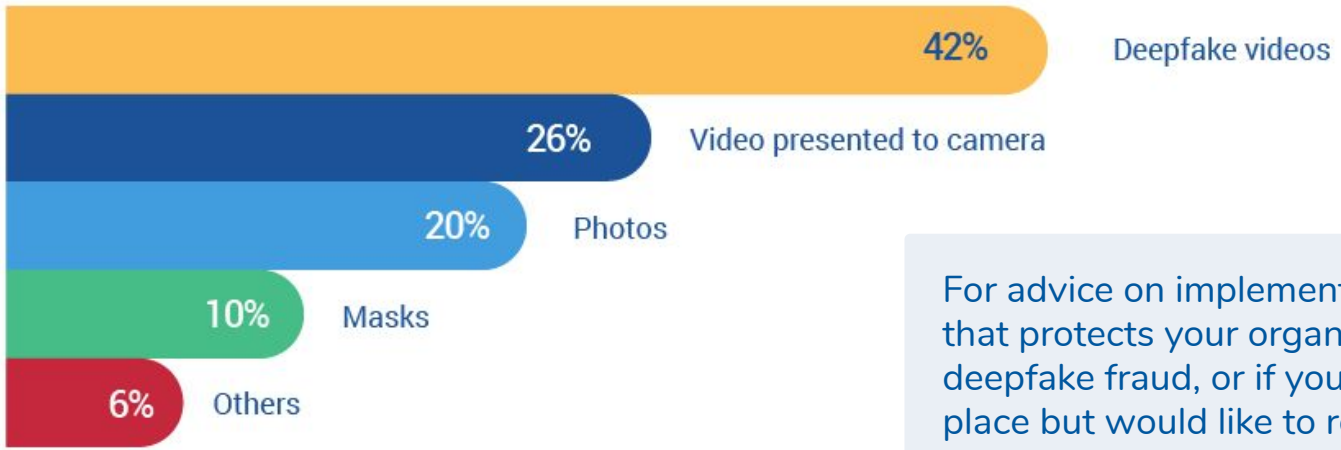
Please select the scale of the threat deepfakes pose to your organisation

Almost a third (29%) see deepfakes as a significant or severe threat to their organisation, with 40% rating deepfakes as a slight threat.

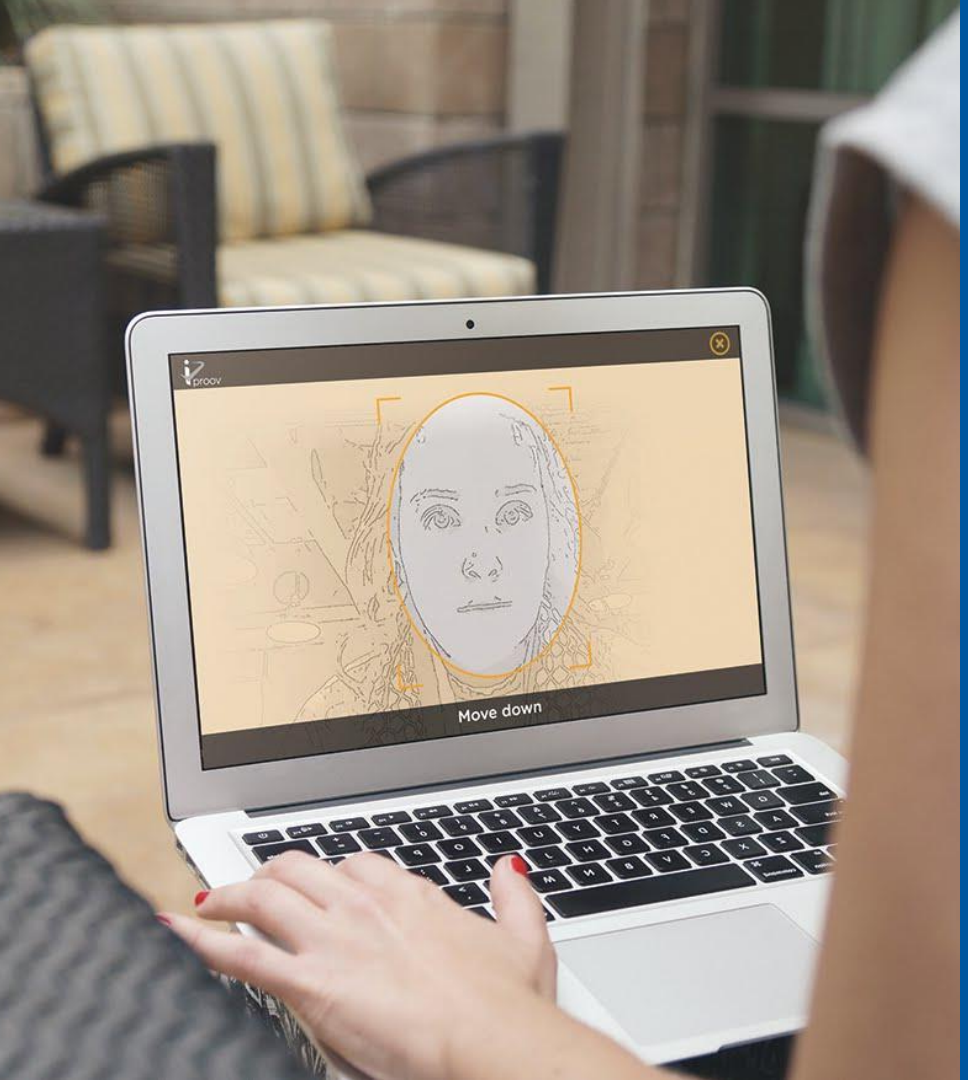


Which of these tactics is most likely to compromise facial authentication measures in financial services?

The majority of respondents said that deepfakes were the biggest risk to facial authentication.



For advice on implementing authentication that protects your organisation against deepfake fraud, or if you have measures in place but would like to review them, please contact us at enquiries@iproov.com



iProov Genuine Presence Assurance provides:

- ✓ Effortless Usability
- ✓ High Security
- ✓ Spoof Protection

Genuine Presence Assurance:
Right person, real person, right now?

enquiries@iproov.com