National Mortgage News

ARTIFICIAL INTELLIGENCE

AI deepfakes and mortgages: how big is the risk?

By Spencer Lee May 27, 2024, 10:43 a.m. EDT 6 Min Read

With artificial intelligence able to create convincing clones of everyone from Warren Buffett to one's own family members, the mortgage industry, like others in the financial world, will need to address the rise of deepfakes.

Deepfakes have already shown they can hobble a company financially, and artificial intelligence technology can make fraud easier to commit and costlier to fix. While the ability to manipulate video and audio is nothing new, ease of access to the newest cyber weapons expedited their arrival in mortgage banking. But growing awareness of the problem and authentication tools, when employed, may also help keep fraudsters at bay. A recent survey conducted by National Mortgage News parent company Arizent found that 51% of mortgage respondents felt AI could be used to detect and mitigate fraud.

"Every industry right now is grappling with these issues from the retirement industry to the banking industry to auto," said Pat Kinsell, CEO and co-founder of Proof, which facilitates remote online notarizations used in title closings. Previously known as Notarize, Proof also provides other forms of video verification solutions across business sectors.

the Sloan School of Management at the Massachusetts Institute of Technology. He also serves as the founding director of Cybersecurity at MIT Sloan, an interdisciplinary consortium focused on improving critical infrastructure.

"A lot of times we're dealing with people that you're not necessarily personally familiar with, and even if you were, could easily be deceived as to whether you're actually dealing with them," he said.

"All these things involve relying on trust. In some cases, you're trusting someone who you don't know but that theoretically has been introduced to you," Madnick added.

Threats aren't just coming from organized large-scale actors either. Since creation of a convincing AI figure relies on having a great deal of data about an individual, deepfakes are often "a garden variety problem." Kinsell said.

"The reality is these are local fraudsters often or someone who is trying to defraud a family member."

Deepfake technology has already proven to have the ability to deceive to devastating effect. Earlier this year, an employee at a multinational firm in Hong Kong wired more than $25 million after video meetings with company leaders, all of whom turned out to be generated by artificial intelligence. In a recent meeting with shareholders, Berkshire Hathaway Chairman, himself, commented that a cloned version of himself was realistic enough that he might send money to it.

Growing threat with no clear remedy

With video conferencing a more common communication tool since the Covid-19 pandemic, the

Compounding the risk is the ease at which a fraudulent video or recording can be created through "over-the-counter" tools available for download, Madnick said. The technology is also advancing enough that software can tailor a deepfake for specific types of interactions or transactions.

"It's not that you have to know how to create a deepfake. Basically, for $1,000 you buy access to a deepfake conversion system," Madnick said.

But recognition of risk doesn't mean a silver-bullet solution is easy to develop, so tech providers are focused on educating businesses they work with about prevention tools and methods.

"Things that we would recommend people pay attention to are the facial aspects, because the way people talk and how your mannerisms reflect on video — there are things you can do to spot if it appears real or not," said Nicole Craine, chief operating officer at Bombbomb, a provider of video communication and recording platforms to assist mortgage and other financial services in marketing and sales.

Possible signs of fraud include patterns of forehead wrinkles or odd or inappropriate glare seen on eyeglasses based on the position of the speaker, Craine noted.

As the public becomes more aware of AI threats, though, fraudsters are also elevating the quality of videos and voice mimicking techniques to make them more foolproof. Digital watermarks and metadata embedded on some forms of media can verify authenticity, but perpetrators will look for ways to avoid using certain types of software while still sending intended victims toward them.

While taking best practices to protect themselves from AI-generated fraud, mortgage companies using video in marketing might serve their clients best by giving them the same regular guidance they provide in other forms of correspondence when they develop the relationship.

"I do think that mortgage companies are educated about this," Craine said.

meeting, according to Kinsell. "What's critical is that it's a multifactorial process," he said.

Steps include knowledge based authentication through previously submitted identity-challenge questions, submission of government credentials verified against trusted databases, as well as visual comparisons of the face," he added.

To get through a robust multi authentication process, a user will have to have manipulated a ton of data. "And it's really hard — this multifactor approach — to go through a process like that."

AI as a source of the problem but also the answer

Some states have also instituted biometric liveness checks in some digital meetings to guard against deepfakes, whereby users demonstrate they are not an AI-generated figure. The use of liveness checks is one example of how the artificial intelligence technology can provide mortgage and real estate related companies with tools to combat transaction risk.

Leading tech businesses are in the process of developing methods to apply their learning models to identify deepfakes at scale as well, according to Craine. "When deployed appropriately, it can also help detect if there's something really unnatural about the internet interaction," she said.

While there is frequent discussion surrounding potential AI regulation in financial services to alleviate threats, little is in the books currently that dive into the specifics in audio and video deepfake technology, Madnick said. But criminals keep their eyes on the rules as well, with laws perhaps unintentionally helping them in their attempts by giving them hints to future development.

For instance, fraudsters can easily find cybersecurity disclosures companies provide, which are sometimes mandated by law, in their planning. "They must indicate what they've been doing to improve their cybersecurity, which, of course, if you think about it, it's great news for the crooks to know about as well," Madnick said.

said.

Spencer Lee Reporter, National Mortgage News

ARTIFICIAL INTELLIGENCE MORTGAGE TECHNOLOGY TECHNOLOGY

National Mortgage News
DIGITAL MORTGAGE
September 9–10, 2024 | Manchester Grand Hyatt, San Diego, CA
Your roadmap for acquisition, retention and innovation
REGISTER NOW

National Mortgage News
DIGITAL MORTGAGE
September 9–10, 2024 | Manchester Grand Hyatt, San Diego, CA
Your roadmap for acquisition, retention and innovation
REGISTER NOW

TRENDING

GROWTH CONTENT