



2021

DEEPPFAKES: THE BUSINESS THREAT

Inaugural Deepfakes in Business Survey Results



Attestiv Inc.

209 W. Central Street
Natick, MA

info@attestiv.com

<https://www.attestiv.com>

May 2021

A hand holding a smartphone, with a blurred background of a document or screen. The hand is in the foreground, and the phone is held vertically. The background is out of focus, showing what appears to be a document or a screen with some text and graphics. The overall lighting is warm and soft.

Newly emerging deepfakes

While photo and video editing tools are not new, Deepfakes, a newly emerging breed of AI-enhanced videos, have started demonstrating the ability to blur the public's perception of reality.

<https://www.attestiv.com>

Copyright © 2021 Attestiv Inc. All rights reserved

Unlike conventional video editing, Deepfakes utilize AI to eliminate forensic traces from altered or synthetically generated videos, bringing a new level of realism, closely matching the likeness and voices of real-life individuals. With the rapid proliferation and advancement of Deepfake tools, many researchers have concluded it is only a matter of time before Deepfakes become nearly undetectable to the human eye and subsequently undetectable even to elaborate forensic tools¹.

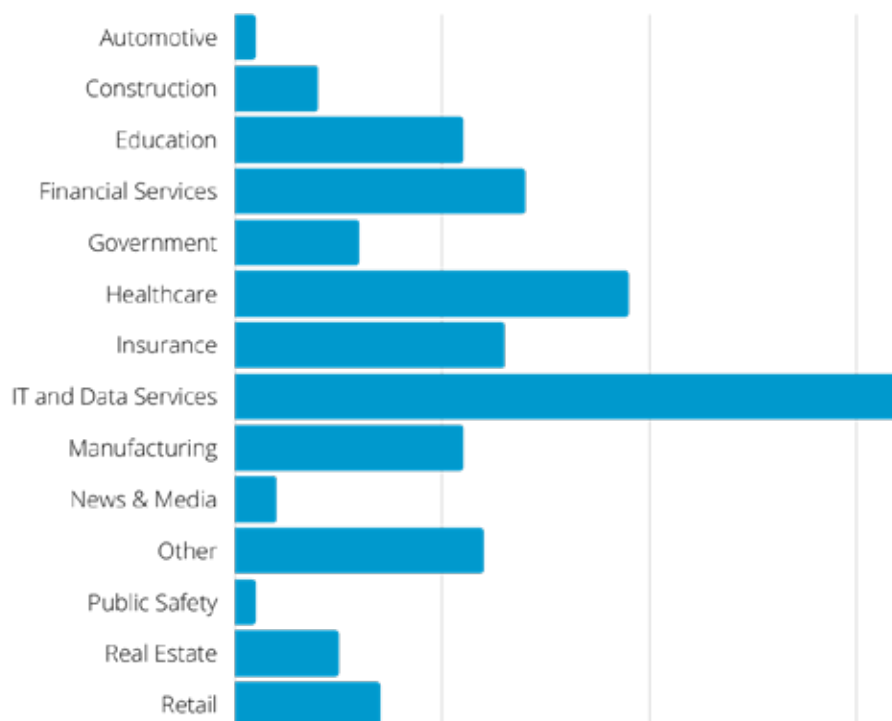
While much of the concern to date around Deepfakes has focused on social media and pornography, it is worth noting that Deepfakes pose a significant threat to people portrayed in these videos and their circle of trust, by hijacking their identities to promote misinformation or disinformation. As a result, Deepfakes also pose an existential threat to businesses, particularly in industries that depend on digital media (photos, videos, voice) to make important decisions. Moreover, the FBI warned earlier this year that Deepfakes are a new cyber-attack threat targeting businesses². As a result many organizations are pondering strategies to mitigate the risks and potentially bad outcomes that may result.

1 <https://www.techspot.com/news/88592-ucsd-scientists-developed-technique-fools-deepfake-detection-systems.html>

2 <https://www.forbes.com/sites/glenngow/2021/05/02/the-scary-truth-behind-the-fbi-warning-deepfake-fraud-is-here-and-its-serious-we-are-not-prepared/>

Promoting Deepfake Awareness

To help promote awareness in the corporate realm, Attestiv recently surveyed US based business professionals about the threats to their businesses related to altered or manipulated digital media re: “Deepfakes”, their plan of action and defense strategies. This paper summarizes the results of the survey, identifying the concerns and awareness of these threats and also highlights the current inaction gap to mitigate risks. Respondents of the survey work across a broad spectrum of business industries. However, the largest number of respondents work in IT and Data Services, Healthcare and Financial Services.



Awareness Levels

Respondents were asked about the ways in which deepfakes and altered digital media are a potential risk for their business. This question allowed respondents to select from any or all of the following that apply to their companies:

- Disinformation on social media
- IT threats
- Reputational threats
- Fraud threats
- Compliance concerns
- I don't feel like my company is at risk

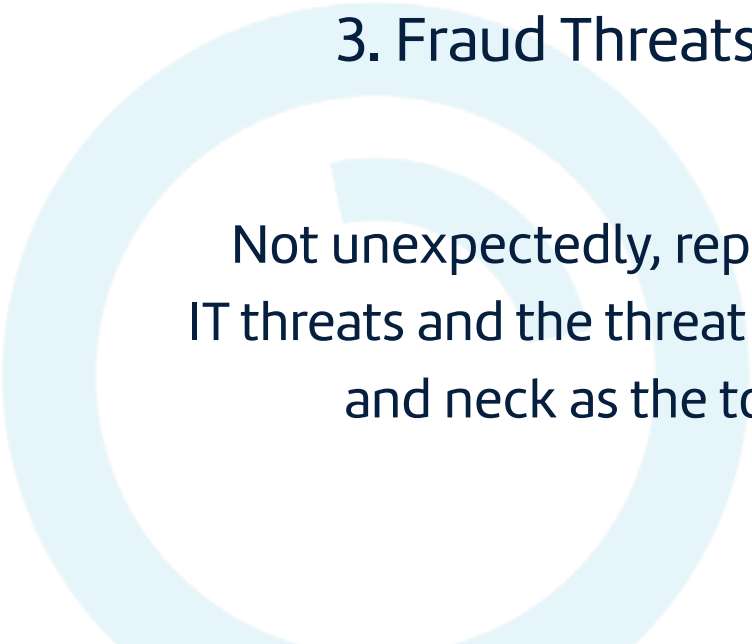


Acknowledging that Deepfakes pose a risk to their organization, over eighty percent of respondents identified that at least one of these listed threats pose a potential risk to their organization.



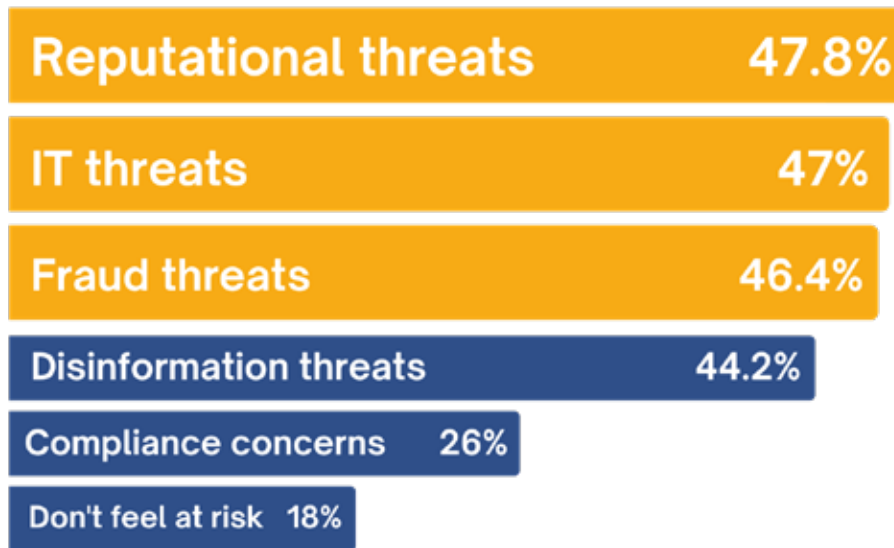
The top three Deepfake concerns included:

1. Reputational Threats
2. IT Threats
3. Fraud Threats



Not unexpectedly, reputational threats, IT threats and the threat of fraud were neck and neck as the top concerns.

Without question, there is widespread awareness of the Deepfake issue, but is there a solution?

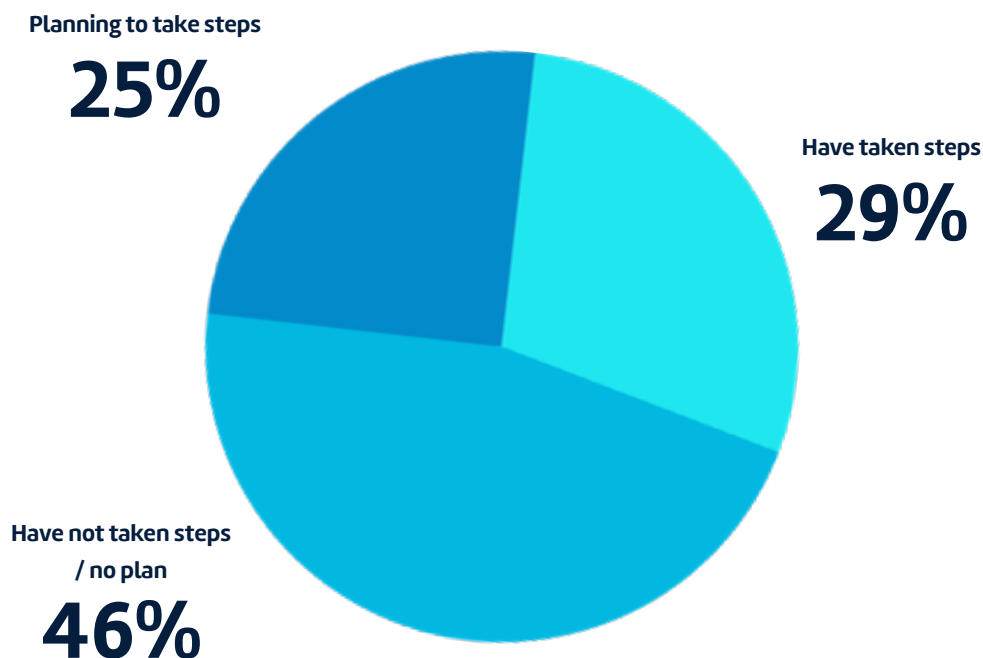


The fraud aspect is not surprising, particularly for industries which use digital photos, videos and documents to make business decisions, such as insurance companies, which are already subject to billions of dollars in annual fraud in the US alone. IT threats are potentially indicative of the ability for Deepfakes to spoof the identity of individuals online and potentially cause harm by spreading disinformation under the guise of a trusted individual. In a similar vein, reputational threats can arise from the disinformation spread by Deepfakes.

Inaction Gap

Next, our survey sought information about what steps organizations will take to protect themselves against altered digital media. Surprisingly, **less than 30 percent of respondents have taken steps** when asked “Will your organization take steps against altered digital media?” While answers varied across the industries of participants, by and large the majority, **greater than 80%**, are currently concerned about Deepfake threats.

While the amount of inaction exposes a problem, one consolation is that 25% of respondents said they are planning to take action, meaning they recognize the threat and a solution is in the works. On the other hand, that leaves a total of 46% of respondents without a plan or without a knowledge of the plan.



As we break down the results across industries, a number of key takeaways emerge:



**Most
Action
Healthcare**

In healthcare, over 36% of respondents have already taken steps. This is the highest amount of action by any specific industry in the survey.



**Highest
Awareness
Finance**

Over 68% of respondents in Finance and 64% of respondents in IT have indicated they are either taking or planning steps to mitigate the risk. Perhaps these particular respondents were most familiar with Deepfakes.



**Lowest
Awareness
Insurance**

Only 39% of respondents in Insurance indicated they are either taking or planning steps to mitigate the risk. These numbers are surprisingly lower than the mean, in an industry that already is hit with tens of billions of dollars in fraud annually.

Proposed Solution

Finally, participants were asked to consider a possible solution to their potential deepfake problem. When asked “What’s the best defense organizations can take against altered digital media?” those surveyed were provided with the following choices which best described their ideal solution:

- Automated detection and filtering via software or SaaS solution
- Training employees to detect it
- Hope for an industry-wide solution
- Wait until an incident occurs and plan mitigation

This question provided rich insight into how participants are considering a possible solution. 48% of respondents felt the best defense was an automated detection and filtering solution, while 38% felt training employees to detect Deepfakes was the best solution.

What's the best defense organizations can take against altered digital media?

Automated Detection



Training Employees



Hoping for an industry-wide solution



Wait until an incident occurs
and plan mitigation



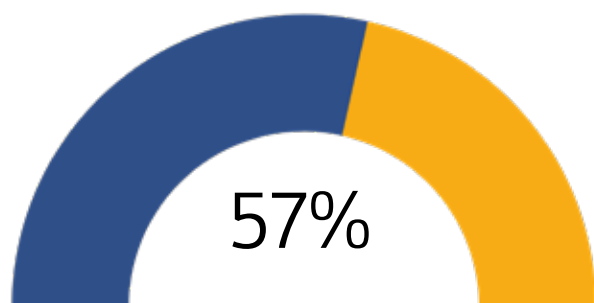
Training employees to detect Deepfakes may not be a viable solution given the likelihood that they are rapidly becoming undetectable to human inspection

Automated detection and filtering solutions are a viable approach to stopping Deepfakes, as there are currently solutions on the market employing technologies such as blockchain or AI to prevent or detect manipulated media. On the other hand, training employees to detect Deepfakes may not be a viable solution given the likelihood that they are rapidly becoming undetectable to human inspection. It appears there may be a need for further education regarding the Deepfake threat and the trajectory the technology is taking.

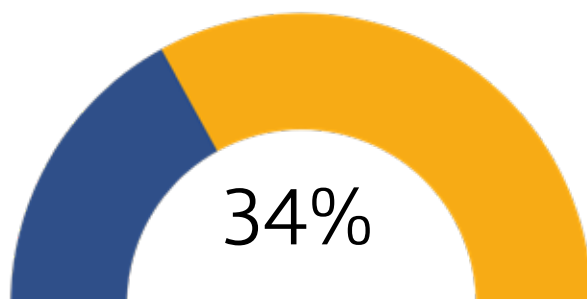
In both Insurance and Finance, the results showed over 57% of respondents felt the best defense was an automated detection and filtering solution, while 34% felt training employees to detect Deepfakes was the best solution, perhaps indicating a better familiarity with the broader long-term threat.

Insurance & Finance

Automated detection and filtering solution



Training employees to detect Deepfakes



<https://www.attestiv.com>

Summary

The Attestiv study involved 138 respondents across various industries to help establish an indicator of the current perception around the threats of Deepfakes to Business and the type of action plans businesses are adopting. We anticipate, as the threats from Deepfakes continue to grow and begin to affect organizations, the inaction gap will close and more businesses will begin to take action.



About Attestiv

We are on a mission to put authenticity into all digital media

Attestiv offers a tamper-proof media validation platform focusing on insurance, healthcare, public safety, government, and media markets. Established in 2018, Attestiv verifies and protects the authenticity of digital media and data (photos, videos and documents), helping organizations build efficient processes, improve customer experience, and provide the highest standard for

information exchange. Utilizing artificial intelligence and blockchain technology, Attestiv assures the authenticity of digital media at scale with attractive economics, enabling trust, chain of custody, digital transformation, cost savings, and fraud prevention.

Learn more about our products and services at <https://www.attestiv.com>.

For more information about the survey data and collection information, please email marketing@attestiv.com