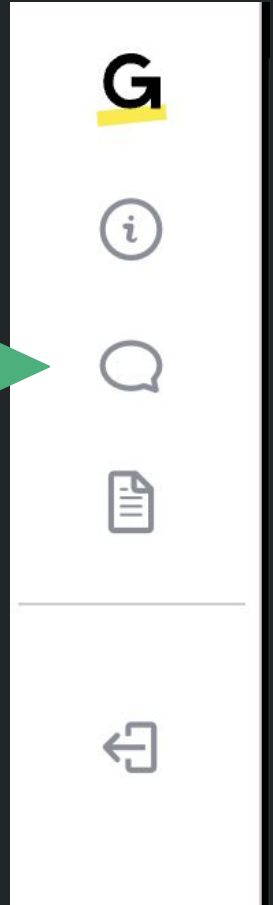




Guarding Your Closing Funds: Strategies to Combat Wire Fraud

Housekeeping

- Check the stability of your internet connection. Try refreshing if you have audio issues.
- We want to hear from you! Ask questions in the chat.
- Please take a moment to complete our survey after the webinar ends. We value your feedback.
- Stream the webinar recording and share it with your team.



Today's Speakers



Jeremy Yohe
Vice President of
Communications, ALTA



Jewel Quintyne
Senior Title Operations Consultant,
Qualia



Nikki Pfleger
Specialty Deposits RM Lead,
Encore Bank

Agenda

**The Wire Fraud Threat
Landscape 05**

Recent Insights & Trends 09

Why Now 12

**Tactics to Safeguard Your
Business with People,
Process, & Technology 13**

Q&A 23

Wire Fraud Threats Are Becoming More Sophisticated

\$145MM

The real estate industry suffered millions in adjusted losses in 2023 due to cybercrime

4,151%

Since ChatGPT launched in 2022, there has been a 4,151% surge in malicious phishing messages

1 in 4

1 in 4 of title companies experienced at least one seller impersonation attempt in 2023

\$2.9B

Business email compromise was the second costliest cybercrime in 2023 across industries

3,000%

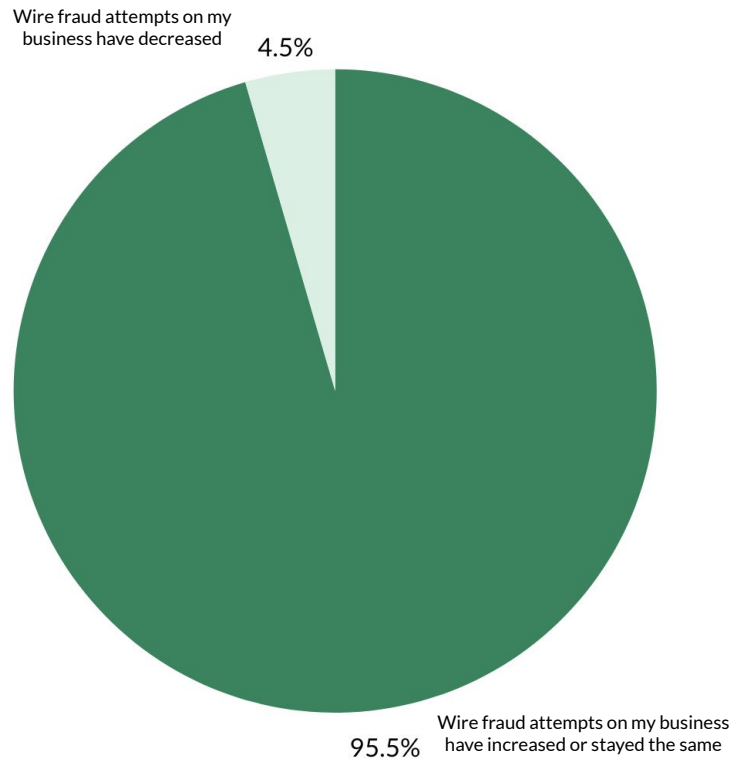
Between 2022 and 2023, the number of deepfakes increased 3,000%

\$143K

\$143k is the average title insurance claim cost for fraud and forgery according to ALTA

The Frequency of Wire Fraud Attacks Isn't Slowing Down

In a recent Qualia survey, **95%** of respondents said the number of wire fraud attacks on their business **remained the same or increased** in the last 12 months.

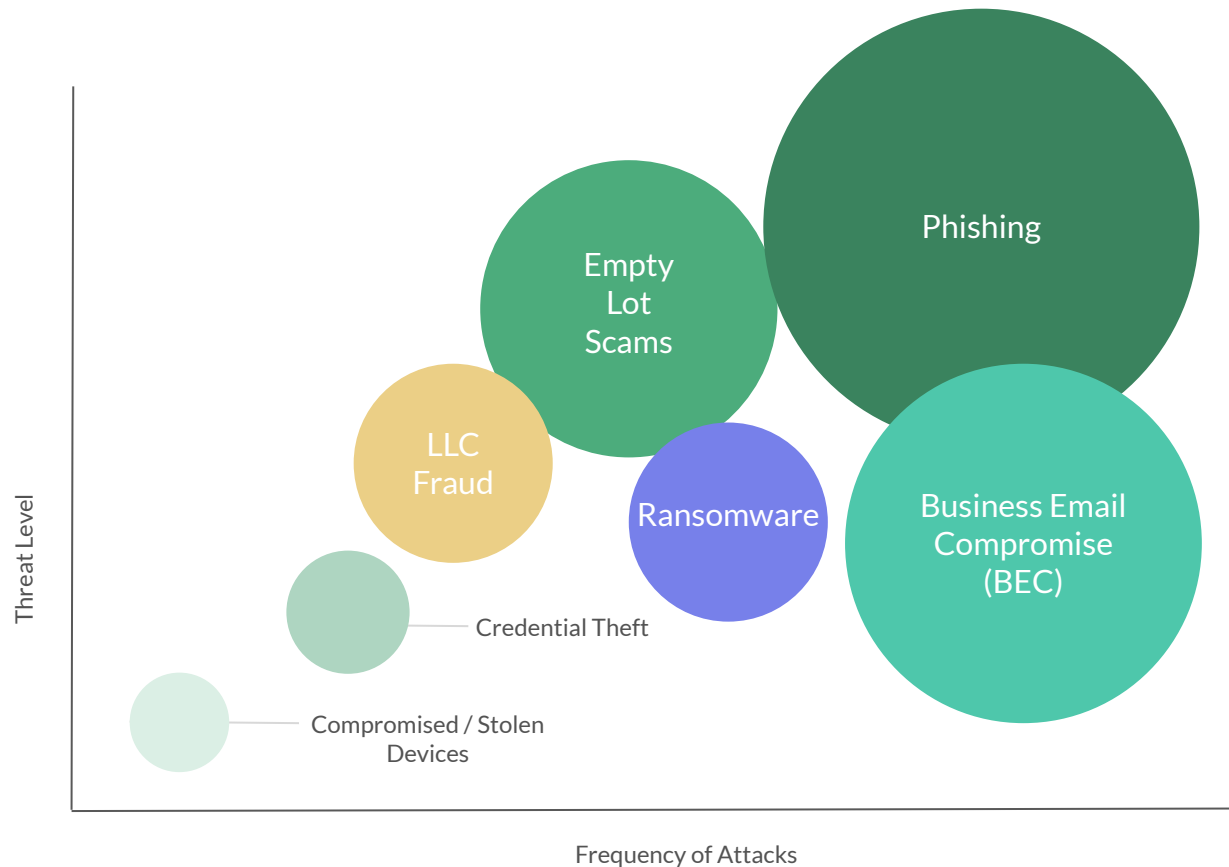


Select the statement which you most agree about the frequency of cyber security attacks on your business in the last 12 months.

Fraud is becoming more complex and multi-layered, and therefore requires a multi-pronged approach to prevent it.

Survey Question

How often has your business experienced these types of cyberattacks in the past 12 months?

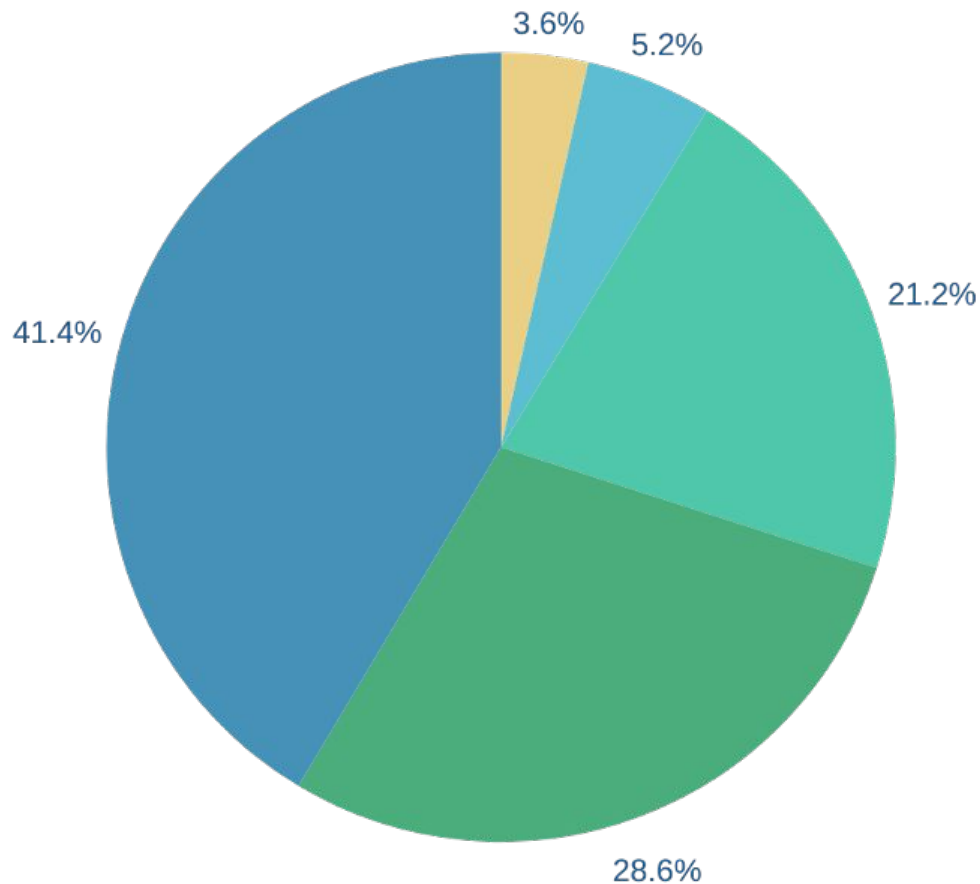


A deepfake attempt occurred once every 5 minutes in 2024.

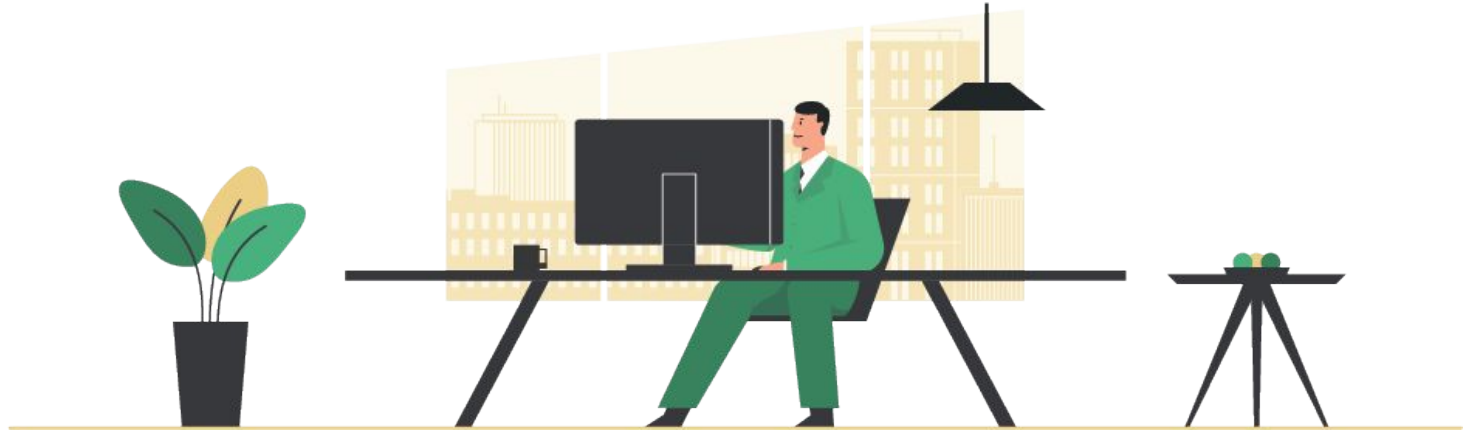
A **deepfake** is a type of synthetic media that uses artificial intelligence (AI) and deep learning techniques to create highly realistic but entirely fabricated content, including text, audio, images, and video.



Fraudsters use several techniques to try and bypass biometric checks, and deepfakes are the most prominent.



A Multilayered Approach to Security Helps You Combat Wire Fraud Attacks



People —> Process —> Technology



People



Process



Technology

Guide transaction parties to **operate securely.**

- Discourage use of personal email to send sensitive information
- Explain that banks will never email unexpected wire transfer requests
- Warn against clicking links or opening attachments if the sender is unknown or the email looks suspicious



People



Process



Technology

Create a culture of security within your organization.

- Encourage clients to call and verify wire transfer instructions prior to initiating a wire transfer
- Train and retrain staff regularly - not just once a year
- Due to rapid evolution in fraud vectors, security training should be part of regular employee trainings

How to Identify Deepfakes

Blurring in the face but not elsewhere



Change of skin tone near the edge of the face



Unnatural blinking or movements



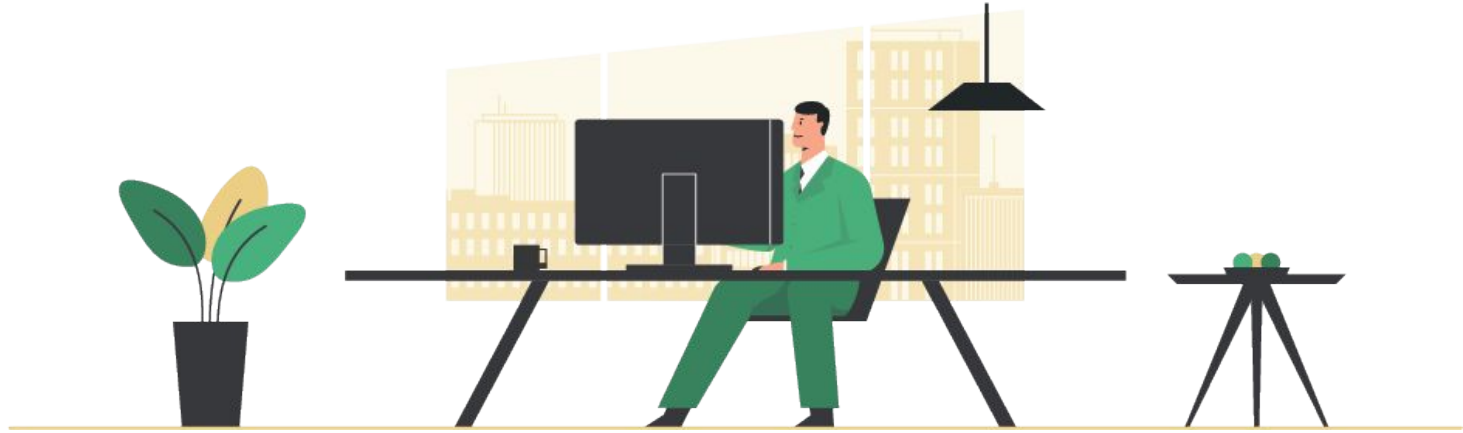
Relevancy of speech



Varying tone inflection



A Multilayered Approach to Security Helps You Combat Wire Fraud Attacks



People —————> **Process** —————> Technology

**Technology**

Embed security into **your processes**.

Maintain a Written Information Security Plan (WISP)

Required under ALTA Best Practices Pillar 3, this document defines what it means for your business to operate securely.

Build security best practices into your workflows

Analyze your team's processes to identify weaknesses and fill those with process improvements or technology.

Ensure your vendors' security is consistent with your own standards

Request and review your vendors' security packets.

Periodically review system login activity

Look for anomalies and suspicious behavior.

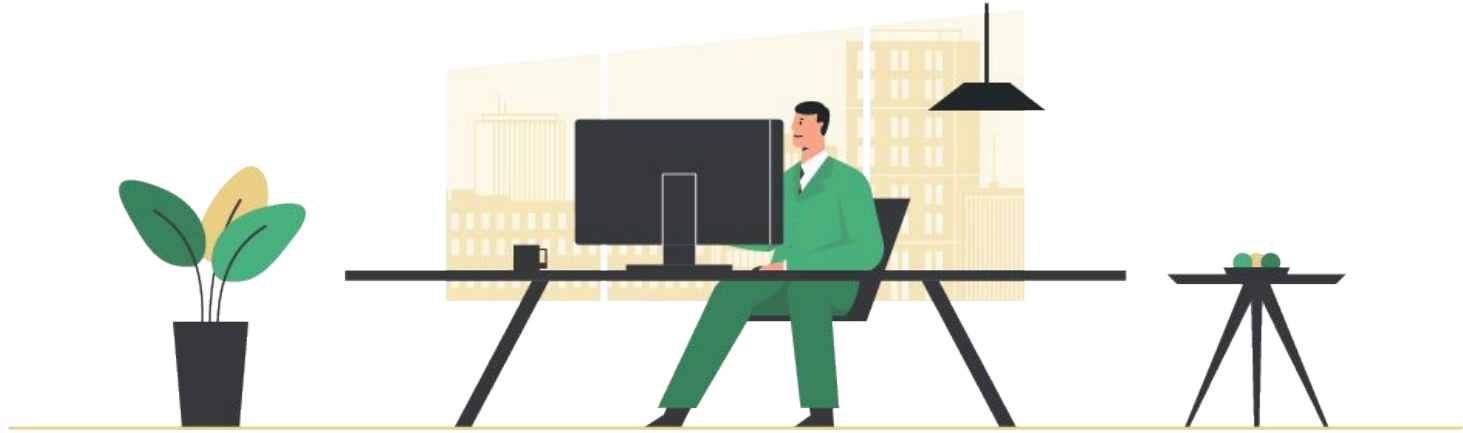
Keep systems up-to-date

Always run the latest updates and patches.

Maintain strong banking relationships

Know a specific bank partner's contact information should the worst occur.

A Multilayered Approach to Security Helps You Combat Wire Fraud Attacks



People —> Process —> Technology

Adopt the Latest Technology to Stop Bad Actors in Their Tracks

Communicate in secure channels

- ❑ Business email compromise (BEC) and social engineering account for most wire fraud, so keep all transaction parties communicating through a secure portal wherever possible.
- ❑ Use an email plugin to flag when an email address isn't recognized by your title production system.

Adopt a wire fraud detection solution

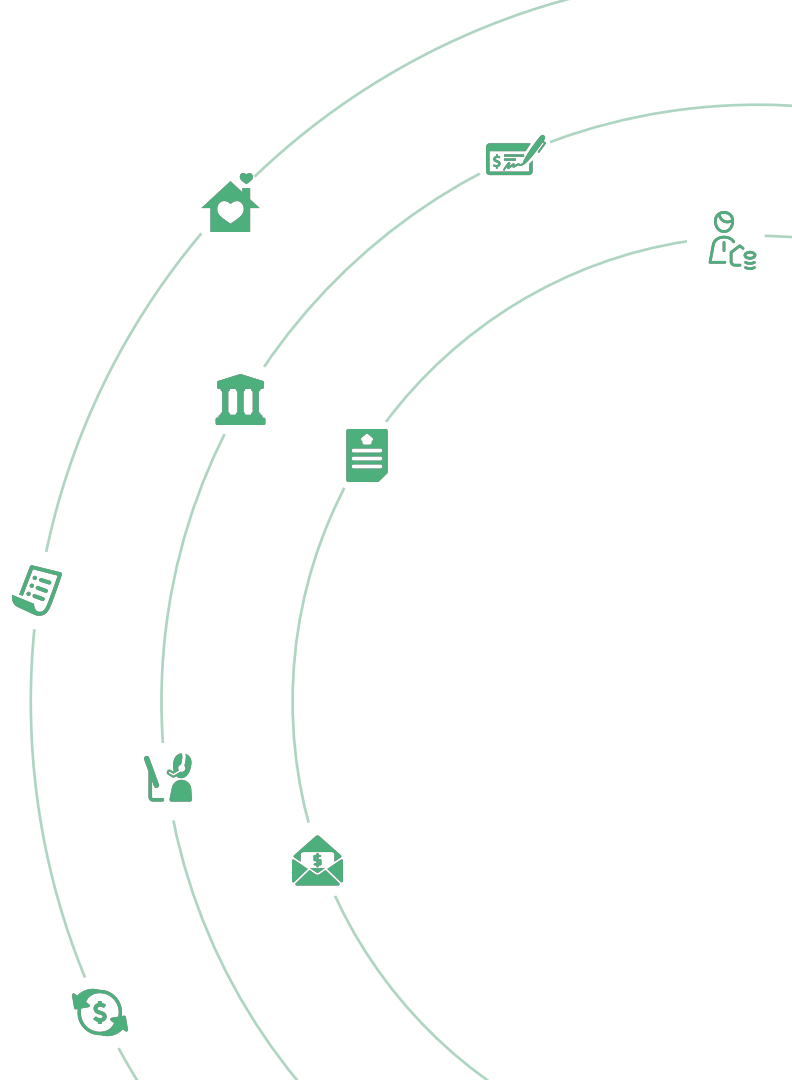
- ❑ Leverage multivariable assessments throughout the transaction to confirm both the identities of transaction parties and the destination of funds.
- ❑ Verify that IDs were government-issued.
- ❑ Examine public records to confirm you're working with a legitimate person.



Your Questions Answered.

Type your questions into the Q&A field to have them answered by our experts.

If your question is not answered today, please feel free to contact partners@qualia.com.





Thank You

How to Identify Deepfakes: Audio

Choppy sentences



Varying tone inflection



Phrasing



Relevancy of speech



Background sounds
consistent with location

