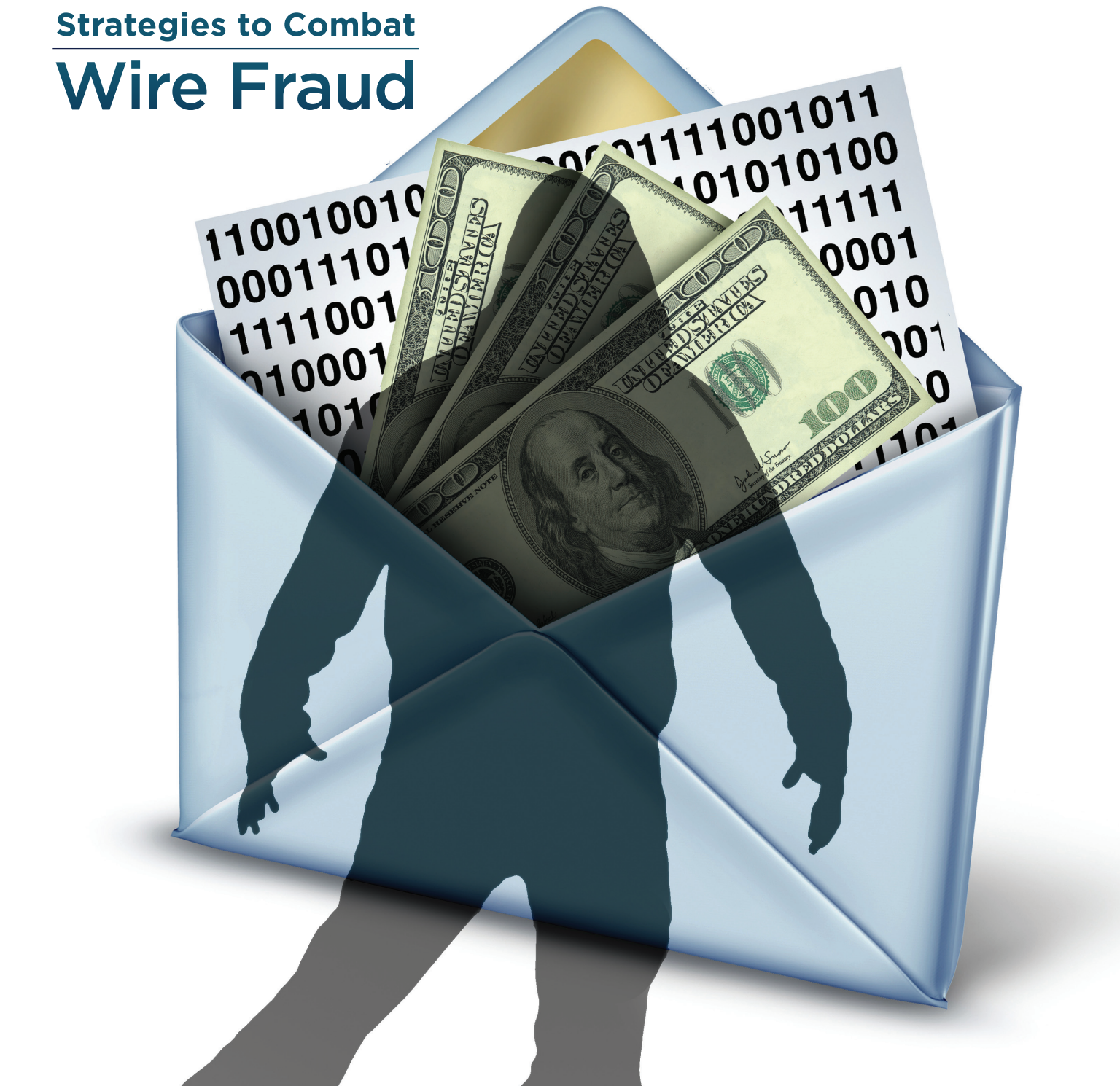
TITLE News
MARCH 2025
AMERICAN LAND TITLE ASSOCIATION

Strategies to Combat

Wire Fraud



iN This Issue

VOLUME 104 | NUMBER 3 | MARCH 2025

COVER STORY

FEATURES

DEPARTMENTS

DON'T MISS THIS MONTH'S DIGITAL ISSUE OF

TiTLENews

The digital edition of **TITLENews** includes a webinar recording as experts examine emerging wire fraud schemes, including the use of AI deepfake technology and seller impersonation. The webinar discusses essential strategies for companies to protect themselves and their clients.

Go to **alta.org** to get your copy of *Digital TitleNews Today*.

TitleNews is published monthly by the American Land Title Association. United States and Canadian subscription rates are $100 a year for members and $300 a year for nonmembers. For subscription information, call 800-787-ALTA.

Send address changes to *TitleNews*, American Land Title Association, 1800 M Street, Suite 300 S, Washington, D.C. 20036-5828.

Members Call Toll Free: 800-787-ALTA
Members Fax Toll Free: 888-FAX-ALTA
Visit ALTA Home Page: alta.org
Email Feedback to: service@alta.org

TiTLENews

OFFICIAL PUBLICATION OF THE **AMERICAN LAND TITLE ASSOCIATION**

PUBLISHER + EDITOR IN CHIEF
Jeremy Yohe

DIRECTOR OF DIGITAL AND PRINT MEDIA
Shawn Sullivan

Confirmation Hearing Focuses on Housing

LAST MONTH, THE SENATE COMMITTEE ON BANKING, HOUSING, AND URBAN AFFAIRS, held a confirmation hearing to consider President Trump's nominees to head the Federal Housing Finance Agency (FHFA) and the Consumer Financial Protection Bureau (CFPB).

JEREMY YOHE
ALTA vice president of communications

During his testimony, Bill Pulte, nominee for FHFA director, said his top mission at the FHFA will be to strengthen and safeguard the housing finance system. He added that any exit from conservatorship by the government-sponsored enterprises (Fannie Mae and Freddie Mac) "must be carefully planned to ensure the safety and soundness of the housing market without upward pressures on mortgage rates."

Jonathan McKernan, the nominee for CFPB director, said that under his watch, the bureau "will take all steps necessary to implement and enforce the federal consumer financial laws and perform each of its other statutorily assigned functions. But the CFPB will do this by centering its regulation on real risks to consumers and by focusing its enforcement on bad actors."

What's next now that the hearing is over? The committee will schedule a vote to move the nominees on to the full Senate for its consideration before final confirmation. If confirmed, ALTA looks forward to collaborating with Pulte and McKernan to expand homeownership opportunities by reducing regulatory barriers to development and increasing the supply of housing.

The FHFA plays a key role in ensuring the safety and soundness of the U.S. housing finance system, and while work is done to address the housing shortage, we will continue to educate the agency staff that title insurance is one of the most essential pillars to reducing risk and is the ultimate safeguard to protecting property rights of homeowners and ensuring the integrity of all real estate transactions. Answering a question from Sen. Mike Rounds (R-S.D.) about credit-risk transfers, Pulte said transferring risk from taxpayers to the private market is always a good thing. This is an important point and one with which we agree, as the FHFA's Title Acceptance Pilot would do the opposite, transferring risk to the GSEs—and ultimately taxpayers—from well reserved, capitalized and regulated title insurance underwriters.

In regard to the CFPB, we will continue to work with the bureau to help provide positive and compliant real estate settlement experiences for consumers. ALTA remains ready to serve as a resource on important issues, such as wire transfer fraud, third-party oversight and mortgage disclosures. McKernan noted in his nomination hearing that, should he be confirmed, the CFPB under his watch would move away from regulation by enforcement. ALTA has long held that businesses regulated by the bureau should be provided clear rules and guidance consistent with statute rather than subject to regulation by enforcement.

Stay tuned to ALTA's communications as we keep you updated on the nominees. In the meantime, we hope you enjoy this edition as we focus on wire fraud, tips to protect your business and steps the industry is taking to mitigate the risk of this kind of fraud.

ALTA News
AMERICAN LAND TITLE ASSOCIATION
HAPPENINGS, NEWS, UPDATES & EVENTS

ALTA Joins Letter in Call for National Data Privacy Law

ALTA joined 37 other organizations in a letter requesting Congress take legislative action to develop a comprehensive national privacy law.

The letter says that legal certainty is crucial to achieving policies that respect individual privacy, and promote choice and competition, while spurring innovation. It outlines several principles for a national data privacy standard:

1. The need for a federal privacy framework that fully preempts state laws related to data privacy and security to establish a uniform privacy standard.
2. Individuals should have the right to determine how personal information is collected, used and shared.
3. Federal privacy legislation should promote transparency and require companies to disclose their data practices in a public privacy policy.
4. Companies should limit collection of personal data to what is reasonably necessary in relation to the purposes for which that personal data is processed, as disclosed to the consumer.
5. Organizations processing consumer data should establish, implement and maintain reasonable administrative, technical and physical security practices that are appropriate to the volume and nature of the data being used.
6. Federal privacy legislation should explicitly preserve the processing of personal data for beneficial purposes such as offering goods and services.
7. Federal privacy legislation should encourage cooperation between the business community and government, not promote adversarial action that results in frivolous litigation.

The letter was sent to Sen. Ted Cruz (R-Texas), chair of the Senate Committee on Commerce, Science and Transportation; Sen. Maria Cantwell (D-Wash.), ranking member of the Senate Committee on Commerce, Science and Transportation; Rep. Brett Guthrie (R-Ky.), chair of the House Committee on Energy and Commerce; and Rep. Frank Pallone (D-N.J.), ranking member of the House Committee on Energy and Commerce.

The National Association of Insurance Commissioners (NAIC) currently is working to update its model insurance data privacy law for states to consider for adoption.

Last year, in a letter to the NAIC, ALTA requested the inclusion of a small-business exemption to the model law due to the cost of implementing a comprehensive data privacy program.

Help Shape Policy at ALTA Advocacy Summit

Your voice is one of the most powerful tools for change. At ALTA Advocacy Summit, title professionals come together to share their expertise, tell their stories and shape public policy. In a year of transition, with a new president and Congress, this is your chance to make an impact where it counts. Join us May 5-7 in Washington, D.C., to ensure the concerns of title professionals are heard loud and clear.

Congressional staff and policymakers rely on your firsthand experience to understand how legislation affects businesses, homebuyers and communities. Together, we can share the stories and expertise that shape the future of the title industry, ensuring our role in safeguarding American property rights is fully understood and supported.

Click here to register.

ALTA 2025 TIPAC Donors

The Title Industry Political Action Committee (TIPAC) is ALTA's voluntary, nonpartisan political action committee (PAC). TIPAC raises money to help elect and re-elect candidates to Congress who understand and support the issues affecting the title industry. So far in 2025, TIPAC has raised $199,712 from 119 people. In addition, 19 companies have pledged $138,750 to the TIPAC Education Fund. Check out who has supported the industry at alta.org/tipac.

ALTA, Housing Trade Groups Applaud Reintroduction of Bipartisan Congressional Real Estate Caucus

ALTA along with 13 housing trade groups, thanked U.S. Reps. Mark Alford (R-Mo.), Tracey Mann (R-Kan.), Luis Correa (D-Calif.) and Brittany Pettersen (D-Colo.) for reintroducing the Bipartisan Congressional Real Estate Caucus.

Other groups thanking the members of Congress include, the National Association of Realtors (NAR), National Multifamily Housing Council (NMHC), National Apartment Association (NAA), Mortgage Bankers Association (MBA), Real Estate Technology and Transformation Center (RETTC), US Mortgage Insurers (USMI), National Association of Home Builders (NAHB), LGBTQ+ Real Estate Alliance, Asian Real Estate Association of America (AREAA), National Association of Hispanic Real Estate Professionals (NAHREP), American Property Owners Alliance (APOA), National Association of Real Estate Brokers (NAREB) and Leading Builders of America.

The desire for homeownership and housing development is strong nationwide, yet the shortage of affordable housing units and limited supply continues to hinder countless Americans from realizing this dream. It is crucial for Congress to back policies that drive growth in the real estate sector, a mission central to the goals of the reintroduced caucus. Last year, the caucus urged the FHFA to halt its misguided title insurance waiver pilot until the agency solicits public input and thoroughly vets the program.

Tackling the affordability crisis begins with addressing the nation's critically low housing inventory. Research from leading economists reveals that the United States is short more than 4.5 million housing units, reflecting a severe underinvestment in housing infrastructure and driving home costs way beyond an affordable threshold for many Americans. U.S. tax policy must play a greater role in fostering homeownership, strengthening communities, expanding rental housing across all price points and driving economic growth. The groups commended the caucus for initiating vital discussions on overcoming the barriers to building affordable housing and easing the challenges first-time buyers face in entering the market.

"We commend Representatives Alford, Mann, Correa and Pettersen for continuing to lead the Bipartisan Congressional Real Estate Caucus in the 119th Congress," ALTA said. "Title and settlement professionals nationwide work every day to protect homebuyers and their property rights. At the core of those efforts is expanding the dream of homeownership and enhancing housing affordability and opportunity for all Americans. We look forward to working with the Caucus in advancing common sense policies to support this critical need."

Membership by the Numbers

ALTA is the title insurance and settlement services industry resource for advocacy, education, communications, networking and policy standards. Here's a look at some membership figures from the past month.

- New Members: 39
- Title Agents: 27
- New Attorney Members: 4
- State With the Newest Members: Florida and Georgia with 7
- Total Members: 4,546

CALENDAR

2025 ALTA EVENTS

ALTA EDGE
March 19-21
Louisville, Ky.

ALTA ADVOCACY SUMMIT
May 5-7
Washington, D.C.

For more information, go to alta.org/events.

STATE CONVENTIONS

Oklahoma
Norman, Okla.
April 24-26

Arkansas
Branson, Ark.
May 7-9

Tennessee
Chattanooga, Tenn.
May 7-9

Montana
Helena, Mont.
May 14-16

Palmetto
Mount Pleasant, S.C.
May 14-16

Pacific Northwest
Coeur d'Alene, Idaho
May 19-21

New Mexico
Bernalillo, N.M.
May 22-23

Strategies to Combat Wire Fraud

Multilayered Approach to Security Helps Combat Attacks

BY JEREMY YOHE

In 2012, former FBI Director Robert Mueller opined, "There are only two types of companies: those that have been hacked and those that will be." That statement rings true 13 years later. Today, wire fraud remains one of the most pressing threats facing title and escrow companies. Fraudsters are becoming increasingly sophisticated, leveraging business email compromise, seller impersonation and even deepfake technology to infiltrate transactions.

As the threats have escalated, the types of strategies criminals use to steal funds continue to evolve. This highlights the importance of continuous training, robust verification processes and industry collaboration to protect businesses and consumers from financial loss.

"We know that real estate transactions are prime targets for fraud due to their high-value nature," said Jewel Quintyne, senior title operations consultant at Qualia. "The numbers are staggering—$145 million in adjusted losses from cybercrime in 2023 alone, according to the FBI."

Why Wire Fraud is a Growing Concern

Real estate transactions are attractive targets for fraudsters due to the large sums of money involved. "Just one or two fraudulent transactions can result in a huge payday for cybercriminals," Quintyne noted.

In addition, one in four title companies reported experiencing a seller impersonation attempt in 2023, according to a study conducted by ndp | analytics. When the next report come out, it's expected this number increased in 2024.

Nikki Pfleger, executive vice president and specialty deposits relationship manager lead at Encore Bank, highlighted another reason real estate transactions are particularly vulnerable: consumer inexperience. "These scams work because buyers and sellers don't always know what to expect," she said. "They trust the professionals they're working with, and fraudsters exploit that trust."

Emerging Trends: Deepfake Technology and Seller Impersonation

A growing concern in real estate fraud is the use of deepfake technology, which allows criminals to manipulate audio and video to impersonate legitimate parties.

Quintyne highlights the 2025 Entrust Identity Fraud Report that showed a deepfake fraud attempt occurs every five minutes. "These scams are getting more sophisticated, making it harder for professionals to identify fake identities," she added.

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 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 compromised 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

Sources: FBI's 2023 Internet Crime Report; SlashNext State of Phishing Report 2023; ALTA; Qualia

STOCK.ADOBE.COM / FRESHIDEA.

Fraudsters also exploit gaps in title verification processes to commit seller impersonation fraud, particularly in transactions involving vacant land or unencumbered properties.

"One of my clients recently caught a seller impersonation scam because of a simple discrepancy—the name on the seller's email didn't match how they signed legal documents," Pfleger said. "That small detail led her to investigate further, and she ultimately prevented a fraudulent sale."

These incidents highlight the critical need for increased vigilance and verification throughout the entire transaction process.

Best Practices to Prevent Wire Fraud

To effectively combat fraud, title professionals must take a multi-layered approach to security, focusing on people, process and technology, Quintyne recommended.

1. Strengthening Employee Training and Consumer Awareness

People are the first line of defense against wire fraud. Continuous training helps employees recognize red flags and respond effectively to potential threats.

"Fraudsters rely on urgency to pressure employees into bypassing security measures," Pfleger explained. "If a request seems rushed, that's a red flag."

According to an ALTA survey of title companies:

- 78% conduct employee training at least once a year.
- 62% provide training on a weekly, monthly or quarterly basis.

However, experts warn annual training is not enough. "Fraud tactics evolve rapidly," Quintyne stressed. "Companies that implement frequent training sessions—whether monthly or quarterly—are more successful in stopping scams before they happen."

In addition to training employees, consumer education is equally important. "Most scams can be avoided if consumers know to verify wire instructions directly with their title company," Quintyne added.

To raise awareness, title companies should:

- Provide written warnings in emails and transaction documents.
- Encourage consumers to call a known number before wiring funds.
- Offer educational materials about common fraud tactics.

ALTA provides several **resources** to help title and settlement companies protect against wire fraud and to raise awareness about the threat with customers. Here are a few:

- **ALTA Outgoing Wire Preparation Checklist:** Companies can use this checklist as a best practice for verifying outgoing wire information.
- **ALTA Rapid Response Plan for Wire Fraud Incidents:** This documented process has been developed by the ALTA Information Security Committee.
- **Protect Your Money From Wire Fraud Schemes Video:** Buying and selling a home is an exciting time, but there can be pitfalls for unsuspecting consumers.
- **ALTA Wire Fraud Infographic:** This handout explains the steps a consumer should take to avoid becoming a victim of wire transfer fraud.

2. Implementing Rigorous Verification Processes

Verification procedures must be thorough and multi-layered to reduce the risk of fraud. Key steps include:

- Using secure communication portals instead of email to prevent business email compromise.

9 Red Flags to Identify Deepfakes Targeting Financial Institutions

The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued an alert to help financial institutions identify fraud schemes associated with the use of deepfake media created with generative artificial intelligence (GenAI) tools.

FinCEN said the potential for deepfake media to be used in fraud schemes is one of several risks associated with emerging GenAI technologies.

GenAI provides the ability to produce synthetic content that is difficult to distinguish from unmodified or human-generated outputs. GenAI-rendered content that is highly realistic is commonly referred to as "deepfake" content or "deepfakes." Deepfakes can manufacture what appear to be real events, such as a person doing or saying something they did not actually do or say.

FinCEN's analysis of Bank Secrecy Act (BSA) data indicates that criminals have used GenAI to create falsified documents, photographs and videos to circumvent financial institutions' customer identification, verification and customer due-diligence controls.

For example, some financial institutions have reported that criminals employed GenAI to alter or generate images used for identification documents, such as driver's licenses or passport cards and books. Criminals can create these deepfake images by modifying an authentic source image or creating a synthetic image. Criminals have also combined GenAI images with stolen personal identifiable information (PII) or entirely fake PII to create synthetic identities.

Additional FinCEN analysis shows these criminals have opened accounts using fraudulent identities suspected to have been produced using GenAI. These accounts have been used to launder proceeds from other fraud schemes, including loan fraud.

Red Flags

FinCEN has identified the following red flags to help detect, prevent and report potential suspicious activity related to the use of GenAI tools:

1. A customer's photo is internally inconsistent (e.g., shows visual tells of being altered) or is inconsistent with their other identifying information (e.g., a customer's date of birth indicates that they are much older or younger than the photo would suggest).
2. A customer presents multiple identity documents that are inconsistent with each other.
3. A customer uses a third-party webcam plugin during a live verification check. Alternatively, a customer attempts to change communication methods during a live verification check due to excessive or suspicious technological glitches during remote verification of their identity.
4. A customer declines to use multifactor authentication to verify their identity.
5. A reverse-image lookup or open-source search of an identity photo matches an image in an online gallery of GenAI-produced faces.
6. A customer's photo or video is flagged by commercial or open source deepfake detection software.
7. GenAI-detection software flags the potential use of GenAI text in a customer's profile or responses to prompts.
8. A customer's geographic or device data is inconsistent with the customer's identity documents.
9. A newly opened account or an account with little prior transaction history has a pattern of rapid transactions; high payment volumes to potentially risky payees, such as gambling websites or digital asset exchanges; or high volumes of chargebacks or rejected payments.

Best Practices

FinCEN has identified certain best practices that may help financial institutions reduce their vulnerability to deepfake identity documents. For example, multifactor authentication (MFA), including phishing-resistant MFA and live verification checks in which a customer is prompted to confirm their identity through audio or video, are two such processes. ALTA's Best Practices recommends the use of MFA. Click here to learn how to install an MFA app.

Deepfakes: The New Face of Video Biometric Fraud

Fraudsters use several techniques to target a biometric check. These differ depending on whether the biometric check involves a static photo (selfie) or a video element (video/motion).

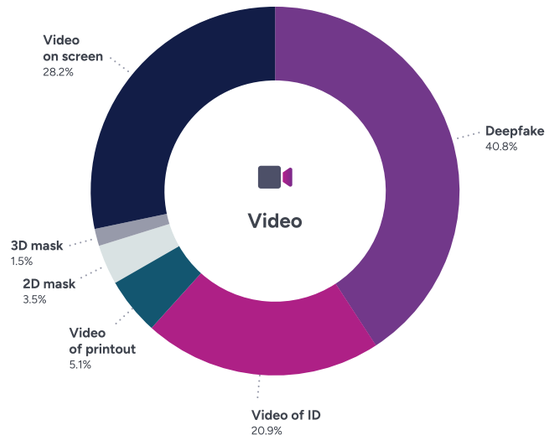


Photo on screen (selfie only): A photo of an image on screen (such as a profile picture from a social media account)

Photo of printout (selfie only): A photo of an image printed on paper

Photo/Video of ID: A photo or video of the face on the identity document

2D mask: A photo or video of a 2D-printed mask

3D mask: A photo or video of a 3D mask or other 3D object

Deepfake: Digitally manipulated photo or video where a person's face is altered to appear as someone else

Video on screen (video/motion only): A video of a video on a screen

Video of printout (video/motion only): A video of an image printed on paper

Source: Entrust Identity Fraud Report 2025

- Verifying identities early and throughout the transaction—not just before closing.
- Conducting call-back verifications using previously verified phone numbers, not numbers provided in emails.

Quintyne also suggested title and settlement companies maintain a Written Information Security Plan (WISP), which is now required in ALTA's Best Practices. They should also ensure vendors' security is consistent with their own company standards, periodically review system login activity and look for anomalies and suspicious behavior, keep systems updated with latest patches and maintain strong banking relationships.

A common red flag is an urgent request for wire changes. "Fraudsters want to create a sense of urgency to prevent verification," Pfleger noted. "They push for quick action because once the money is wired, it's gone."

Another dangerous type of transaction involves LLCs and other corporate structures:

- Independently verify corporate documents through official state websites.
- Scrutinize changes in ownership or management—sudden transfers may indicate fraud.
- Look for inconsistencies in naming conventions (e.g., "Company LLC" vs. "Company CO").

"A small detail like a missing letter or abbreviation can be the difference between catching a fraud attempt or losing thousands of dollars," Pfleger warned.

3. Leveraging Technology to Detect Fraud

Technology can strengthen fraud prevention efforts when used correctly. Title professionals should integrate:

Wire Fraud Detection Software

Modern fraud detection tools analyze multiple data points to flag suspicious activity. Features to look for include:

- Public record checks to verify ownership history.
- ID verification software that detects forged or manipulated documents.

- Transaction monitoring tools that identify unusual patterns.

"Technology is a powerful tool, but it's only as strong as the people using it," Pfleger emphasized. "Firms need to carefully evaluate their bank partners, and their software and cybersecurity vendors, and stay proactive in implementing new fraud prevention measures."

Multi-Factor Authentication (MFA) and Secure Portals

Secure communication channels prevent business email compromise by ensuring sensitive information isn't transmitted via unprotected emails. Many regulations require MFA. The latest iteration of ALTA's Best Practices now requires the use of MFA.

"Fraudsters will exploit any weak link," Pfleger cautioned. "Every organization should be using multi-factor authentication, password management protocols and encrypted communication tools."

The Role of Industry Collaboration

Stopping wire fraud requires cooperation between title companies, financial institutions and law enforcement agencies.

"The bad actors are sharing information," Quintyne noted. "That means we need to do the same. If an attempt happens, report it. The more data we share, the better we can protect ourselves."

ALTA urges companies to report fraud incidents to the FBI's Internet Crime Complaint Center (IC3.gov). Even if a fraud attempt is unsuccessful, reporting it helps law enforcement track trends and build cases against these criminals, Quintyne added.

Staying Ahead of the Fraudsters

As fraud tactics evolve, businesses must remain proactive, adaptable and collaborative in their defenses.

"Crime thrives in silence," Pfleger said. "It may feel embarrassing if your company experiences an attack, but hiding it only helps the fraudsters. The more we share and collaborate, the better we can protect our industry."

Quintyne emphasized that wire fraud isn't going away, but companies can stay ahead by continuously improving their security strategies.

"Fraud prevention isn't just about reacting—it's about preparing," she said. "Strengthen your people, processes and technology. The more layers of defense you have, the harder it becomes for criminals to succeed."

"By prioritizing employee training, consumer education, robust verification processes and advanced technology, title companies and escrow agents can significantly reduce the risk of wire fraud and protect their clients from devastating financial losses," Quintyne concluded. ■

JEREMY YOHE *is ALTA's vice president of communications. He can be reached at jyohe@alta.org.*

STOCK.ADOBE.COM / FRESHIDEA.

Title Companies Help Mitigate Risk of Wire Fraud, ALTA Cybercrime Study Shows

Title professionals continue to be targeted by attempts to steal funds from real estate transactions, but consumer education and staff training are helping mitigate losses, according to ALTA's latest cybercrime study.

More than 40% of title companies reported receiving at least one email per month in 2023 attempting to change wiring/payoff instructions. Despite the monthly attempts, only 7% of companies sent wire funds to a fraudulent account, the CertifID-sponsored study of 360 participants showed. Meanwhile, 13% of respondents reported their customers wired funds to a fraudulent account.

"Title and settlement companies take protecting their clients' funds extremely seriously," said Diane Tomb, ALTA's chief executive officer. "That's why title professionals make it a priority to educate consumers about wire transfer fraud. By raising awareness about red flags, secure communication practices and verification steps, homebuyers are better equipped to protect their hard-earned money from cybercriminals. Knowledge is the first line of defense in ensuring a safe and secure homebuying experience."

Title companies utilize an array of tools to mitigate the risk of wire fraud, including consumer (51%) and real estate agent (37%) training, wire/payee verification software (48%) and simulated phishing email testing of employees (26%). These mitigation efforts require investments by title companies ranging anywhere from $1,000 to $25,000 annually, the survey showed.

An overwhelming majority of title companies inform and warn consumers about cybercrime risks through email (84%) or by telephone/in person (72%). In addition, title companies also mail information to consumers about cyber risks and provide warnings on their websites.

Internally, 78% of companies that took the survey train employees at a minimum on a yearly basis on identifying and preventing wire fraud attempts, with 62% educating staff weekly, monthly or quarterly.

"It's clear the title industry has taken many proactive steps to protect and educate their customers about the threat of wire fraud, but cyberattacks continue to evolve and are becoming more difficult to recognize," Tomb said. "Protecting against criminal actors takes a collaborative approach from everyone involved in real estate and mortgage transactions."

Additional Survey Highlights

- 94% of title companies remain concerned about the threat of wire fraud over the next 12 to 18 months.
- About half the companies that took the survey reported cybercrime attacks targeting their operation stayed the same in 2023 compared to 2022, while 40% reported attacks increasing slightly or significantly.
- Results were similar for attacks targeting customers, with 52% of companies reporting the number of attacks on customers remained the same when comparing 2023 versus 2022. Meanwhile, 39% reported cyberattacks on customers increased slightly or significantly year-over-year.

Wire Fraud Resources

ALTA provides several resources to help title and settlement companies protect against wire fraud and to raise awareness about the threat with customers. Here are a few:

- Protect Your Money from Wire Fraud Schemes Video: Buying and selling a home is an exciting time, but there can be pitfalls for unsuspecting consumers.
- ALTA Wire Fraud Infographic: This handout explains the steps a consumer should take to avoid becoming a victim of wire transfer fraud.
- ALTA Outgoing Wire Preparation Checklist: Companies can use this checklist as a best practice for verifying outgoing wire information.
- ALTA Rapid Response Plan for Wire Fraud Incidents: The standard ALTA Rapid Response Plan for Wire Fraud Incidents has been developed by the ALTA Information Security Committee.

More resources can be found on ALTA's website.

Mapping Out Elements of a Robust Cybersecurity Implementation Program

Training, Education of Staff Must Be Continuous, Comprehensive

By Shawn Fox

CYBERSECURITY IS AN ESSENTIAL ELEMENT OF EVERY MODERN BUSINESS in an era of escalating cybercrime. But for the title insurance industry, it is imperative digital security is given the highest priority not only for the safety of the internal processes of the title agency itself, but also for the protection of the customer information and funds that flow through the agency's systems every day. Our industry is being called on to protect consumers and secure their real property at a level we've never seen before.

It is no longer a question of "if" or "when" something might happen, since more than 90% of U.S. companies are reporting recent cyber intrusion attempts. Consider the statistics from the FBI's 2023 Internet Crime Report issued last year:

- IC3 received 880,418 complaints in 2023
- Potential losses exceeded $12.5 billion
- Losses to investment scams rose from $3.31 billion in 2022 to $4.57 billion in 2023
- 21,489 BEC complaints were received, amounting to $2.9 billion in losses
- Ransomware incidents increased 18% with reported losses rising 74%

This escalating danger can only be contained by a comprehensive cybersecurity program that encompasses not only broad technology protections, but also the internal company practices and safety measures to prevent cybercriminals from gaining a foothold through unwary individuals within your company, your customer base or lurking behind a well-crafted phishing email.

Create a Plan

The purpose of a cybersecurity plan is threefold: to ensure the security and privacy of sensitive customer data, to meet the strict regulatory requirements that exist to protect customers from fraud and ensure fair transactions, and to build and maintain client trust through appropriate risk management protocols.

There are four key steps to consider when establishing a strong cybersecurity program:

- **Assessment:** An evaluation of current security measures and vulnerabilities.
- **Strategic Planning:** Developing a robust strategy to address cybersecurity risks
- **Employee Training:** Educating staff to recognize and prevent breaches
- **Implementation:** Putting security measures into action across the organization.

To ensure all of these goals are met, it is helpful to appoint someone within the company who is designated as the cybersecurity monitor. This person would be responsible for overseeing and implementing security measures and also tasked with the ongoing process of analyzing and mitigating potential cyber threats.

As you are setting up your program, there are seven primary focus areas to include in your plan, including cybersecurity awareness training, access control measures, configuration and patch management, email security, endpoint detection and response (EDR), backup and disaster recovery, and managed detection and response (MDR).

Cybersecurity Awareness Training

One cannot emphasize strongly enough that it is often human error that opens the door to outside threats. The only way to mitigate human error is through education, and that training must be comprehensive and ongoing.

Often, employees don't understand that their actions may be dangerous, such as when they access applications and software outside company-approved programs.

This use of "shadow IT" can be managed through careful monitoring and the creation of safe portals, but the top security measure to mitigate access is to make employees aware of the dangers and how to prevent unwanted intrusion.

In addition, surveys have shown employees often circumvent security protocols to work more efficiently and—often unknown to the company—regularly email documents to their unprotected at-home computers to continue their work into the evening or over the weekend.

It is not sufficient to provide a cybersecurity handout or post the rules and regulations for all to see. Employees must see actual cyberthreats through interactive training modules to gain a deeper understanding of what the threats look like and to become proficient at knowing when and how to take action.

This can be accomplished in-house but tapping a professional security training company such as Phin Security or KnowBe4 security awareness training, may ensure a more robust and effective training program for your staff.

An effective cyber security awareness training program should include interactive training modules, social engineering simulations with real-life scenarios and simulated phishing emails to test employees' responses and enhance awareness of phishing threats.

Access Control Measures

The first consideration in creating a more secure system is limiting access to data, applications and resources to only those persons and devices within the company that require this access to do their jobs. By limiting unnecessary access, you curtail exposure and make it easier to track intrusion in a more limited pool.

The second consideration is authentication. Creating a program that emphasizes secure login credentials, strict password policies and advanced multi-factor authentication can dramatically reduce intrusion risk.

Encryption of data is the third pillar of a strong access control protocol. This is another area that is particularly critical for title

agents, since highly sensitive personal data can easily be put at risk if not protected.

And finally, an ongoing monitoring and auditing program which looks at user activities and points of access is imperative.

As has already been acknowledged, human error is often what opens the door to cyber intrusion, so leaving password selection and management up to the individual within the company can sometimes be a dangerous game in the title world. The safer way to approach this dilemma is to use password management software such as NordPass or LastPass.

Secure Configuration, Patch Management

Secure configuration are those measures that are established when installing new systems. It is never sufficient to rely on default configurations because out-of-the-box systems are designed for simplicity first and security second. Always go above and beyond when considering what is needed when installing new equipment and programs.

Essential security protocols include establishment of firewalls, automation of patch management, installation of malware protection, and establishing strict access control, which is covered above.

In addition, some basic system hygiene practices include:

- Deleting obsolete user accounts
- Changing default passwords
- Removing unnecessary or antiquated software
- Disabling autorun features
- Implementing geographic access restrictions

Email Security

Title agencies are prone to business email compromise schemes, so email security is a high priority. Authentication, encryption, and education are foundational for eliminating this threat.

Establishing a requirement for strong and unique passwords for email accounts and implementing multi-factor authentication should be compulsory.

End-to-end encryption for emails is a highly effective deterrent, since only the sender and the recipient can read the content of messages. Returning to the human element, raising awareness about email security best practices through ongoing training can minimize the most vulnerable issue in email security.

And finally, make sure you have a protocol for backing up email data to prevent loss in the event of a cyberattack or hardware failure.

Managed Detection and Response (MDR)

An MDR is a security solution that looks at all the activity occurring within the larger enterprise system and constantly monitors for cyber threats. This includes anything that feeds into or accesses the company's systems and could potentially provide an entry point for cyber intrusion, such as:

- Laptops
- Mobile devices
- Printers
- Servers
- Tablets
- Network-attached storage devices
- Battery Backup units

MDR solutions monitor each login, downloaded file and unusual actions taken on the network. Once identified, it works to block that activity and alert the organization of the potential risk.

MDR is about speed. It is a see all/know all application that can react much more quickly to identify and shut down threats. SentinelOne Vigilance and SMB Defender are examples of these types of solutions.

Backup and Disaster Recovery

Pillar 3 of ALTA's Best Practices addresses the important of having a written information security plan (WISP), which includes having a backup and recovery plan for data in the case of a loss of access to technology through a cyber intrusion or natural disaster.

Backups protect against data loss due to hardware failures or cyberattacks and ensure data integrity and quick recovery from such disasters. Off-site backups and cloud storage solutions can not only mitigate losses but can also ensure the agency is up and running again in short order.

In addition to implementing backup and recovery processes, agencies should test these systems on a regular basis to ensure their effectiveness.

Security Operations Center (SOC)

Whereas MDR is a solution embedded in the system, SOC is a service that combines a range of solutions with an expert cybersecurity team. Security teams can provide a range of services, but the biggest advantage is that they provide 24/7 monitoring and guidance so you are getting constant input on how to improve your security systems.

SOC also relies on advanced technologies and—in addition to providing monitoring and detection—can manage incident responses, advanced threat hunting, forensics and analysis, plus reporting and communication.

Never Trust, Always Verify

Finally, the underlying approach to a robust cybersecurity system is the concept of "zero trust" security, which is a holistic security approach that encompasses continuous monitoring, micro-segmentation and strict access controls.

Implementing zero trust involves a fundamental shift toward explicit verification and authentication of all resources to ensure the ongoing safety of data and systems.

How robust a cybersecurity system each agency needs is going to entirely depend on the size of the company and the complexity of its technology. However, even in a small agency, strong security practices are available and within reach to effectively secure the company and the information of its customers.

SHAWN FOX *is chief revenue officer for Premier One, a cybersecurity and managed services firm serving the title insurance and community banking industries. He can be reached at shawnf@premier-one.com.*

U.S. District Court in Michigan Holds Bank not Liable for Fraudulent Wire Transfer

By Stephen Gregory

Citation

Title, Inc. v. U.S. Bancorp*, 2024 WL 3761258, --- F.Supp.3d--- (August 12, 2024), U.S. District Court, E.D. Michigan, Southern Division*

Facts

Title Inc. (Title) was handling a refinance transaction for Jeffrey and Karyn Carter which was to pay off an existing mortgage of approximately $139,000 to lender Mortgage 1. In conjunction with the payoff, Mortgage 1 emailed a payoff to Title directing the payment be made to a Chase Bank account. Some five days later, Title received an email purported to be from Karyn Carter stating that she had discovered an error in the instructions and to be on the lookout for an updated payoff from Mortgage 1. Subsequently, Title received a fax payoff directing the payment be sent to an account at U.S. Bank. After closing, Title wired the "payoff" funds to U.S. Bank to the account number listed on the faxed payoff, with instructions that it was to be to the credit of Mortgage 1 in payment of its loan. In reality, the account number to which the wire was directed belonged to an individual, not Mortgage 1, and the funds were quickly drained. Title then sued U.S. Bank alleging that when it determined the name of the owner of the account did not match the name of the intended beneficiary, U.S. Bank should have taken steps to refuse the wire transfer.

In addition to common law claims of negligence, breach of contract, fraud and conversion, Title relied primarily on Article 4A of the Michigan Uniform Commercial Code.

Holding

Article 4A of the Michigan UCC provides that the originator of a wire transfer must provide (1) the amount; (2) the transferee's account number, and (3) the name associated with the transferee's account number. However, citing *Harrington v. PNC Bank, N.A., 684 F.Supp.3d 631 (E.D. Mich. 2023),* the court held that when a payment order includes the account name and the account number, banks have no duty to check if the account name and number match and are free to rely upon the account number only. The court held that banks are only liable if the account number refers to a nonexistent account or if the bank has actual knowledge of a mismatch. Having determined that there was no liability on U.S. Bank under Article 4A, the court then held that the common law claims were pre-empted by the UCC and, therefore, dismissed those claims as well.

Importance to the Title Industry

Cyber fraud continues to plague the real estate industry due in no small part to the amount of money that can be stolen in any one transaction. Hacked emails and bogus payoff statements are but one source of theft, but perhaps the easiest to prevent by parties to a real estate transaction. Courts are consistently holding that the transmitter of funds has the last and best clear chance to prevent a fraud; that then makes it incumbent upon the agent to take whatever steps it can to ensure that the information it relies upon to send money is in fact valid. The small amount of time it may take to place a call to a verified party can save potentially hundreds of thousands of dollars.

STEPHEN GREGORY *is claims and underwriting counsel for WFG National Title Insurance Co., and a member of the bar in North Dakota, Ohio, Virginia and West Virginia. He is active in the Virginia Land Title Association and the Ohio Land Title Association. He can be reached at sgregory@wfgtitle.com.*

Sneaky New Phishing Attack: Corrupted Word Documents

By Genady Vishnevetsky

There's a new phishing campaign that's using a clever trick: corrupted Word documents. This technique allows malicious content to pass through to the user without detection by any email security tools.

The attacker intentionally (slightly) corrupts the attached Word document so antivirus and security tools can't scan it. Because the file has a .docx extension, when the unsuspecting victim opens it, Microsoft Word detects the corruption and asks the user if they want to repair it. If the user confirms, Word will repair and open the file.

Inside the recovered file is a QR code that leads to a credential harvesting page that steals both the user's credential and the MFA.

The timing of this attack is impeccable. Security firm Any.Run, which discovered it, found the email appeared to come from Human Resources and focused on end-of-the-year benefits and bonus payouts.

Takeaways:

- Hackers frequently time and theme their attacks to seasonal, disaster or business events. Always stay alert during business seasonality, such as end-of-month, quarter, year activities, benefits, payouts, and income-tax events).
- Attackers continuously attempt to find ways to stay under the radar of security technologies. Always proceed with caution.
  - Every attachment from an unknown source should be considered malicious until proven otherwise.
  - Any new behavior (recovery of a corrupted attachment) should be a red flag.
- QR codes have alarmingly become mainstream for cybercrooks due to the inability to analyze the destination with the naked eye. Scrutinize all QR codes and avoid using them in emails and attachments if possible.
- Do not enter any credentials on the site you landed on from the email or attachments unless it came from a trusted and verified source.

FBI Warns Generative AI Used for Financial Fraud

The FBI issued an alert warning that criminals are using generative artificial intelligence (AI) to commit fraud on a larger scale.

Generative AI reduces the time and effort criminals must expend to deceive their targets. The technology takes what it has learned from examples input by a user and synthesizes something entirely new based on that information. These tools assist with content creation and can correct for human errors that might otherwise serve as warning signs of fraud. The creation or distribution of synthetic content is not inherently illegal; however, synthetic content can be used to facilitate crimes, such as fraud and extortion.

Since it can be difficult to identify when content is AI-generated, the FBI provided several examples of how criminals may use generative AI in their fraud schemes to increase public recognition and scrutiny. Fraudsters may use generative AI to create fake text, images, audio (vocal cloning) and videos.

Tips to Protect Yourself

- Create a secret word or phrase with your family to verify their identity.
- Look for subtle imperfections in images and videos, such as distorted hands or feet, unrealistic teeth or eyes, indistinct or irregular faces, unrealistic accessories such as glasses or jewelry, inaccurate shadows, watermarks, lag time, voice matching and unrealistic movements.
- Listen closely to the tone and word choice to distinguish between a legitimate phone call from a loved one and an AI-generated vocal cloning.
- If possible, limit online content of your image or voice, make social media accounts private, and limit followers to people you know to minimize fraudsters' capabilities to use generative AI software to create fraudulent identities for social engineering.
- Verify the identity of the person calling you by hanging up the phone, researching the contact of the bank or organization purporting to call you, and call the phone number directly.
- Never share sensitive information with people you have met only online or over the phone.
- Do not send money, gift cards, cryptocurrency or other assets to people you do not know or have met only online or over the phone.

GENADY VISHNEVETSKY *is chief information security officer for Stewart Title Guaranty Co. and chair of ALTA's Information Security Work Group. He can be reached at genady.vishnevetsky@stewart.com.*

Industry Update

Qualia Acquires RamQuest, E-Closing

Qualia Labs will acquire the RamQuest and E-Closing platforms from Old Republic National Title Holding Co.

The companies announced that the partnership represents a shared vision for the future of technology in the title industry. By combining Qualia's technology solutions and Old Republic Title's industry experience, Qualia and Old Republic believe the partnership will deliver enhanced value and efficiency.

"Old Republic Title has been a leader in real estate technology for decades, and we're excited to partner with their leadership and technology teams," said Nate Baker, CEO of Qualia. "We believe that this strategic partnership will enable Old Republic Title to be the title insurer best positioned to take advantage of the coming AI wave, and to be at the forefront of our industry's technological evolution. We are excited to build a large-scale, long-term strategic partnership with Old Republic Title that has meaningful benefits to both businesses, our mutual customers and our industry."

The deal allows Qualia to expand the capabilities of title production offerings, which Old Republic will use to support its direct division, agents and customers. In 2020, Qualia acquired Adeptive Software, the developer of title and escrow production software ResWare.

"Technology has become integral to the process of conducting smooth and secure real estate transactions," said Carolyn Monroe, President and CEO of Old Republic Title. "Throughout Old Republic Title's 117-year history in serving the American homeowner, we have embraced opportunities to improve the method of transferring real estate. As the speed of technological innovation in our industry accelerates, partnering with Qualia will help us provide an improved experience for both our agents and our insureds. It creates a mutually effective path for offering the expertise of Qualia in the rapidly changing technology environment, and the strength of Old Republic Title as a leader in the title industry."

Utah Regulator Fines Title Companies for Closing Deals Without Lender's Policies

The Utah Insurance Department in November took regulatory action against three title companies for violating state law by closing transactions without issuing lender's title insurance policies.

In a Notice of Agency Action, the department ordered Silver Leaf Title Insurance Agency to pay a fine of $6,111.07 for closing eight transactions through United Wholesale Mortgage's (UWM) Trac Loan Program. According to the notice, the title company did not issue lender's title policies as required by Utah law.

According to another Notice of Agency Action, Title Guarantee LLC issued letter reports on two transactions, which the title company acknowledged "is not a title insurance policy and should not have been issued in lieu of a title insurance policy during the settlements/closings." The Utah Insurance Department ordered the title company to avoid issuing letter reports in lieu of a lender's policy and to pay a fine of $892.50.

In addition, following an investigation opened in September 2024, the Utah Insurance Department discovered South Valley Title Insurance Inc. was included on a list to provide closing/settlement services for UWM's Trac Loan Program. The department reported South Valley Title closed one transaction without issuing a lender's policy. The department ordered South Valley Title to avoid issuing letter reports in lieu of a lender's policy and to pay a fine of $585.

HUD to Modify Procedures for Partial Claim Payoffs, Extend Recording Time

In a draft Mortgagee Letter, the U.S. Department of Housing and Urban Development announced it will extend the time allowed to record partial claim security instruments and establish a new procedure for mortgagees to obtain and provide partial claim payoff statements.

The changes will apply to all FHFA Title II single-family forward mortgage programs.

According to the draft letter, mortgagees will need to submit executed partial claim security instruments for recordation within 15 business days from:

- the date of receipt from the borrower, or
- bankruptcy court approval, if required; or
- where HUD execution is required, receipt from HUD
- If there are any outstanding partial claims or payment supplements associated with a mortgage when a mortgagee receives a payoff request for an FHA-insured mortgage, the mortgagee will need to:
- include a letter with the payoff statement for the FHA-insured mortgage that indicates the borrower has one or more outstanding partial claim(s) or payment supplement(s) and information about how to obtain a payoff statement from HUD
- submit the email address and/or fax number where the partial claim payoff statement should be sent in HUD's SMART Integrated Portal (SIP) – Partial Claim Payoff Dashboard.

Mortgagees will be responsible for ensuring the accuracy of the data entered into SIP. Mortgagees must confirm payoff statements have been successfully delivered by verifying the status of the partial claim payoff statements in the Partial Claim Payoff Dashboard in SIP. When a payoff statement has not been successfully delivered, as indicated in SIP, mortgagees must obtain the partial claim payoff statement from the dashboard in SIP and provide it directly to the requestor. Where partial claims have not been legally recorded and delivered to HUD or a claim has not been filed, mortgagees must produce and provide a payoff statement for any partial claims to the requestor.

In addition, mortgagees will need to be retained in the servicing files, including documentation of any payoff statement for partial claim(s) that were provided by the mortgagee. Last year, HUD reported persistent instances in all areas of the country where the lien is successfully recorded but not detected by title agents.

Treasury Suspends Enforcement of BOI Reporting

The Treasury Department announced it will not enforce any penalties or fines associated with the beneficial ownership information reporting rule required under the Corporate Transparency Act (CTA).

The rule requires roughly 32 million legal entities to file a report on their beneficial ownership with the Treasury Department's Financial Crimes Enforcement Network. Most title companies were already exempt from this reporting requirement due to the rule's exemption for state licensed insurance producers.

This move follows efforts by department lawyers attempts to dissolve injunctions in cases assessing the constitutionality of the statute, following a Supreme Court opinion earlier this year indicating the law was constitutional

Additionally in the announcement, the Treasury said it will issue proposed rulemaking that will narrow the scope of the BOI rule to only foreign reporting companies. Treasury is likely to face legal challenges in its effort to alter the law. Generally, it's viewed as an abuse of power when an agency issues a rule that is inconsistent with its authorizing act.

31 USC 5336(b) states, "In accordance with regulations prescribed by the Secretary of the Treasury, each reporting company shall submit to FinCEN a report..." The law specifically defines a reporting company to mean, "a corporation, limited liability company, or other similar entity that is—(i)created by the filing of a document with a secretary of state or a similar office under the law of a State or Indian Tribe; or (ii)formed under the law of a foreign country and registered to do business in the United States by the filing of a document with a secretary of state or a similar office under the laws of a State or Indian Tribe;"

While courts have held that regulators can impose additional or more specific requirements, they may not generally add to, detract from or modify the statute. An initial question will be whether any litigant other than Congress has the standing to sue. Courts are more likely to scrutinize agency motives in the wake of the repeal of the Chevron doctrine by the US. Supreme Court.

The Treasury's announcement could still impact the title and settlement services industry as it works to prepare for the anti-money laundering (AML) regulations for residential real estate transfers. This rule, which goes into effect Dec. 1, 2025, requires real estate professionals to submit reports and keep records about certain high-risk, non-financed transfers of residential real property to specified legal entities and trusts.

Over the past few years, ALTA has worked with allies in Congress and FinCEN to try to narrow the scope of the AML rule. While this latest announcement doesn't directly affect the AML rule, it could impact ALTA's ability to obtain further relief for the industry either because Treasury is more open to changes or because the data provided by settlement agents under the rule becomes more valuable.

Georgia Law Requires Proper ID When Filing Documents

January 30, 2025

A law that went into effect Jan. 1 requires a process to validate a person's identity when any real estate or property records are filed.

Georgia HB 1292 was enacted to ensure that the "persons presenting electronic documents for recording provide identifying information," according to the state Legislature.

Under the new law, self-filers of any documents affecting real estate and personal property must do so via electronic filing. A self-filer is anyone who is not an insurance agent, attorney, bank or credit union agent, mortgage lender or servicer, land surveyor or public official.

As part of the e-filing, the self-filer must provide any information requested, including their driver's license, passport, military identification card or another type of personal ID card. Additionally, notaries must confirm the identity of the document signer or affirmant through verification of a government-issued photo ID. Notaries are also required to maintain a written or electronic journal that includes an entry for each notarial act performed at the request of a self-filer, and to complete an educational training class related to the new requirements.

In a statement, the state's attorney general's office said, "Title theft occurs when a criminal impersonates a property owner and sells or takes out a second mortgage on the owner's property. In the worst-case scenario, the home goes into foreclosure and/or is deeded to a new purchaser. It is a complicated and expensive process to rectify, if it can be rectified at all."

The law also addresses predatory and unsolicited real estate purchase offers. As of May 2, 2024, solicitations of this nature must state that the offer may not be the fair market value of the property.

Specifically, if the solicitation includes a monetary offer, the following text is required in capital letters: "THIS OFFER MAY OR MAY NOT BE THE FAIR MARKET VALUE OF THE PROPERTY." Further, if

the solicitation includes a monetary offer that is less than the value of the previous year's assessed value for ad valorem taxation by the county tax assessor for the county in which the property is located, the following text is required in capital letters: "THIS OFFER IS LESS THAN THE COUNTY ASSESSED VALUE FOR THIS PROPERTY."

The bill also creates a private right for those individuals who believe they were deceived. To help property owners stay apprised of any unauthorized changes to their deed, they can sign up to receive notifications of certain changes in filing status through the Filing Activity Notification System (FANS) at https://fans.gsccca.org/.

Stewart Title Launches TPS for Attorney Agents

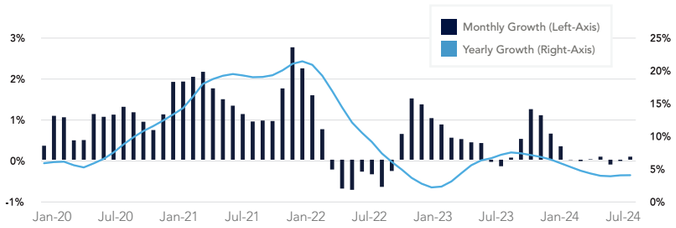
Stewart Title unveiled a new title production system built specifically for attorney agents. Called Connect Close, the system features include streamlined order entry; integrated search orders; document preparation; premium, taxes and recording fee calculations; a customizable document module; advanced closing disclosure and HUD; cost-free setup; a web-based platform; and personalized one-on-one training.

The system is currently available in Connecticut, Massachusetts and Rhode Island.

"With this launch, Stewart is reinforcing its position as a trusted partner in the real estate industry, delivering solutions that align with the evolving needs of attorney-led transactions," said Iain Bryant, group president of Stewart's Agency Services. "As the industry continues to modernize, Connect Close ensures that attorney agents have access to the best tools and resources, making transactions more efficient, reliable and user-friendly than ever before."

House Price and Buying Power Snapshot

First American Data & Analytics National House Price Index, December 2024



Source: First American Data & Analytics, Dec. 2024

+0.1% Monthly Growth

+3.9% Yearly Growth

+54.8% Change from Pre-Pandemic (Feb. 2020)

*The First American Data & Analytics HPI report measures single-family home prices, including distressed sales, with indices updated monthly beginning in 1980 through the month of the current report.

National Consumer House-Buying Power

How much home one can afford to buy given the average income and the prevailing mortgage rate

December 2024

$381,817 House-Buying Power

+5.0% Year-Over-Year

Where House-Buying Power is Strongest

Top States and Markets

1	New Jersey $526,631	1	San Jose, CA $785,434
2	Massachusetts $502,578	2	San Francisco, CA $658,583
3	Hawaii $486,971	3	Washington, DC $620,695
4	Colorado $477,051	4	Boston, MA $542,584
5	Maryland $473,195	5	Denver, CO $524,461

Source: Mark Fleming, Chief Economist at First American Financial Corporation

Have a Plan Before You're Punched in the Face

RICHARD H. WELSHONS MTP, NTP
ALTA president

IN TODAY'S DIGITAL LANDSCAPE, CYBERSECURITY IS NO LONGER AN OPTION—it is a necessity. With the increasing frequency and sophistication of cyber threats, businesses and individuals alike in the title and settlement services industry must implement a comprehensive cybersecurity plan to protect sensitive data, prevent financial losses and maintain trust..

The threat landscape dramatically increased following the introduction of ChatGPT in November 2022. Cybercriminals swiftly adapted, using large language model (LLM) chatbots to launch a multitude of highly targeted phishing attacks at an alarming scale. A report from Europol estimates 90% of online content could be AI-generated by 2026. For cybercriminals, the advent of generative AI tools has ushered in a new era of sophistication, enabling more advanced business email compromise (BEC) attacks, refined social engineering tactics and enhanced malware.

Despite the strides in technological advancements, it's crucial to remember that people remain an organization's most targeted and vulnerable link. The surge in attacks across various platforms—including email, mobile and collaboration tools—serves as a stark reminder of the evolution of cyberattacks. Hackers now also target less protected channels like mobile. This human element of cybercrime underscores the imperative need for comprehensive security measures.

As we all know, data breaches, ransomware attacks and phishing scams can have devastating consequences. A single cyberattack can compromise nonpublic personal information disrupt business operations and lead to significant financial and reputational damage. Without a cybersecurity plan in place, organizations and individuals are left vulnerable to these risks.

Two resources that should be part of any company's cyber playbook are the Written Information Security Plan (WISP) and the Cyber Incident Response Plan (CIRP). These documents serve as a blueprint during a cyberattack. Having these plans prepared and regularly rehearsed is crucial, as many companies fail to practice their response strategies. Pillar 3 of ALTA's Best Practices addresses the importance of having a WISP, which includes having a backup and recovery plan for data in the case of a loss of access to technology through a cyber intrusion or natural disaster.

Professional boxer Mike Tyson once said, "Everyone has a plan until they get punched in the face." He said this in response to a reporter asking if he was concerned about his opponent's fight plan. The point is that, when faced with an unexpected event, it's recommended to adapt your current plan rather than starting over. The same is true with a cyberattack. While the quote illustrates how plans can change with unexpected events, the point, is that you need a plan to begin with.

FNF FAMILY OF COMPANIES

Alamo TITLE INSURANCE
CHICAGO TITLE INSURANCE COMPANY
Commonwealth
Fidelity National Title
National Title

At FNF, we pride ourselves on being more than just a title insurance provider.

Our goal is to help you run your business more efficiently and successfully by providing insight into how a Fortune 500 company operates.

We openly share what we have learned with our agents, empowering them to apply the same principles and processes in their operations.

When you're thinking about who to trust with your business, trust the leader in the industry. Trust the FNF Family of Companies.