

# TITLE NEWS

AUGUST 2019

AMERICAN LAND TITLE ASSOCIATION



## Here Phishy, Phishy

Title Pros Must Be  
Vigilant Against Email  
Phishing Attacks





# Expertise. Quality. Efficiency. Title and Property Report Services

**DataTrace**® provides nationwide title and property report production services across all 50 states and is the leading provider of data and title search automation.



## Expertise

Largest provider of title data with regional, on-shore search and exam experts that have produced millions of reports...and counting.



## Quality

Stringent verification and auditing process conducted on every file to ensure the highest quality and accuracy.



## Efficiency

Single point of contact to manage your entire search and examination process, saving you time managing multiple vendors.

**Call today** to learn how our Title and Property Report Services can give you the quality and efficiency needed to grow your business.

[datatracetitle.com/efficiencyalta](https://datatracetitle.com/efficiencyalta) | 800.221.2056

**DataTrace**®

© 2019 DataTrace Information Services LLC. All rights reserved. DataTrace Information Services LLC makes no expressed or implied warranty respecting the information presented and assumes no responsibility for errors or omissions.



# iN This Issue

VOLUME 98 | NUMBER 8 | AUGUST 2019

## COVER STORY

### 10 Here Phishy, Phishy

## FEATURES

### 8 Former NSA Director to Speak at Address Cybersecurity at ALTA ONE

### 16 Is Your Browser Secure?

### 20 White House Hopes to Eliminate Regulatory Barriers to Affordable Housing

### 21 Q1 2019 Title Premium Volume Dips 5 Percent

### 22 FDIC Highlights RESPA Section 8 Violations in Compliance Report

## DEPARTMENTS

- 5 Publisher's Desk
- 6 ALTA News
- 23 Industry Update
- 28 Movers & Shakers
- 30 Closing Comment



**DON'T MISS THIS MONTH'S  
DIGITAL ISSUE OF**

# TITLENews

The digital edition of **TITLENews** includes a webinar recording that reviews the inner workings of phishing and social engineering techniques often used to launch a fraud scheme and discuss the best practices that could effectively reduce your risk profile.

Go to [alta.org](http://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.

Anyone is invited to contribute articles, reports and photographs concerning issues of the title industry. The Association, however, reserves the right to edit all material submitted. Editorials and articles are not statements of Association policy and do not necessarily reflect the opinions of the editor or the Association.

Reprints: Apply to the editor for permission to reprint any part of the magazine. Articles reprinted with permission must carry the following credit line: "Reprinted from *TitleNews*, the monthly magazine of the American Land Title Association."

©2019 American Land Title Association

Members Call Toll Free: 800-787-ALTA  
Members Fax Toll Free: 888-FAX-ALTA  
Visit ALTA Home Page: [alta.org](http://alta.org)  
Email Feedback to: [service@alta.org](mailto: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**

## ASSOCIATION OFFICERS

PRESIDENT  
**Cynthia Durham Blair NTP**  
Blair Cato Pickren Casterline LLC  
Columbia, S.C.

PRESIDENT-ELECT  
**Mary O'Donnell**  
Westcor Land Title  
Insurance Company  
Maitland, Fla.

TREASURER  
**Don Kennedy**  
First American Title Insurance  
Company  
Santa Ana, Calif.

CHAIR, FINANCE COMMITTEE  
**Jack Rattikin III**  
Rattikin Title Company  
Fort Worth, Texas

CHAIR, TITLE INSURANCE UNDERWRITERS  
SECTION  
**Daniel M. Wold**  
Old Republic National Title Insurance  
Company  
Minneapolis, Minn.

BOARD REPRESENTATIVES,  
TITLE INSURANCE UNDERWRITERS  
SECTION

**David Townsend MTP, NTP**  
Agents National Title Insurance Co.  
Columbia, Mo.

CHAIR, ABSTRACTERS AND TITLE  
INSURANCE AGENTS SECTION  
**William Burding Jr. NTP**  
Orange Coast Title Family of  
Companies  
Santa Ana, Calif.

BOARD REPRESENTATIVES, ABSTRACTERS  
AND TITLE AGENTS SECTION  
**Richard H. Welshons**  
DCA Title  
Hastings, Minn.

**Maureen Pfaff WTP, NTP**  
Olympic Peninsula Title Company  
Port Angeles, Wash.

IMMEDIATE PAST PRESIDENT  
**Steven G. Day NTP**  
Fidelity National Title Group  
Jacksonville, Fla.

## ASSOCIATION EXECUTIVE STAFF

CHIEF EXECUTIVE OFFICER  
**Diane Tomb**

CHIEF OPERATING OFFICER  
**Cornelia Horner CMP**

SENIOR VICE PRESIDENT  
OF POLICY  
**Justin Ailes**

VICE PRESIDENT  
**Kelly Romeo CAE**

VICE PRESIDENT OF COMMUNICATIONS  
**Jeremy Yohe**



# Have You Been Pwned?

## CONCERNED IF YOU'VE BEEN COMPROMISED IN A DATA BREACH?



**JEREMY YOHE**

ALTA vice president of communications

There's an interesting website ([haveibeenpwned.com](http://haveibeenpwned.com)) that allows you to quickly assess whether you've been put at risk due to an online account having been compromised or "pwned" in a data breach. The free site was launched after the data breach of Adobe—which at the time was the largest ever single breach of customer accounts. The data on this site comes from breaches where customer information was exposed to those who should not have been able to view it.

So, what should you do if you learn your account has been pwned? First, take a breath and don't freak out. At last count, more than eight billion compromised accounts are listed on Have I Been Pwned. The Equifax, Yahoo and Marriott breaches account for nearly two billion of the username and password combinations. With every large data breach—especially if it's a service you use—you may feel a heightened sense of anxiety that your account was involved. Should you panic? Should you change your password?

In reality, it's likely you've been pwned for some time, multiple times. You just didn't know it. I read an article that said data breaches aren't like a bank robbery in broad daylight. They're like heists. No one knows until it's too late. (Think Mission Impossible, not Point Break.)

Often, companies won't know about a breach until their data shows up online in database dumps or paste bins for usernames, emails and passwords. Sometimes these are reported by good Samaritans—or as we call "white hat" hackers in our story on page 15—who stumble upon them on the Dark Web.

In our cover article, we provide some concrete ways you can help avoid getting phished. Scammers will use familiar company names or pretend to be someone you know. They may ask you to click on a link or give passwords or bank account numbers. If you click one of these links, programs can be installed that lock you out of your computer and steal your personal information. Often, the emails pressure you to act now or something bad will happen.

To avoid getting hacked, double-check the website for the person or company contacting you and make sure the domain matches the incoming email address. Call that person directly, using a known number. Do not reply using the address or phone number in the suspicious email or text. If you suspect or verify that an email or text you got was phony, notify the legit company about the message you received.

There are some quick tip-offs that might indicate an email is a scam. If you don't have an account with the company the email is from, that's a red flag. Others include messages that are missing your name, or have bad grammar and misspellings. A sure sign is a message that asks for personal information, including usernames and passwords. Just remember that some phishing schemes are sophisticated and look very real.

It's likely you've been pwned, given the volume of breached data. Sure, you will be concerned but don't panic. ALTA is here to help you stay ahead of your security needs.

## Former NSA Exec to Address Cybersecurity at ALTA ONE



honestly, most of us are a mixture of being a little afraid and yet a little naive about how much of our money and data—as well as our customers’—is at risk.

The director of cybersecurity for Morgan Stanley Wealth Management and Investment Technology, Rachel Wilson, knows exactly the dangers you face. Considering increasingly sophisticated cyber threats, Wilson will share her insight at ALTA ONE on how best to protect your business and avoid falling prey to scams and attacks.

Wilson spent the first 15 years of her career running counterterrorism operations at the National Security Agency (NSA). She focused on detecting and disrupting terrorist plots against the United States. She also led the planning and execution of thousands of cyber exploitation operations.

At Morgan Stanley, Wilson is responsible for protecting the



confidentiality of firm and client data. She advises on a host of cybersecurity issues ranging from secure code development standards, secure network architecture, vendor relationships, advanced persistent threat (APT) detection and mobile security.

For more information about ALTA ONE or to register, go to [meetings.alta.org/one](https://meetings.alta.org/one).

Cybersecurity is top of mind for all of us, whether we're thinking about our professional or personal lives. Quite

## 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 numbers from the past month.

- New Members: 31
- New Associate Members: 3
- New Attorney Members: 14
- Total Members: 6,283
- State With Most New Members: Florida

For a list of the latest new and associate members, as well as real estate attorneys who recently joined, go to [alta.org/new-members](https://alta.org/new-members).



### NEWS TO SHARE?

If you have information you'd like

us to consider for TITLE News, send company announcements to [communications@alta.org](mailto:communications@alta.org).



**OLD REPUBLIC TITLE**

**FINDING APPEALING  
TITLE AND REAL ESTATE  
INDUSTRY INFORMATION IS** **HARD  
WORK**



***We got you covered***

**[oldrepublictitle.com/blog](http://oldrepublictitle.com/blog)**

06/2019 | © Old Republic Title's underwriters are  
Old Republic National Title Insurance Company  
and American Guaranty Title Insurance Company.



**OLD REPUBLIC INSURANCE GROUP**

## ALTA Announces RynohLive as an Elite Provider

ALTA announced that RynohLive has been named an ALTA Elite Provider. ALTA's Elite Provider Program features distinguished vendors committed to furnishing extensive benefits to the title insurance and settlement services industry. Elite Providers promote the highest industry standards and provide effective solutions for ALTA members' critical needs.

RynohLive is a patented automated escrow management system that provides settlement agents the tools necessary to track and manage their escrow accounts. These tools include daily three-way reconciliation; daily and monthly reporting, including tracking and alerting of critical disbursements; end-to-end account auditing; and integration with bank Positive Pay systems. Using a cybersecure cloud application with proprietary anti-fraud algorithms, RynohLive helps clients stay steps ahead of would-be fraudsters and thieves with near real-time escrow account monitoring.

"ALTA's Elite Provider list is highly selective, and RynohLive is honored to be part of the program," said Dick Reass,



founder and CEO of RynohLive. "We are the industry standard for escrow and financial management software for the settlement industry, and it is great to have ALTA recognize the work that we do on a daily basis to keep escrow accounts secure."

As a special benefit for ALTA members, RynohLive waives its \$250 onboarding fee.

For more information about the Elite Provider program or to apply, please visit [alta.org/elite](http://alta.org/elite).

## Help Us Save a Tree, or Two

As the cost to print and mail *TitleNews* continues to increase and becomes a larger percentage of ALTA's budget, we'd like you to consider opting out of the print copy. If you no longer wish to receive a hard copy of *TitleNews*, simply select opt out. You will continue to receive the digital edition every month. You can also review and manage the information you receive from ALTA at [alta.org/membership/manage-subscriptions.cfm](http://alta.org/membership/manage-subscriptions.cfm).

# CALENDAR

## 2019 ALTA CONFERENCES

### ALTA ONE

Oct. 21-25  
Austin, Texas

### DIGITAL CLOSING & MORTGAGE BOOT CAMP

Dec. 11-12  
Scottsdale, Ariz.

## 2019 STATE CONFERENCES

### MISSOURI AND KANSAS

Sept. 4-7  
Kansas City, Mo.

### OHIO

Sept. 8-10  
Columbus, Ohio

### COLORADO

Sept. 11-13  
Vail, Colo.

### ARIZONA

Sept. 11-13  
Prescott, Ariz.

## ALTA 2019 TIPAC Donors

The Title Industry Political Action Committee (TIPAC) is ALTA's voluntary, non-partisan 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. TIPAC has received \$477,228 from 713 donors so far in 2019. Check out who has supported the industry at [alta.org/tipac](http://alta.org/tipac).



# A SPOT-ON STRATEGY THAT HELPS YOU STAND OUT

In a competitive market, you can't afford to blend in. You need every advantage and a competitive edge. That's what Stewart Trusted Providers™ enjoy every day. When you partner with Stewart, you get renowned underwriting expertise, marketing resources, training and education, and eClosing guidance – tools that help you strategically move business ahead.

**Want a stand-out strategy for being an eClosing leader?  
Download our eClosing guide: [stewart.com/ALTA192](https://stewart.com/ALTA192).**

The Stewart logo consists of the word "stewart" in a white, lowercase, sans-serif font, positioned on a solid red square background.





# Here Phishy, Phishy

Title Pros Must Be Vigilant  
Against Email Phishing Attacks

By Jeremy Yohe

**ONE IN EVERY 99 EMAILS** is a phishing attack, according to Avanan's phishing statistics. This amounts to 4.8 emails per employee in a five-day work week. Considering close to a third or 30 percent of phishing emails make it past default security, the threat is very much present.

The success rate of these attacks has emboldened scammers to launch more of them. Avanan reports an increase of 65 percent in phishing attacks from 2016 to 2017. And this is a global phenomenon affecting every region and economy.

In 2018, 83 percent of people received phishing attacks worldwide resulting in a range of disruptions and damages. This includes decreased productivity (67 percent), loss of propriety data (54 percent) and damage to reputation (50 percent). When it comes to the attacks, two in three phishing attempts use a malicious link and over half contain malware.

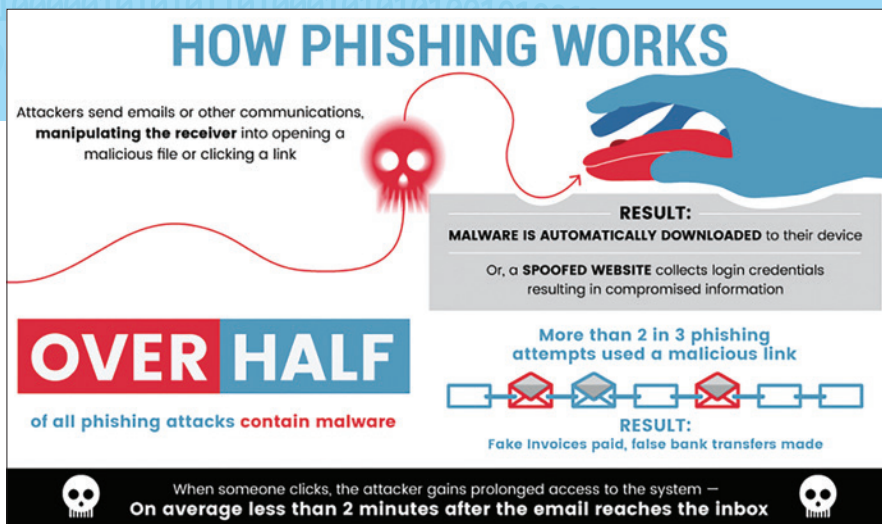
Malware—or malicious software—describes any program or code that is harmful to systems. Malware seeks to invade, damage, or disable computers, computer systems, networks, tablets, and mobile devices, often by taking partial control over a device's operations. Once infected with malware, scammers gain access to a wide variety of functions, including

taking computer screenshots, sending, downloading and deleting files, and stealing passwords.

Alarmingly, more than 75 percent of title professionals don't conduct simulated phishing tests, according to a survey conducted by ALTA's Data & Analytics Work Group. Additionally, only 11 percent of respondents conducted monthly testing and only 6 percent performed annual tests. Nearly 700 agents nationwide participated in the survey.

Phishing occurs when a scammer uses fraudulent emails, texts or copycat websites to get someone to share valuable personal information such as account numbers, Social Security numbers, login IDs or passwords. Scammers use this information to steal

## Digital Titlenews Extra: The Changing Face of Fraud



someone's money or identity, or both. In real estate transactions, this is a precursor to what the FBI refers to as business email compromise (BEC) often resulting in wire transfer fraud. The FBI reported 11,300 people suffered losses of nearly \$150 million due to wire fraud in 2018.

Simulated phishing tests are orchestrated fake phishing emails sent by companies to their employees to heighten employee awareness reduce the

likelihood of an employee falling victim to an actual malicious attack. According to ALTA's Data & Analytics Work Group, these tests measure a company's vulnerability, and can present trends and offer some measure of improvement.

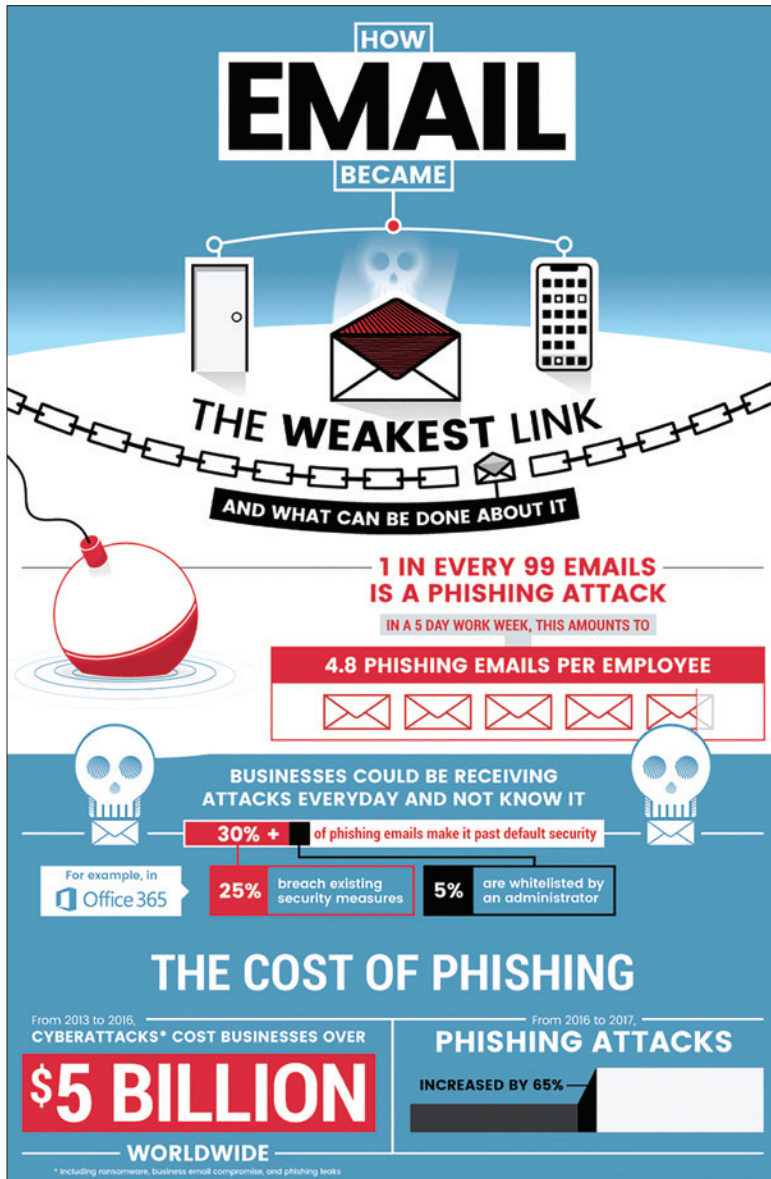
Phishing tests also can present a training opportunity for those employees that did not catch the phishing attempt and increases awareness regarding phishing. It should be noted that simulated phishing

tests should complement any training strategy and not be used as a replacement for employee training. These tests can be adapted for the latest schemes.

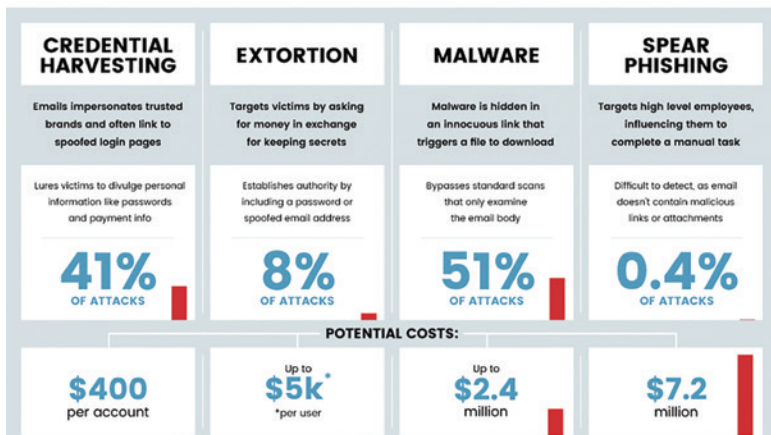
Ken Kirkner, director of global operations and senior vice president for Trident Land Transfer Co., says his company's information security department sends out tests on a weekly basis.

"We get a report back on how each division and department fared," he said.

Many vendors provide tools that integrate with email systems. These systems support linking an employee to rewards for finding the email, a training web page for those that missed it, and provide measurement and tracking. Several technology providers make free phishing testing available and links are provided on ALTA's website ([alta.org/business-tools/information-security.cfm](http://alta.org/business-tools/information-security.cfm)). Many companies in ALTA's Marketplace ([alta.org/marketplace](http://alta.org/marketplace)) also



## CATEGORIZING PHISHING ATTACKS



provide information security services, including phishing testing.

### Ditch the Complex Password?

If a company fails to properly educate and make employees aware of the dangers of phishing, the most complex password requirements won't matter. Studies show that poor password security instead of password complexity is often a major cybersecurity weakness for most organizations and employees that leads to criminals accessing non-public personal information. The latest password guidelines issued by National Institute of Standards and Technology (NIST) recommend significant changes to the way companies and people approach the complexity and usage of passwords.

Among the changes, NIST recommends the removal of periodic password change requirements, dropping the algorithmic complexity that often resulted in passwords that are easily cracked with password cracking tools, and the use of long passphrases instead of developing complex passwords.

### Make Passwords Easy to Remember, Hard to Guess

In what may seem like a 180-degree turn, NIST moved away from what's been promoted for more than decade, recommending long passphrases in lieu of complex passwords. These new security guidelines are more focused on creating unique passphrases that users will remember easily, using whatever characters they want, instead of using convoluted and complex passwords that make no sense to the user.

### Special Characters Not So Special

NIST still recommends using special characters, but the organization no longer requires their use when it comes to memorized secrets. Although the use of any special characters is recommended, the NIST password guidelines no longer require their use when it comes to memorized secrets. Concerning the use of characters in general, the password guidelines in SP 800-63B 5.1.1.2 stipulate:

*"All printing ASCII [RFC 20] characters as well as the space character SHOULD be acceptable in memorized secrets. Unicode [ISO/ISC 10646] characters SHOULD be accepted as well. To make allowances for likely mistyping, verifiers MAY replace multiple consecutive space characters with a single space character prior to verification, provided that the result is at least 8 characters in length. Truncation of the secret SHALL NOT be performed. For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character."*



## More Is More

The NIST password guidelines update requires users to create passwords that consist of a minimum of eight characters. However, it also allows the password form fields to include the use of up to 64 characters.

This change was made to help support the use of passphrases. According to the Verizon 2018 Data Breach Investigations Report, length and complexity of passwords are not enough on their own. “No matter who administers your technology environment (whether in-house or outsourced) they should be required to use two-factor authentication,” the report advises. In an upcoming article, we’ll provide tips to easily implement two-factor authentication.

“Users should use long password phrases consisting of three or more words that normally don’t go together but are easily remembered and be at least 15 characters long,” suggested Paul Noga, director of information technology and cybersecurity for Southern Title. “Passwords should be screened against lists of commonly used or compromised passwords. Users should only change their passwords when they suspect there could be a potential compromise.”

## Requiring Password Time Periods Has Expired

The new password guidelines no longer require users to create new passwords after a certain period. Studies have shown the requirement of frequent changes to be counterproductive to good password security. Instead, it specifies that new passwords are mandated only in the event of a password breach. According to NIST, “Verifiers SHOULD NOT require memorized secrets to be changed arbitrarily (e.g., periodically). However, verifiers SHALL force a change if there is evidence of compromise of the authenticator.”

## Copy and Paste Functionality

Another change in the NIST password guidelines is the enablement of being able to use a “paste” feature in the password field. NIST says this facilitates the use of password managers, which increase the likelihood that users will choose stronger memorized secrets.

## What Title Agents Are Doing

Noga said his company’s minimum password length is set to 15 characters and it still requires character complexity (special characters, upper and lowercase). He added that Southern Title will soon revisit its policies and likely switch to passphrases with a minimum of 15 characters and maximum of 64.

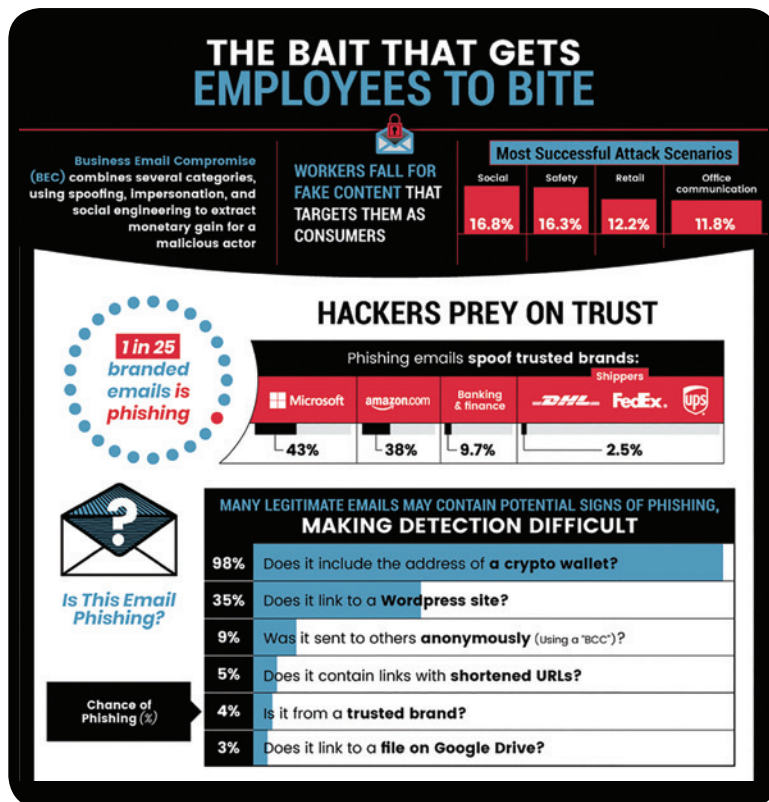
“A passphrase of five words would take a hacker eight years to crack,” Noga said. “We are going to set the password expiration to one year and only have



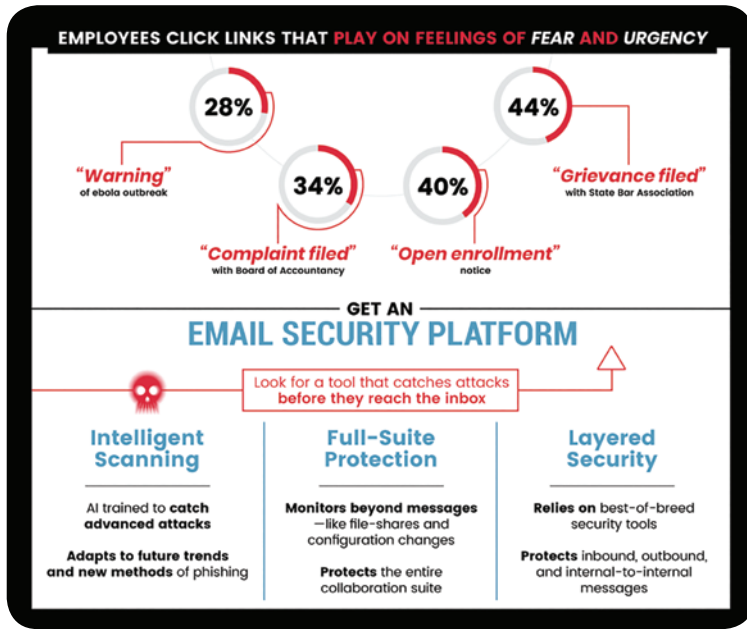
user’s change their password if we suspect suspicious activity or compromise. Passphrases are easier for users to remember and allowing them to make a long enough passphrase that will be hard to crack with in the password age we set.”

Remembering complex passwords or long passphrases can be difficult, so many use password managers. Southern Title is looking to purchase the business plan for the password manager Keeper. This will give staff the ability to access the program from multiple devices so the company can centrally manage accounts and allow for recovery.

“Password manager’s allow users to use a different password for every application and website they access,” Noga said. “All they need to remember is their password



HERE PHISHY, PHISHY



to their vault and they can have the manager randomly generate long complex passwords for everything else. The manager allows them to log on from the vault and it automatically fills in the credentials. This makes their lives much easier and more secure.”

Ken Kirkner, director of global operations and senior vice president for Trident Land Transfer Co., agrees that password managers simplify the process. His company uses Lastpass, which provides an extension for Chrome, Safari, Firefox and other browsers.

“It is easy to use and a good route to go,” he added.

**Core Principles**

While the types of attacks cyber criminals deploy may evolve over time, the principles companies can implement generally stays the same. The overriding point to understand is that incidents will occur at some time and the responsibility of security is everyone on staff—not just the IT department. According to Online Trust Alliance, here are some core principles to help organizations remain vigilant against attacks:

- 1. Responsibility for incident protection and readiness is organization wide.** Data stewardship, security and associated privacy practices are the responsibility of the board, executives, all employees and all departments (not just IT).
- 2. Data is an organization’s most valuable asset.** Identify what you have, where it is, why and how you use it and the potential risks to your organization and

**With SoftPro LIVE, a customizable communication portal, you can provide all authorized parties with secure access to track the status of your closings anytime, anywhere. Elevate your closing experience and save time for everyone with automatic emails, messages and the ability to share documents with your customers – 24 hours a day, seven days a week!**



**KEY STANDARD FEATURES**

- Post documents electronically to a secure website where your customers can view them.
- Provide your customers with appropriate access for the orders with which they are associated.
- Automate tasks and track the status of your closing with real-time updates.
- Send automated, customized email notifications regarding order status and tasks.
- Send two-way messages with your customers that flow directly into SoftPro.
- As an option, create your own custom SoftPro LIVE website and domain, branded specifically for your company.



**CUSTOMIZABLE WEB ORDER ENTRY**

As an optional add-on, you can receive and accept new orders securely and directly from your SoftPro LIVE website – anytime, day or night. There’s no need to re-key any information, so you’ll minimize errors and maximize efficiency.



**GO MOBILE**

SoftPro LIVE is also available for Android and iOS smartphone and tablet devices. Download the appropriate SoftPro LIVE app to access contact information, documents and orders when you’re on the go. Includes satellite or street views of properties, powered by Google Maps.

For more information and pricing, visit [softprocorp.com/live](http://softprocorp.com/live) or contact SoftPro Sales at **800-848-0143** or [sales@softprocorp.com](mailto:sales@softprocorp.com)

800-848-0143

[www.softprocorp.com](http://www.softprocorp.com)

©SoftPro. All Rights Reserved. SoftPro is a trademark and the property of SoftPro, its subsidiaries, and affiliated companies. All other trademarks are the property of their respective owners.





individuals should it be inappropriately accessed, held hostage, released or erased.

**3. Only collect and retain data that has a business purpose for as long as it is needed.** Secure it while it's held; delete it when it's no longer needed. Criminals cannot steal or hold hostage data you don't have, and such minimization may be a regulatory requirement for your organization.

**4. The level of data security you apply must be commensurate with the data held.** The security in place should reflect the risk of damage to consumers and the organization should that information be inappropriately accessed. Organizations should develop a data minimization strategy including a classification matrix that guides how various types of data should be protected, stored and discarded across an organization.

**5. Protection involves not only the specific incident (data loss, ransom paid), but also the costs of business interruption.** This includes locked data, network and system interruption and connected device takeover

Genady Vishnevetsky, Stewart's chief information security officer, says an additional security measure a title professional should employ is multifactor authentication for everything that supports it.

In June, ALTA's Board of Governors in June approved recommendations to update and modify various portions of ALTA's Title Insurance and Settlement Company Best Practices. One of the approved changes is the recommendation that companies use multifactor authentication for all remotely hosted accessible systems storing, transmitting or transferring non-public personal information. The proposed change is under a 60-day comment period that closes Sept. 15. Once finalized, changes will go into effect Jan. 2, 2020. Email comments to [bestpractices@alta.org](mailto:bestpractices@alta.org).

Vishnevetsky added that user email protection services can help title agents protect against phishing attacks.

"Microsoft and Google both offer a solution as additional service," he said. "There are standalone services such as Mimecast or Proofpoint that provide the same capabilities."

As a security practitioner, Noga believes layered security is the best advice for businesses. Complete protection against attacks isn't a reality. Noga said the best that can be achieved is to reduce the risk by putting in controls that will protect, detect and respond to incidents.

"The goal is to protect but be able to detect and respond when a protection fails," he said. "The faster you can detect and respond the faster you can reduce the impact."

In addition to multifactor, examples of layers include firewall, intrusion detection and prevention system (IDS/IPS), data loss prevention, encryption (at rest and in transit), VPN access for remote users, next-gen endpoint protection (which replaces most antivirus programs that use only signature-based detection), security information and event management (to get visibility into your network and systems through log and event aggregation and correlation), patch management (updating firmware, operating systems, software, etc.) and security awareness training.

"These are just a few of the controls that work together in a layered defense, but security awareness training is really the best bet to combat this," Noga said. "Spam and malware filters only catch about 10 to 15 percent of phishing emails. Educating users on spotting the red flags is truly the best route for combatting social engineering attacks and scams." ■



**JEREMY YOHE** is ALTA's vice president of communications. He can be reached at [jyohe@alta.org](mailto:jyohe@alta.org).

## Title Company Data Allegedly Exposed in Phishing Attack

**ON JULY 3, ALTA LEARNED** that roughly 600 title and settlement company usernames and passwords were allegedly acquired using a phishing campaign.

This was not a breach of ALTA's system. The data was sent to ALTA by an outside source and the association felt it had a duty to inform and protect industry professionals as much as possible.

The information sent to ALTA offered no indication of:

- how the credentials were obtained
- whether the credentials are current or active
- if the credentials provide access to any individual company networks, software applications, online email systems, or other credential-based products or services

Analysis by ALTA's Information Technology Department found:

- 182 unique email addresses (some email addresses are listed more than once with different associated passwords).
- 154 unique domains (some domains were listed more than once with different associated email addresses).

ALTA contacted the companies if their domain was found in the data.

In the meantime, it's important to watch for unauthorized access to your system. If you suspect that any contact information was obtained or your system was accessed, alert your IT department or engage an IT specialist to implement your information security program and response plan. Some steps you can take to protect your system include:

- scanning your systems and devices to make sure that you are free from malware
- update or patch your software and operating systems
- require your staff to update and change system passwords, especially those containing customer information and banking services

ALTA also suggests reporting any suspicious emails to the Federal Bureau of Investigation Internet Crime Complaint Center at [ic3.gov](http://ic3.gov). If you have additional information about this incident or similar attacks, please contact ALTA's IT staff at [vulnerabilities@americanlandtitleassociation.org](mailto:vulnerabilities@americanlandtitleassociation.org).

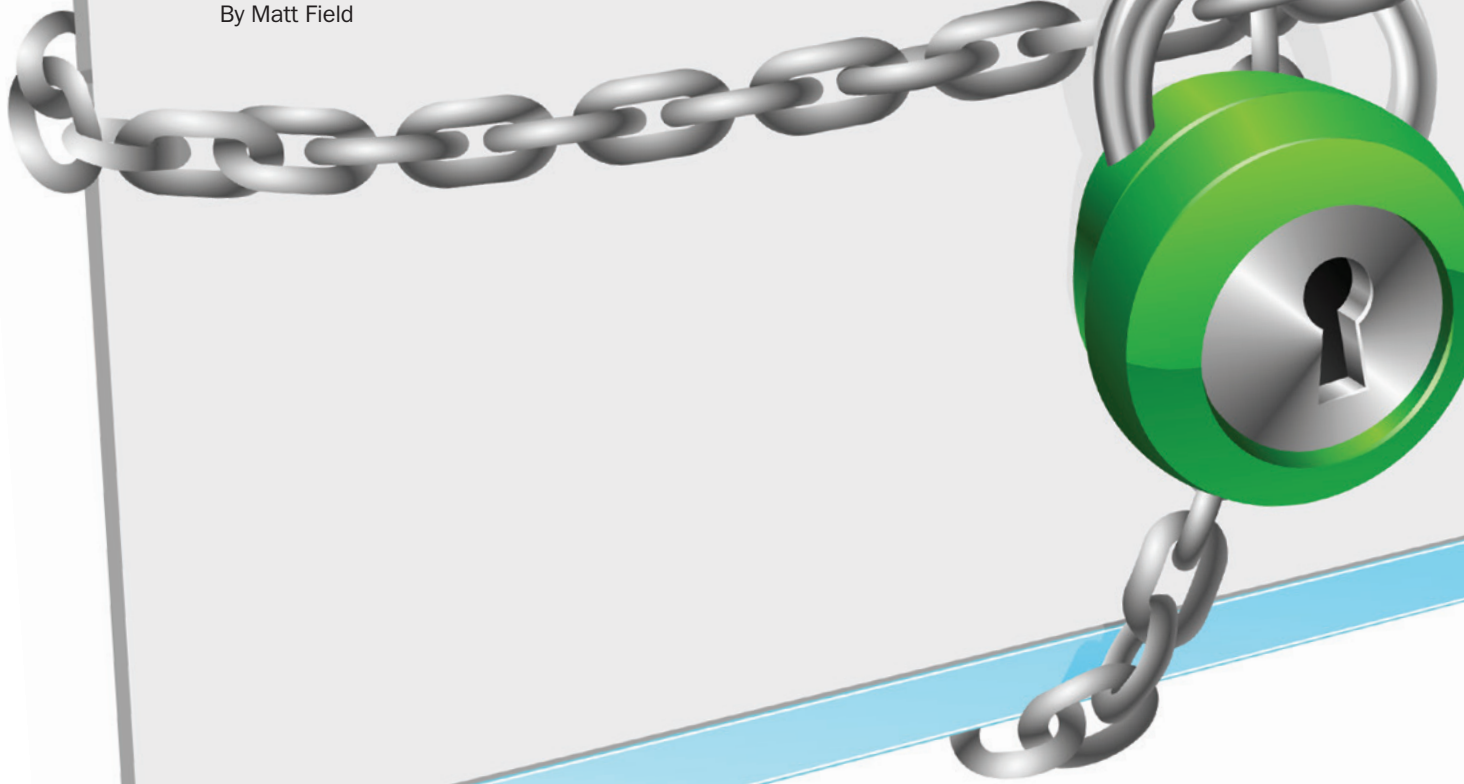


http://www.iteonthe.interne

# Is Your Browser Secure?

## Key Things to Consider When Selecting a Web Browser

By Matt Field





From work-related documents to banking and financial information, many of us regularly use our web browser to transmit confidential and personally identifiable information. Having a secure browser is critical: A browser that is not well-secured could expose you to some significant risk. But with web browsers being a commonplace (and sometimes virtually invisible) application, how can you make sure that your browser has the security features needed to protect you?

Let's discuss some of the most important things to consider when selecting a web browser, in addition to some of the most popular web browsers available—starting with Microsoft's own Internet Explorer.

### Microsoft Internet Explorer Isn't Your Best Bet

IE has the advantage of coming pre-installed on many computers, but while it is convenient, it isn't always the most secure option. Internet Explorer runs on a tremendous amount of technical debt—and it's become an outdated, unsupported technology. That doesn't mean you should immediately switch to Microsoft Edge, but it does mean that you should look closely at any applications using IE.

In order to maintain its compatibility with older websites, Internet Explorer has become progressively larger and more cumbersome. Support for older websites introduces a greater potential for exploits, and many new web standards are specifically designed to avoid security flaws and privacy breaches. The larger a system is, the more likely it is to have introduced faults.

Additionally, since Internet Explorer is often implemented as an easy, fast solution, it isn't locked down as much as it should be. By default, Internet Explorer's security settings are broad, allowing websites ease of control over the user's system in favor of an easier user experience. While this does facilitate a smoother user experience, it also opens users to potential danger.

And, of course, there's Microsoft, which has been attempting to push people off Internet Explorer in favor of Edge for some time. Because of this, the company has not been investing a lot in making sure that Internet Explorer is secure. Microsoft Edge is the spiritual successor to Internet Explorer, and Microsoft has put quite a lot of effort into its development and its adoption.

Ultimately, IE is an outdated platform that's been all but abandoned: Its chief advantage is that it's intuitive and ubiquitous. It's an inherently insecure solution both because it encourages bad security practices and because it prioritizes usability over security to begin with.

So, if IE is a bad browser, what is a good browser?

## What Makes Browser Applications More or Less Secure?

If not Internet Explorer, then which browser should you use? In fact, what makes a browser more secure at all? Secure browsers enforce web standards and make security settings transparent and accessible. A secure browser puts security before issues of appearance and compatibility, though user experience still does matter.

Features of a secure web browser include:

- **Frequent updates:** New exploits are discovered all the time; if a browser's development team isn't regularly patching it against these security exploits, then it is not secure. In terms of Internet Explorer, the software itself is no longer supported and will be discontinued.
- **Malware detection:** Browsers can maintain blacklists of websites that are known to be malicious in nature. Chrome has this turned on by default. By warning you when a site is dangerous, it can help you avoid internet "bad neighborhoods": areas that are likely to involve malicious programs or scams.
- **Sandboxing:** Sandboxing ensures that the browser itself operates in an isolated environment, without interacting with the rest of your computer environment: Even if something malicious runs in the browser, it won't be able to escape the sandbox.
- **Transparent security features:** Easily visible, transparent and modifiable security features, such as the ability to easily deploy a VPN to your browser, make it simpler for you to protect yourself.

Many people choose a browser based on ease of use rather than security. But as security is becoming an even larger concern, both in business and for individuals, it's become important to prioritize. The above features are the hallmarks of a browser that is putting security first.

## Choosing the Right Browser for You

Besides security and ease of use, some other considerations for choosing a browser include reliability and cross-platform support. Many people may use different browsers for their tablet than their PC, or may find that a browser isn't natively supported on their smartphone.

Considering all of this, Chrome is likely to be the most secure and most functional browser. While there are other browsers such as Brave and Tor that could be considered more secure because of their focus on privacy, they are less user-friendly and less popular overall.

## Rundown of the Most Popular Browsers

### Chrome

Chrome has an extremely rapid update frequency, but it also experiences more attacks and exploits than other browsers because it is so popular. Nevertheless, as the major web browser for both mobile devices and personal computers, Chrome has a lot of advantages: It's well-supported, simple, and free. Chrome has a number of add-ons that can be used to enhance security and its security interface is accessible and simple. It also features advanced security options such as blacklisting and sandboxing.

### Firefox

Firefox is very similar to Chrome in terms of raw security, though it has lagged somewhat in updates. Firefox is an open-source browser solution, which is backed by a large community. A major advantage to Firefox is that it claims to be much faster than Chrome, as well as avoiding some of the memory leaks that often cause Chrome to run sluggishly. It's also available on a larger number of platforms. At the same time, Firefox isn't quite as popular as Chrome and doesn't have as smooth of a user experience.

### Safari

Safari will automatically protect against many malicious programs and phishing attempts. It has exposed security settings, so you can choose the level of security and privacy that you want, and it has a streamlined interface that's direct and easy to use. For those on iOS or Mac, Safari is likely to be the primary choice, and it works very well within that ecosystem. For the Mac, iOS, and iCloud ecosystem, Safari is thoroughly integrated—and historically this ecosystem has been less burdened by security issues altogether.

### Edge

Microsoft Edge is designed to be more secure than Internet Explorer, and as the successor for Internet Explorer, it naturally has frequent updates and modifications. At the same time, it's notable that developers at Google's Project Zero were successfully able to bypass Internet Explorer's security, which called into question its capability of detecting and defeating malicious code. Microsoft Edge is the new default browser for Windows and, consequently, is available virtually everywhere, but it's experienced some significant security issues even as its state-of-the-art new security technology has won awards. Many are waiting to see how this browser evolves as the new version of Edge will be built on Chromium, which has ties to Google.

Ultimately, your choice of browser is likely to come down to the browser that you feel most comfortable with. For most people, Chrome is going to be intuitive, easy-to-use, and safe. However, it's in your best interest to also know more about how to secure your web browsing and the things that could potentially occur if your computer or other device is compromised.

In the future, it's possible that Microsoft Edge will catch up to Chrome in terms of user experience and security—and Safari is already a reliable option for those who are already within the Apple ecosystem. For today, Chrome remains the most popular and secure choice.

Using a secure web browser is one of the first steps toward securing your data. There are many companies such that work tirelessly to explore the technology that will protect your business and help it grow.



**MATT FIELD** is director of security and product development for Rynoh. He can be reached at [matt.field@rynoh.com](mailto:matt.field@rynoh.com).





# Not Just A Bunch of Interfaces... True 2-way Integrations.

RamQuest is all about making connections and our digital marketplace is no exception. We've worked hard for years to develop countless 2-way integrations with your key business partners. That's right. Connect with your trusted service providers, underwriters and lenders. Right there, inside your RamQuest production solution...where you need them, when you need them. That's RamQuest.

**See how to save time and money throughout the closing process with our Integration Infographic: [RamQuest.com/Integrations](https://RamQuest.com/Integrations)**



**RQ**  
RamQuest



RamQuest.com | 800.542.5503





## White House Hopes to Eliminate Regulatory Barriers to Affordable Housing

**P**resident Donald Trump on June 25 signed an executive order establishing the White House Council on Eliminating Barriers to Affordable Housing. The council will engage with state, local and tribal leaders to identify and remove obstacles that impede the development of new affordable housing.

“We’re lifting up forgotten communities, creating exciting new opportunities, and helping every American find their path to the American Dream,” Trump said.

Research indicates that more than 25 percent of the cost of a new home is the direct result of federal, state and local regulations. For this reason, in recent years, the construction of new multi-family and single-family dwellings has not kept pace with the formation of new households. Census Bureau data indicates that from 2010 to 2016, only seven homes were built for every 10 households formed. As a result, Americans have fewer housing opportunities, including the opportunity to achieve sustainable homeownership, which is the number-one builder of wealth for most American families.

“To improve housing affordability in a truly sustainable manner, we need innovative solutions—not simply increases in spending and subsidies for federal housing,” the order said. “These solutions must address the regulatory barriers that are inhibiting the development of housing. If we fail to act, Federal subsidies will only continue to mask the true cost of these onerous regulatory barriers, and, as a result, many Americans will not be able to access the opportunities they deserve.”

To curtail burdensome regulations, the council will be tasked with accomplishing the following items by January 2021:

1. Work across agencies, states, local governments, tribal governments and private-sector stakeholders to identify policies that artificially increase the cost of developing affordable housing.
2. Report on the quantifiable effect that federal, state, local and tribal regulatory barriers have on affordable housing development, the economy and society.

3. Take action to reduce federal regulatory and administrative burdens that discourage private investment and housing development.
4. Take action within existing federal programs to align and support local, and tribal state efforts to reduce regulatory and administrative burdens that discourage housing development.
5. Recommend federal, state, local and tribal policies that would:
  - Reduce and streamline statutory, regulatory and administrative burdens that inhibit the development of affordable housing supply at all levels of government.
  - Incentivize state, local and tribal governments to reduce barriers to affordable housing development.

Ben Carson, secretary of U.S. Department of Housing and Urban Development (HUD), was named chair of the council. The council will consist of members across eight federal agencies and engage with state, local and tribal leaders across the country to identify and remove the obstacles that impede the production of affordable homes—namely, the enormous price tag that follows burdensome government regulations.

“With the signing of today’s executive order, President Trump is prescribing a powerful treatment that correctly diagnoses the source of America’s affordable housing condition: this is a matter of supply and demand, and we have to increase the supply of affordable homes by changing the cost side of the equation,” said Secretary Carson. “Increasing the supply of housing by removing overly burdensome rules and regulations will reduce housing costs, boost economic growth, and provide more Americans with opportunities for economic mobility.”

# Comparative Family/Company Summary (Three Months 2019 vs. Three Months 2018)

Company Name	Three Months Total Premiums Written - 2019	Market Share	Three Months Total Premiums Written - 2018	Market Share	Increase/Decrease in Premiums Written	Market Share
<b>FIDELITY FAMILY</b>						
Chicago Title Ins. Co.	438,321,791	14.3%	458,877,785	14.2%	(20,555,994)	0.1%
Fidelity National Title Ins. Co.	402,336,147	13.1%	405,979,759	12.5%	(3,643,612)	0.6%
Commonwealth Land Title Ins. Co.	127,839,964	4.2%	142,808,117	4.4%	(14,968,153)	-0.2%
Alamo Title Ins. Co.	16,320,422	0.5%	17,001,552	0.5%	(681,130)	0.0%
National Title Ins. of NY	14,847,723	0.5%	16,311,649	0.5%	(1,463,926)	0.0%
<b>TOTAL - FIDELITY FAMILY</b>	<b>999,666,047</b>	<b>32.6%</b>	<b>1,040,978,862</b>	<b>32.1%</b>	<b>(41,312,815)</b>	<b>0.4%</b>
<b>FIRST AMERICAN FAMILY</b>						
First American Title Ins. Co.	717,791,857	23.4%	776,103,088	24.0%	(58,311,231)	-0.6%
First American Title Guaranty Co.	43,157,579	1.4%	29,415,960	0.9%	13,741,619	0.5%
First Canadian Title Ins. Co.	21,264,600	0.7%	24,876,063	0.8%	(3,611,463)	-0.1%
<b>TOTAL - FIRST AMERICAN FAMILY</b>	<b>799,926,298</b>	<b>26.0%</b>	<b>852,135,651</b>	<b>26.3%</b>	<b>(52,209,353)</b>	<b>-0.3%</b>
<b>OLD REPUBLIC FAMILY</b>						
Old Republic National Title Ins. Co.	484,495,325	15.8%	495,052,051	15.3%	(10,556,726)	0.5%
<b>TOTAL - OLD REPUBLIC FAMILY</b>	<b>489,362,750</b>	<b>15.9%</b>	<b>502,098,132</b>	<b>15.5%</b>	<b>(12,735,382)</b>	<b>0.4%</b>
<b>STEWART FAMILY</b>						
Stewart Title Guaranty Co.	263,593,164	8.6%	306,276,480	9.5%	(42,683,316)	-0.9%
Stewart Title Ins. Co. of NY	52,303,414	1.7%	51,934,966	1.6%	368,448	0.1%
<b>TOTAL - STEWART FAMILY</b>	<b>321,800,194</b>	<b>10.5%</b>	<b>363,758,930</b>	<b>11.2%</b>	<b>(41,958,736)</b>	<b>-0.7%</b>
<b>FAMILY TOTALS</b>	<b>2,610,755,289</b>	<b>85.0%</b>	<b>2,758,971,575</b>	<b>85.2%</b>	<b>(148,216,286)</b>	<b>-0.1%</b>
<b>TOP INDEPENDENT COMPANIES</b>						
Westcor Land Title Ins. Co.	103,452,099	3.4%	112,187,092	3.5%	(8,734,993)	-0.1%
Title Resources Guaranty Co.	72,627,317	2.4%	68,168,704	2.1%	4,458,613	0.3%
WFG National Title Ins. Co.	70,863,401	2.3%	81,967,052	2.5%	(11,103,651)	-0.2%
North American Title Ins. Co.	49,837,962	1.6%	53,979,514	1.7%	(4,141,552)	0.0%
Alliant National Title Ins. Co.	26,914,009	0.9%	28,942,863	0.9%	(2,028,854)	0.0%
First National Title Ins. Co.	26,281,695	0.9%	22,524,276	0.7%	3,757,419	0.2%
Connecticut Attorneys Title Ins. Co.	23,591,004	0.8%	24,498,161	0.8%	(907,157)	0.0%
Investors Title Ins. Co.	22,691,067	0.7%	24,095,966	0.7%	(1,404,899)	0.0%
Security Title Guarantee Corp. of Baltt.	11,143,271	0.4%	9,497,924	0.3%	1,645,347	0.1%
Attorneys' Title Guaranty Fund of IL	10,302,837	0.3%	11,162,509	0.3%	(859,672)	0.0%
<b>TOTAL - INDEPENDENT COMPANIES</b>	<b>459,988,404</b>	<b>15.0%</b>	<b>480,775,735</b>	<b>14.8%</b>	<b>(20,787,331)</b>	<b>0.1%</b>
<b>TOTAL - ALL COMPANIES</b>	<b>3,070,743,693</b>	<b>100.0%</b>	<b>3,239,747,310</b>	<b>100.0%</b>	<b>(169,003,617)</b>	<b>0.0%</b>

Note: Individual numbers do not equal totals as not all companies are listed.

Access complete market share data at [alta.org/industry-research](http://alta.org/industry-research)

## Q1 2019 Title Premium Volume Dips 5 Percent

The title insurance industry generated \$3.07 billion in title insurance premiums during the first quarter of 2019 compared to \$3.24 billion during the same period a year ago, according to ALTA's latest Market Share Analysis.

During the latest quarter, the industry paid \$128.3 million in claims. This is up from \$119.4 million in claims paid during the first quarter of 2018.

### Top States

- Texas, \$444,104,985 (-1.5%)

- Florida, \$319,356,959 (-1.6%)
- California, \$318,042,534 (-12.7%)
- New York, \$251,472,266 (0.6%)
- Pennsylvania, \$119,020,274 (-7.4%)

ALTA expects to release Q2 2019 market data around Sept. 1.

## FDIC Highlights RESPA Section 8 Violations in Compliance Report

The Federal Deposit Insurance Corp. (FDIC) on June 13 published its 2018 Consumer Compliance Supervisory Highlights, which provides a high-level overview of the consumer compliance issues identified through approximately 1,200 examinations conducted in 2018 for non-member state-chartered banks and thrifts.

This report provided anonymized 2018 exam findings showing violations of consumer protection laws. Issues related to compliance with the Real Estate Settlement Procedures Act (RESPA) Section 8 were included in the report.

Specifically, the FDIC noted issues with desk rental arrangements that were used to disguise illegal referral fees. According to the report, “One issue involved institutions that purportedly leased offices or desk space from Realtors and home builders, where the amounts paid to Realtors and homebuilders greatly exceeded the fair market value of the rentals. Another issue involved desk rentals that appeared to be sham or subterfuge arrangements to disguise the payment of impermissible mortgage referral fees.”

RESPA permits lenders to enter into bona fide marketing and advertising agreements with title and settlement providers, however, such arrangements must be based on fair market value of the advertising and marketing services received. They can’t be used to conceal the payment of illegal referral fees. The FDIC found that certain arrangements, structured as marketing agreements, were actually used to disguise illegal payments for referrals of mortgage business.

In the past, the FDIC found similar violations for marketing services and lead generation arrangements. These were the topic of a bulletin from the CFPB in 2015.

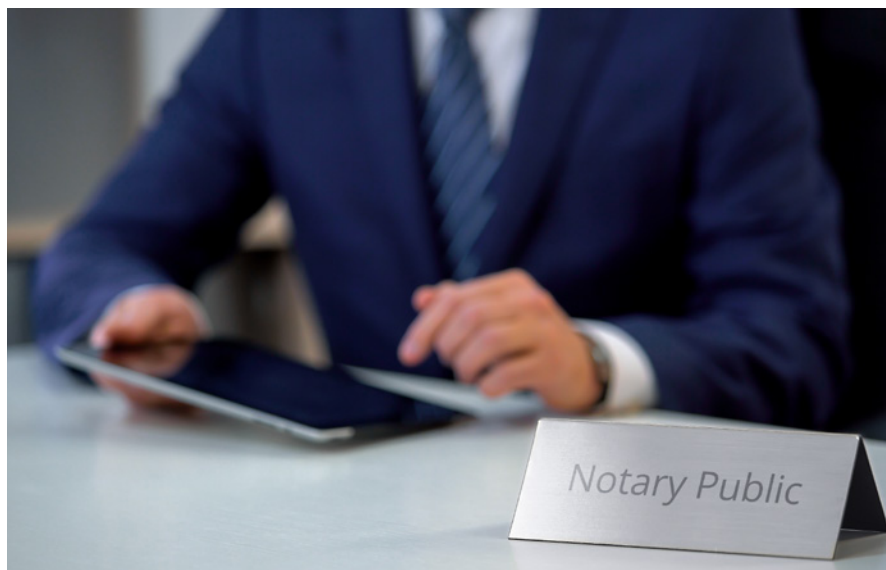
---

## TIAC Announces Coverage for Remote Online Notarization


The Title Industry Assurance Company (TIAC) announced expanded coverage for qualifying firms at no cost to all its new and renewal title agents E&O insurance policy holders effective immediately. The endorsement amends coverage under the TIAC policy providing coverage for remote online notarization (RON)/electronic notarization when in compliance with state requirements.

“As title and closing technology evolves, it’s important to ensure that your E&O policy does, too,” said Sean Hanifin, TIAC’s claims counsel. “Make sure that your policy’s notary services provisions do not eliminate coverage for RON services.”

For more information about TIAC or to receive a no obligation premium estimate, visit [tiacrrg.com](http://tiacrrg.com), email [info@tiacrrg.com](mailto:info@tiacrrg.com) or call 800-628-5136.







## Expert | Legal | Technology

Lean on FNTG, your agency expert. Let us guide you to leverage technology to improve your bottom line, stay on track with legal and regulatory issues, and innovate for the future marketplace. At FNTG, we combine unrivaled expertise in legal, technology, and underwriting to ensure the success of our agent partners.

**FNTG is for you.**



[NationalAgency.fnf.com](http://NationalAgency.fnf.com)



## Attorneys Title Guaranty Fund Issues Its First Policy in Arizona

Colorado-based Attorneys Title Guaranty Fund (ATGF) recently issued its first Arizona title policy through Sonoran Desert Title Agency in Phoenix.

Arizona was selected for expansion due to proximity and potential for overlap with ATGF's operations in Colorado and Utah. The underwriter also serves Minnesota and North Dakota.

"We are pleased to have an independent agency be the first to issue a title policy for us in Arizona," said Brian

Phillips, CEO of ATGF. "With consolidation and other changes at national underwriters, this opens significant opportunities for a stable, regional underwriter with a proven track record of supporting independent title agents. That's where ATGF fits into the Arizona marketplace. Independent agents need a strong partner that will work with them."

## States Title Awarded Machine Intelligence Patent

States Title Holding Inc. received a patent

for "Machine Learning Using Multiple Data Types" on April 9 from the U.S. Patent Office.

The patent for invention number 10,255,550 defines and protects the solution States Title has created to apply machine intelligence and predictive analytics to the most complex and frustrating steps in completing the title and escrow process. Through this solution, States Title says it can provide a closing process that is quicker and dramatically more efficient than title companies that solely offer digitization or automation.

Via proprietary data sources and data-cleaning methodologies, States Title

### *We can Protect you against Costly Allegations*

**E&O Coverage.** In today's litigious society, claims arising from your professional services can have a profound effect on the financial

security of your company. By insuring with TIAC, you're protected by the most reliable and effective coverage in the industry.

# You Never Saw it Coming.

Get a FREE no obligation quote today: **800.628.5136**  
Title Industry Assurance Company • [TIACrrg.com](http://TIACrrg.com)





claims its predictive analytics algorithms can instantly determine a property's ease of closing and identify and reject false positives—eliminating the need for curation in the title process altogether.

States Title, which acquired North American Title Insurance Co. in December 2018, says its machine intelligence technology will replace approximately 80 percent of the manual workflow-related time and activities. Over the past year, by using States Title's now patented method of machine intelligence, large national lenders have had 80 percent of loan files become clear-to-close within minutes, helping them increase their profit margins on loan originations by an average of 35 percent.

"Machine Intelligence transforms everyone's lives," said Max Simkoff, CEO of States Title Holding. "The title company of the future will be an amazing place to work. Even with all the transformative technology, we'll be building to change the nature of the work we do, our people will still be the most valuable asset. The title professional of the future will be able to focus intensely on building and maintaining great customer relationships because machine intelligence will eliminate nearly all the paperwork that plagues today's day-in-the-life."

---

## Fidelity Partners With Vendors to Provide Online Closing Options

Fidelity National Financial (FNF) has partnered with Notarize and NotaryCam to provide remote online notarizations and closings in states where permitted to its network of direct and independent title agents. "FNF and our title divisions are committed to bringing an end-to-end digital real estate experience to the industry, and the consumers we serve,"

said Jason Nadeau, Chief Digital Officer of FNF. "Remote notarization is another important component in our expanding suite of digital options."

---

## SLK Global Enhances Property Tax Solution

SLK Global Solutions announced the addition of two new offerings for its SmartTrak property tax solution, a technology platform used by more than 100 title and tax agents to enhance their tax reporting. The enhancements include a lower-priced rapid tax report and a standalone municipal lien search report (MLSR).

SLK Global Solutions America President Alok Datta noted that the enhancement expands flexibility for title agents in terms of a menu of choices at multiple price points depending upon their business needs.

According to SLK, the new enhancement also means SmartTrak can be used by mortgage servicers to order a quick tax report during a portfolio purchase or to track a loan's delinquency life cycle, including foreclosures and REO.

---

## EnTitle Rebrands as Radian Title

EnTitle Insurance Company has been renamed Radian Title Insurance Inc.

Radian acquired EnTitle in 2018. The name change is consistent with Radian's strategy of uniting all of its subsidiaries under the One Radian brand, Radian said in a release.

Radian Title is rated, "A Exceptional" by Demotech Inc. The underwriter has issued over 125,000 title insurance policies since operations began in 2009.

"As our industry celebrates National Homeownership Month this June, it

is timely that we mark the occasion by further reinforcing the One Radian brand with the name change of another valued subsidiary," said Rick Thornberry, Radian's CEO. "By adopting the Radian name, we are further strengthening industry recognition and appeal in our integrated solutions, whose reach across the residential mortgage and real estate spectrum empowers our customers to succeed throughout the multiple stages of the home buying process."

---

## Stewart Expands Digital Closing Capability in 20 States

Stewart recently expanded its coverage for remote online notarization (RON) to include 20 states, providing electronic closing capabilities to more than 250 of its direct operations offices across the United States.

Stewart partners with technology providers to leverage RON, a technology that allows consumers to opt into executing their documents electronically via a webcam with an online notary.

"Consumers deserve the opportunity to select the best closing option and location for a transaction and Stewart continues to drive solutions that optimize the customer experience," said John Magness, group president of direct operations. "RON will simplify the process for many of our customers with straightforward transactions, saving travel time and enabling greater convenience for certain customers and partners."

In partnership with several technology vendors like Notarize and NotaryCam, Stewart has conducted hundreds of RON closings since completing the first fully digital closing in July 2017 in Texas.

## Recent Integrations

- **Nexsys' Clear Sign** digital signing product will integrate with **Signature Closers' SYNC** platform to provide software solutions for all types of digital closings. In a digital closing—also known as an e-closing—some or all of the documents are signed and submitted digitally.
- The **Closing Exchange** formed a partnership with **DocuSign** to provide electronic signature capabilities and hybrid e-closings. Through the partnership, The Closing Exchange will offer DocuSign e-signature capabilities for CX Choice users, as well as future integrations with the DocuSign Rooms platform.
- **SoftPro** has released a new integration with **WFG National Title Insurance Company** providing enhanced capabilities for ordering title searches and retrieving title evidence. Users also can produce WFG closing protection letters and policy jackets, as they have been able to since SoftPro first integrated with WFG in 2013. The ability to order title work and retrieve services within SoftPro eliminates duplication of data entry as well as phone calls.
- **Rynoh** has expanded its financial protection product line by partnering with construction disbursement software provider **Silver Bay Systems**. The partnership between the two software companies provides Silver Bay Systems' clients utilizing CorrectDraw software to track construction disbursing projects the ability to access Rynoh's financial security solution under a single platform. This integration offers a user-friendly experience and a more efficient workflow while remaining compliant with financial transparency standards and ALTA's Best Practices.
- **LodeStar Software Solutions** announced that its Loan Estimate Calculator is now available through **Lending QB**, a provider of SaaS loan origination technology solutions. The integration allows lenders to access LodeStar's products through LendingQB.

## Housing Market Potential

Existing and Potential Home Sales\* (in Millions, Seasonally Adjusted Annualized Rate)

**5.21** SAAR

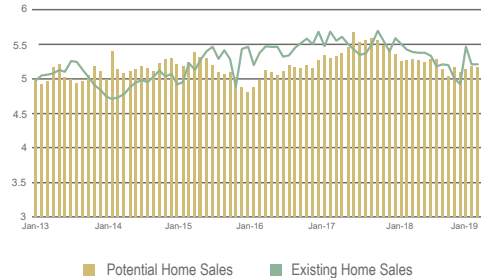
Existing Home Sales

**5.17** SAAR

Potential Home Sales

**+0.8%**

Market Performance Gap



\*Potential home sales measures what a healthy market level of home sales should be based on the economic, demographic and housing market environments.

## National Consumer House-Buying Power

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

April 2019

**\$391,000**

House-Buying Power

**+6.7%**

Year-Over-Year

## Where House-Buying Power is Strongest

Top States and Cities

### States

1. New Jersey: **\$521,960**
2. Maryland: **\$500,453**
3. Connecticut: **\$491,746**
4. Massachusetts: **\$487,008**
5. Hawaii: **\$483,895**

### Cities

1. San Jose, CA: **\$744,167**
2. San Francisco, CA: **\$665,111**
3. Washington, DC: **\$648,244**
4. Boston, MA: **\$555,361**
5. Seattle, WA: **\$544,608**

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



# Don't Be a Mess

Provide accurate information to lenders about your operation.

Get confirmed in the ALTA Registry.



ALTA  
REGISTRY

[ALTA.ORG/REGISTRY](https://ALTA.ORG/REGISTRY)



---

## Old Republic's Zucaro to Retire

Old Republic International announced that Aldo Zucaro will retire effective Oct. 1 after serving 25 years as the company's chief executive officer. Zucaro will continue to serve as chairman of the board and the executive committee. Craig Smiddy, Old Republic's president and chief operating officer, will assume the position of president and chief executive officer. He will concurrently join the Board of Directors and its Executive Committee. Smiddy will become the sixth CEO in Old Republic's 95-year history.



Feinen

---

## ATG Names City Mayor as Vice President of Downstate Operations

Attorneys' Title Guaranty Fund Inc. (ATG) announced it has hired Deborah Frank Feinen, an attorney and mayor of Champaign, Ill., as vice president of downstate operations. Feinen brings more than 25 years' experience in the profession to her new role as the top leader for ATG's downstate operations, including more than a decade as an active ATG member agent. Her law practice in Champaign-Urbana included real estate, estate planning and administration, guardianship, business law and school law. She follows in the footsteps of Jerry Gorman, former senior vice president of ATG's downstate operations, who retired in early 2019 after 37 years at ATG. In April 2019, Feinen was re-elected to a second term as Champaign mayor with a resounding 84.3 percent of the vote.

---

## Adeptive Names SVP of Strategy

Adeptive Software, developers of title and escrow production software ResWare, recently named Gorkem Kuterdem as senior vice president of strategy. In this role, Kuterdem will be responsible for the long-term direction of the ResWare platform. With deep experience in application development and automation in the title and escrow space, Gorkem embraces emerging technologies to help organizations advance and grow their businesses. Prior to Adeptive, Gorkem was the chief technology officer for WFG National Title Insurance Co.

---

## Patten Title Company Names New CFO

Patten Title Company has hired Allen Berryman as chief financial officer. He brings 40 years of financial and operational experience that will enhance the internal financial structure of Patten's top-rated full-service closing practice. Berryman most recently served as chief financial officer for Stewart Information Services Company. Prior to that, he served as head of finance for Cetero Research.

---

## Rynoh Bolsters Sales and Marketing Team

RynohLive recently added two members to its sales and marketing team. Ben Sommers will serve as vice president of sales and marketing for the company's central region, while Paul Smith will serve in the same capacity for the western area. Sommers and Smith will be responsible for establishing relationships and promoting Rynoh's software in order to grow the company's reach in their regions. Prior to joining Rynoh, Sommers spent his career working with various well-known industry organizations including First American Title, Stewart Title, and Title Resource Group. Most recently, he held a position as VP of regional sales for AmTrust Title. Smith brings with him over 20 years of experience in sales and marketing for a variety of industries and organizations including more than four years with Aprio, a CPA firm focused on providing ALTA Best Practices certifications for title agents.

---

## NATIC Names Maryland and D.C. State Agency Manager

North American Title Insurance Co. (NATIC) has added Pandora Nomikos-Hawkins as state agency manager for Maryland and the District of Columbia. She will oversee agency operations in the Mid-Atlantic area, while securing and servicing title agents to promote new and increased business activity. Nomikos-Hawkins joins NATIC with more than 34 years in the title insurance and banking industries. Prior to joining NATIC, she spent five years with a national underwriter.

**“We will begin by examining your bank reconciliation.”**



Being out of compliance can disrupt operations and end careers. Rely on experts to help you stay current on compliance requirements and prepare you for that moment when the auditors arrive.

We have the knowledge, experience and resources to prepare you. We've been doing this for 40 years and have serviced over \$32 trillion in transaction dollars.

We are the premier trust accounting service. You can relax. We'll get you ready.



**TrustLink™**  
You're ready.

TrustLink.Support@firstam.com  
800.767.7833  
www.trustlinkservices.com

## WTF Threat Continues to Spike

**IN A NEW MUST-READ REPORT,** the U.S. Treasury Department's Financial Crimes

Enforcement Network (FinCEN) details attempted theft amounts of more than \$300 million per month in 2018 due to wire transfer fraud (WTF) and business email compromise schemes.

According to FinCEN, real estate was the third highest targeted sector for BEC in 2018, accounting for 16 percent of all reported incidents. While real estate firms represented 9 percent of all targeted firms in 2017, they accounted for over 20 percent of fraudulent transaction amounts. Real estate firms have the highest average fraudulent transaction amount of \$179,000.

FinCEN says frequent high-dollar transactions in the real estate industry, along with the improving real estate market, most likely continued to make real estate an attractive target for perpetrators of BEC fraud in 2017 and 2018. This means we will be constant targets!

In recent years, we've seen the rise of this sophisticated type of fraud by cybercriminals who take advantage of these facts to prey on those involved in real estate transactions. This is why we must continue to raise awareness and educate consumers—especially first-time homebuyers—about how they can protect themselves and their money.

In case you've been too busy or haven't been reading *TitleNews*, BEC is a type of scam that targets businesses and their fund transfers. Scammers generally target organizations that conduct large wire transfers in the course of their usual business and rely on email for much of their communication regarding the wires. The perpetrators typically compromise a key email account by using computer intrusions or social engineering and send an email that fraudulently redirects funds to criminal-controlled accounts. Often, the victim is tricked into thinking a legitimate email from a trusted person or entity is directing them to make a payment for a normal business activity.

FinCEN reports that trends in scam typology indicate that BEC actors are likely changing methods as awareness of their schemes evolves. The most frequently used BEC method in FinCEN's 2017 sample involved fraudulent emails impersonating the CEO or president of a company (33 percent), but type of fraud declined to 12 percent in 2018, likely due to awareness of such schemes in the business community. Fraudulent vendor or client invoices were 30 percent of incidents in 2017, and grew to 39 percent in 2018, becoming the most common BEC method.

FinCEN started tracking impersonation of individuals outside the organization in 2018, to account for a shift in scam methods. In 2018, this type of activity accounted for 20 percent of BEC transactions. The vast majority of these suspicious activity reports showed that the scammer was impersonating a real estate agent on the sale side of a transaction, directing the buyer or buyer's representatives to wire money to a fraudulent account.

If you're interested in helping stop wire fraud, you can join the Coalition to Stop Real Estate Wire Fraud ([stopwirefraud.org](http://stopwirefraud.org)), register to attend the ALTA Innovation Boot Camp on wire fraud in Chicago, Aug. 11-12 ([meetings.alt.org/bootcamp](http://meetings.alt.org/bootcamp)) or check out all the resources ALTA provides its members ([alta.org/wirefraud](http://alta.org/wirefraud)).



**CYNTHIA DURHAM BLAIR NTP**  
ALTA president



# BOWEDIGITAL



## SOCIAL DOESN'T HAVE TO BE SCARY!

### Your social media marketing needs a pro. Put a Bowe on it!

Hootsuite reports that 5.11 billion people now have mobile phones and of those, 3 billion people use their mobile devices to access social media (and they spend nearly 3 hours on social media every day!). If you aren't thinking about your social strategy, you should be! Bowe Digital can help with your social media plan in the following ways:

- Create custom & engaging content
- Hyper-target your audience
- Determine where you should be most active
- Alert you when you should "boost"
- Create social media policies
- Help train your Realtors on social best practices

[bowedigital.com](http://bowedigital.com)

| [contact@bowedigital.com](mailto:contact@bowedigital.com)





ALTA  
**ONE**

**Unbound**

October 22-25, 2019 | Austin, Texas

[meetings.alta.org/one](https://meetings.alta.org/one)