Dear Readers,

Welcome to the 2013 Fraud Report, brought to you by The Legal Description and our sponsor, North American Title Insurance Co. (NATIC).

While the risk of mortgage fraud has decreased according to several studies, title agents have to remain vigilant. CoreLogic stated in a recent report that the propensity for mortgage fraud may be declining, but the overall amount of mortgage fraud is increasing as mortgage loan applications increase.

Fraud schemes are also evolving, always one step ahead of the authorities and their victims. Cyber thieves are targeting title and escrow companies due to their large cash reserves, small IT infrastructure and fewer controls. Trust and lack of controls also tempt employees who have access to company escrow accounts as well.

Despite these dangers to title agencies and the consumers they ultimately serve, there are ways for agency owners and employees to protect their consumers’ assets and themselves from becoming a victim. The National Association of Insurance Commissioners has drafted a white paper outlining ways regulators, title insurers and agents can protect these assets. Industry experts, including NATIC, have also outlined various steps to take to create a fortress around your escrow account.

These tips and tricks are all outlined in this report, as well as the latest mortgage fraud stats and descriptions of emerging fraud schemes. We hope these tools prove valuable to you.

Until next time, stay legal.

Andrew Golby

Table of Contents

- Beware the cyber fraud: Latest trends and tips to protect yourself 3
- Preparing for new schemes and the impact of escrow theft 5
- 2013 mortgage fraud report roundup 9
- Recommendations for fraud prevention (sidebar) 9
- Comptroller discusses cyber threats, solutions 11
- Common schemes and fraud red flags (sidebar) 12-14
- Title Insurance Task Force finalizes escrow theft white paper 13
Cyber theft is a constant threat to everyone, no matter who they are, as long as they have an Internet presence. The results of being phished or having your identity stolen can be devastating for an individual. It can be even more costly for a title company, which is responsible for protecting not only the business, but its employees and customers.

And cyber criminals are smart. As soon as companies and individuals find a way to protect against one malware software or one phishing scheme, the fraudsters come up with another. This is why it’s important to stay as up to date as possible about the latest schemes and how to protect yourself and your company against them. During a recent webinar from October Research LLC, two cyber security experts informed participants about the latest threats and the best ways to guard against them.

Coming after you

During the webinar, David Jevans, founder, chairman and chief technology officer of Marble Security, pointed out a recent news item in which an escrow firm shut down after being the victim of cyber theft. The perpetrators walked away with $1.5 million. He mentioned other recent cyber theft schemes where money was pilfered from the escrow accounts of unsuspecting title and escrow agents.

According to a report from the Financial Services Information Sharing and Analysis Center, criminals go after customers with lots of cash, a small IT infrastructure and few controls. At the top of the list of targets are title and escrow companies, followed by government contractors, municipalities, school districts and other small businesses.

The main way money is stolen, Jevans said, is through account takeover, where criminals take control of online financial services accounts and move large amounts of money off shore. Once out of the country, the money is not reimbursable.

“You and I as consumers, when we go to the store and use our credit cards, if the credit cards get stolen or hacked, or we get a phishing email when we type our credit card online and someone starts using it, we are generally not liable because we are protected by Regulation E and Regulation Z,” he said. “[These] are federal regulations that protect consumers so that if we experience fraud, generally banks are obligated by the federal government to reimburse us for those fraudulent transactions.

“However, for businesses like ours, we do not have any of those statutory protections,” Jevans continued. “If, as a business, our account gets taken over, if our computers inside of our companies get infected with malicious code that allows attackers to get in and start moving money out of our accounts, we are not protected. There is no federal protection law at all, which basically means that protecting ourselves is up to us. We need to have strong protections on our computers, on our networks and on our online banking sites to prevent the bad guys from taking over our accounts.”

How they do it

According to Jevans, there are nine key ways cyber attackers can hack into title company computer systems:

- Malware, Trojans, Zero-day Attacks — Malicious software designed specifically for financial crimes. Jevans said there are more than 100 million different pieces of malicious software out on the Internet right now.

“"The reason there are so many is because this is how the bad guys defeat anti-virus software," he said, emphasizing the need for all attendees to have good, paid antivirus software from a reputable company. But he warned that this still might not be enough.

“The fact remains that even with the latest updated antivirus, bad guys are still able to put malicious code on your computers because they are generating tens of millions of different ones a year, which means antivirus can’t keep up," Jevans said. “So while it’s important to have, recognize that antivirus can only protect you from between 80 and 90 percent of the malicious code, and between 10 and 20 percent of it can sneak past antivirus and get onto users’ computers without anyone being able to detect it.”

- Key loggers — These are invisible pieces of software that get installed on a computer. They track everything that you type, like usernames
and passwords to online banking, payment systems and other secure computer systems. The software sends the information to the thieves who use it to hack into the internal computer systems.

- Compromised Wi-Fi hotspots — Jevans said this has become increasingly prevalent as more and more people work remotely. There is no guaranty of security when you are using a Wi-Fi hotspot in a Starbucks or at an airport, he said.

- Poisoned DNS — These attack the core infrastructure of the Internet, turning the location name, such as mybank.com, into the numbers the Internet uses to route to it. The hackers change the numbers to re-direct the victim to the attacker’s website.

- Malicious and privacy leaking apps — “If you are allowing people to access your online banking or your internal systems from their own devices, know that there are apps out there that may be on the app store that are not necessarily malicious, but might do things that you don’t want, like uploading all of your address book information onto the Internet,” Jevans said. “Think about that information that makes you a prime target for spear phishing and other targeting because if that data is sitting on the Internet, I guarantee some hacker is going to get it at some point and now they know you are a title company, where you are and how to target individual users.”

- Jail broken and rooted devices — Many think that Androids and iPads are very secure, and in general they are, but if they get jail broken or rooted, which allows the installation of software from anywhere, you’ve lost all security controls and those devices are vulnerable.

- Un-patched OS Versions — Keep computers updated with the latest versions of the computer operating system. There are more security controls in the newer versions of the operating systems. Gregory McDonald, chief executive officer and founder of Cloudstar Consulting Corp., noted that Windows XP users will be particularly vulnerable as of April 9, 2014, because at that time, Microsoft will no longer provide security support for Windows XP.

- Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.

- Advanced Persistent Threats — Otherwise known as APTs, these threats happen when criminals target a company and its employees by investigating on LinkedIn, Facebook, etc.

- Advanced Persistent Threats — Otherwise known as APTs, these threats happen when criminals target a company and its employees by investigating on LinkedIn, Facebook, etc.

“Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.”

“Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.

- Advanced Persistent Threats — Otherwise known as APTs, these threats happen when criminals target a company and its employees by investigating on LinkedIn, Facebook, etc.

“Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.”

“Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.

- Advanced Persistent Threats — Otherwise known as APTs, these threats happen when criminals target a company and its employees by investigating on LinkedIn, Facebook, etc.

“Spear-phishing — The hacker sends targeted emails to employees pretending to be from the company’s IT security system or the bank to lure people into providing their usernames and passwords, which the criminal then uses to get into the company’s system.”

Jevans and McDonald noted that there is an entire underground cybercrime market and that it doesn’t take a lot of skill to execute one of these cyber fraud schemes.

“These people do not have to be programmers; they don’t have to be cyber experts; they don’t have to have a Ph.D. in programing,” Jevans said. “They can go onto these online marketplaces and buy software to target you, and buy all the pieces that they want for a few thousand dollars to start creating fraud schemes against you that can [cost you] hundreds of thousands or millions of dollars. There is an entire community out there doing it.”

McDonald agreed.

“It doesn’t always need to be a criminal overseas. It’s not hard to download and install [software],” he said. “Maybe they don’t know what they are doing, but we can all point and click and we can enter into a company’s website, have those password hashes, run some more tools and before you know it, you are stealing money.”

**Protect yourself**

McDonald walked participants through ways to protect themselves. He started by talking about password security.

“More often than not, what I see when I’m out in the field are passwords that are the child’s first name, or your pet’s name is always a favorite,” he said. “So you have a pet and his name is Rover, its Rover1. A little bit of research on Facebook and [the hacker] is going to get that person’s pet’s name, that child’s name or spouse’s name. It’s really important to make sure you have strong passwords.”

He noted that cracking passwords is easy to do. Criminals can go on the Internet and Google “WindowsXP password cracker” or “Windows 7 password cracker” and find free tools to crack someone’s password and break into the computer system.

McDonald said having a secure password means having one with...
a minimum of eight characters, capital letters, lowercase letters, and alternative characters like the pound sign or exclamation point. It is important that each password is unique.

“I’m sure everyone on this webinar has 50, 60, 70 different places we log into and who wants to manage all these passwords?” he said. “But if you think about it, in the physical world, you wouldn’t use the same key for your car as your house. You wouldn’t use the same key for your house as your safety deposit box. You wouldn’t use your safety deposit box key for anything else you would lock up. … so in the real world, we have different keys for different doors and it should be the same way online. We need to use separate passwords, complex passwords and do our best so when folks go to pwaudit.com after a server has been breached, it becomes a hard task for them.

Old fashioned precautions

It is also important for those in charge of escrow to have an office with a locked door.

“We are talking about cyber security and malware software, but sometimes simply locking a door is a really good thing to do if you have a workstation with permissions to go in and disburse funds within your settlement services software or use that work station for wire transfers,” McDonald said.

McDonald also advised attendees to make sure company computers are encrypted. He said there is free software out there that, once installed, will protect the information on the computer if the computer itself is stolen.

“Old fashioned precautions

It’s really important because one of the things we forget about is the old fashioned smash and grab,” he said. “These criminals are targeting companies they know have access to the dollar amounts we have in this industry. Break a window, take a computer, go through the computer.”

In addition, McDonald emphasized the importance of performing updates on your operating system and software.

“They are not fun. I don’t think they are fun. The computer usually needs to reboot, and I don’t have time for that,” he said. “But, it’s a decision that needs to be taken seriously and that needs to be done in order to safeguard your future, your company’s reputation and the money that is in your escrow account.”

Preparing for new schemes and the impact of escrow theft

Escrow theft, be it from a trusted employee or a cyber fraudster who hacked into your computer system, has been a fear of the industry for a long time. While agents watch for these schemes, new ones constantly evolve, requiring increased due diligence from everyone handling client money.

During the National Settlement Services Summit, four presenters familiar with the trends — including a supervisor from the FBI — shared insight into what new schemes they are seeing, controls and procedures to protect your company from falling victim to these schemes, and the reality of what could happen should you become a victim of these schemes.

What they are seeing

“I always have to look at it from the standpoint of the threats that you all face internally and externally,” said Jason Watson, supervisor for the FBI in Cleveland. “When you evaluate the internal threats, generally what the FBI sees is simply a tried and true scam where it is typically a crime of opportunity and embezzlement. The only change over the years is simply technology. Maybe the way it’s done has evolved, but the basic scam in and of itself is just an embezzlement.”

In terms of external fraud, Watson said that while the schemes are constantly evolving, there is always a human element to them. With the growing knowledge about phishing schemes, that human element has become a more critical component of the schemes. Often now, Watson said, a phone call will precede the phishing email, causing the victim to lower their guard, open the phishing email and infect the company’s computer system.

“One thing I have not seen as far as fraud cases coming in related to the title industry — but I wouldn’t be surprised if it evolves into that because it has infected other industries — is social engineering, and it has to do with vendors that are vulnerable,”
Watson said. “A company receives an email from what purports to be a vendor that simply says, ‘To an accounts payable clerk, we changed our bank account information. For the next payment that we are due, please change the routing number and account number to this and this.’ And of course, there is a slight variation on the email being received.

“We’ve had numerous companies out there being hit for anywhere from $80,000 to $320,000,” Watson continued. “Ultimately when it is discovered that this was a fraud, at that point forget it, it’s not coming back.”

He also cautioned attendees to be watchful of their vendors as well.

“If I wanted to get into Apple, I’m not going to spend my resources trying to break into Apple, trying to get through to an employee of Apple,” Watson said. “I’m going to look to somebody down the supply chain to see if I can work my way through. We all have vendors or customers that we trust that we provide access. There has got to be some self-evaluation as far as how many resources that entity is putting into its own security. If I’m communicating with somebody that I trust, I am going to get infected because they are the weakness, not me.”

**Escrow theft fallout**

One of the things that was reiterated a few times during the presentation was the fact that once money has been stolen from an escrow account, it is very hard to get it back.

“Typically after a breach, and money has left your account, it is extremely difficult for us to get back that money,” Watson said. “It’s extremely difficult for the banks to get back the money once it has left the country. Typically by the point that I’m actually getting a call, the money is gone.”

He explained that the laws of the United States apply only to those in this country.

“Once money goes over to another country, we are dealing with the laws of another country, where we are simply guests, or in some countries, where we are not even guests,” he said.

Brent Scheer, treasurer, chief financial officer and chief operations officer for Agents National Title Insurance Co., said he once identified a loss within five months of the actual fraud occurring, and knew exactly what the money was spent on, but the company has yet to see that money. The FBI got involved and discovered that this was part of a bigger dragnet that involved real estate agents, appraisers and possibly lenders. The fraudster was dealing with some of the players in the larger scheme, and it was four years until a verdict was handed down against the fraudster because the FBI couldn’t compromise the case it was working on within the construct of the larger scheme.

“That was frustrating,” Scheer said. “We understood, and we kept up with the FBI agent, but it was frustrating because [the money] was gone.”

Watson said that for white collar cases, it typically takes two or three years from the point the case is opened until an indictment or information is filed in court. If the case goes to trial, that can push the case another year.

“The challenges we face with white collar is we have to prove criminal intent,” Watson said. “It is often a very document-intensive type of investigation and that is one of the reasons for the duration. We also look at the availability of our prosecutors.”

**Safeguards and controls**

The presenters also discussed safeguards and controls that attendees could put in place to protect their companies.

“Typically, when the conversation does turn to the FBI, that means there must have been some type of breakdown, whether it’s a breakdown in controls, or whether controls were never there in the first place,” Watson said.

“I think there is a combination of three things when you start talking about escrow fraud and protecting your money and your business,” said Dick Reass, chief executive officer and founder, Reliant Title and RynohLive. “You have to protect your documents, your data and your dollars. You can’t tackle them individually. I think they are all interrelated.”

“There are physical safeguards, administrative safeguards and technical safeguards,” said Chris Loeffler, an attorney at Kelley Drye & Warren LLP. “These are the three big categories to look at. At the end of the day, it can be, what is the low hanging fruit I can pick to make my office a little bit better and a little bit safer.”

Loeffler discussed physical safeguards, saying that agents should think about the office environment and the structure.

“This can be everything from locked doors to files and cabinets, key card access with limitations for people who actually should have access,” he said. “If everyone has access to the back room where everything is stored, does everyone in the office really need to have access to the back room?”

Loeffler said he helped resolve a breach earlier in the year that occurred
over the holiday season. The company had gone through some consolidations and a number of employees were no longer going to be staying with the company in 2013. Those employees had access until their passes were no longer valid. They used the holiday season, when they knew everyone was going to be out of the office for three or four days, and made themselves comfortable using their keys. They also knew where all the cameras were and turned the cameras away. When everyone came back to the office after the holiday, seven computers were missing, along with a box of documents to be shredded and one employee’s personal check.

Scheer noted that when disposing of an old computer it is important to make sure the hard drive is wiped out. The same should be done to old copiers.

Reass said it is essential to have a good CPA, a good attorney and a good bank that supports the company.

Reass also said daily reconciliation of accounts is critical. “There have been a lot of studies and they said the number one protection against fraud is frequent reconciliation,” he said. “That is the number one way to protect yourself is to reconcile your account frequently, more than once a month.

Read your company’s bank wire agreements because your agency may have indemnified the bank in terms of any problems that occur.

Also make sure to have dual controls for sending wires. Scheer emphasized both of those points with another story of an agency he worked with. When the company set up its wiring procedures, it was set up with a single wire authorization.

The signatory thought he was doing his coworkers a favor by setting it up so he didn’t have to bother anyone with getting a second authorization. Their computer contracted a virus and some fraudsters from Nigeria pulled $440,000 out of the account.

“Once money goes over to another country, we are dealing with the laws of another country, where we are simply guests, or in some countries, where we are not even guests.”

- Jason Watson
FBI

“Once money goes over to another country, we are dealing with the laws of another country, where we are simply guests, or in some countries, where we are not even guests.”

- Jason Watson
FBI

They put the money back and tried to recoup it, but the bank looked to them and said you signed off on this,” Scheer said. “Here is the other scary part: The moment the agency asked for that single user, the bank said, ‘You realize that is wrong. You shouldn’t do that.’ ‘Yes.’ ‘Ok, well, sign here. This says we told you that.’ And of course when they try to recover that from the bank in the court room, that was front and center. So, be aware of what can happen in terms of who is authorized to do what with your bank.”

In terms of technical safeguards, Loeffler said there are numerous software solutions. This includes considering who has access to company computers, ensuring employees have unique logins and robust password requirements.

Loeffler cautioned that while outsourcing some of these technical safeguards can be useful, remember the liability to customers and users is not being outsourced along with it.

“At the end of the day, when we use certain service providers, we have a contractual protection in place, but that doesn’t mean your company’s reputation and business isn’t on the line and that you can’t ultimately be held liable to a regulator or a state attorney general who comes asking questions after you have had a breach of security incident,” he said.

Evaluate your firewall protection. Scheer said that some of the biggest names providing firewalls actually rank lower than their less well known counterparts.

“Question your firewall, question network security, because that is one way you can mitigate this,” Scheer said. “Then make sure, of course, in your employee manuals that you guys have an Internet policy and computer policy.”

“That is a great point,” Watson said. “We have all these policies in place, including the FBI. All it takes is one employee not to follow the policy to infect all of the systems that are in place. Internally, we always talk about that thumb drive that is just left on the floor or on the desk, how there is no way in the world you should be sticking that in the computer to see what’s on it.”

Questions? Comments? Contact Andrea Golby at agolby@octoberresearch.com.

“Once money goes over to another country, we are dealing with the laws of another country, where we are simply guests, or in some countries, where we are not even guests.”

- Jason Watson
FBI
North American Title Insurance Company (NATIC) knows what it takes to own and operate a title business in today’s economic environment. That’s why in 2012, we increased our independent agent premiums by over 250%. As a true business partner, we provide our agents with:

- A one-hour underwriter response guarantee
- Access to our AgentLink web portal, replete with resources, business tools and technologies our agents need to become successful
- A team of seasoned veterans who will work with you to help increase your business and convert your prospects and clients into real bottom-line profitability
- Personalized service and transparency between your business and our experienced team of professionals
- All the resources of one of the best risk-managed title insurers in the nation: NATIC currently maintains a national best average (2:1) of premiums issued to policy holder surplus
- Exceptional financial ratings: NATIC is rated A’ (Unsurpassed) by Demotech, Inc. and B++ (Good) by A.M. Best

While legacy underwriters across the country jockey for the same old market share, we have a different strategy: grow our agents. In a market that has been defined for decades with limited and indistinguishable options, NATIC has emerged as the only truly unique choice in title insurance underwriters. All signs are pointing our way. Start in a new direction with a new kind of underwriter.

©2013 North American Title Group and its subsidiaries. All Rights Reserved North American Title Group and its subsidiaries are not responsible for any errors or omissions, or for the results obtained from the use of this information. | NATIC 13-2550 R 10-17-13

GEOFFREY B. GINN, ESQ.
Senior Vice President,
Independent Agency Division
10150 Mallard Creed Road | Suite 505
Charlotte, NC 28262

t: 980.229.6657
d: 866.596.2842

www.natic.com
Financial Crimes Enforcement Network

The Financial Crimes Enforcement Network’s (FinCEN) Mortgage Fraud SAR Filings in Calendar Year 2012 showed that suspected mortgage fraud reports declined 25 percent in 2012 (from 92,561 to 69,277) as compared to the previous year. The past three years of suspected mortgage fraud suspicious activity reports (SARs), if counted by the date they were received by FinCEN, accounted for approximately 46 percent of the past decade’s mortgage fraud SARs.

However, suspicious activity is often only recognized and reported years after loan origination, after a review of origination documents is prompted by a loan default, repurchase demand, or other factors. As a result, many mortgage fraud SARs are filed much later than the date that the suspicious activity actually began. Thus in 2012, 57 percent of SARs received reported mortgage loan fraud (MLF) activities that started more than five years before the SAR was filed.

The bulk of FinCEN’s MLF SARs, regardless of filing date, reference suspicious activity that filers believe began in calendar years 2006 and 2007. The statistics show that there was an extraordinary concentration of suspicious mortgage origination activity beginning in 2006 and 2007, the years immediately preceding the financial crisis of 2008.

Depository institutions filed 37,457 MLF SARs in 2006 and 52,862 in 2007. At the time, those numbers represented huge increases over previous years, but they seriously underrepresented the amount of suspicious mortgage fraud activity that could have potentially been reported in those years if the suspicious activity had been detected closer to loan origination.

Interthinx

Interthinx’s national Mortgage Fraud Risk Index value is 104 as of the second quarter, a 4 percent increase from both last quarter and from one year ago. Among the four fraud categories indexed nationally, identity fraud risk is at 91, up 7 percent since last quarter; property valuation fraud risk is at 105, a 4 percent drop from last quarter; occupancy fraud risk is at 126, up 10 percent from last quarter and up 14 percent from one year ago; and employment/income fraud risk is at 92, a 2 percent increase from last quarter.

With housing prices and interest rates rising, it is likely that demand for adjustable-rate mortgages (ARMs), which still have rates below 3 percent, will increase. For all fraud risk types, index values are much higher in adjustable-rate mortgages than in fixed-rate mortgages.

Nevada displaced California as the riskiest state, with a Mortgage Fraud Risk Index value of 132, a jump of 7 percent from last quarter. California is the second riskiest state with an index value of 132, a 4 percent climb from last quarter. The District of Columbia and Florida are in third and fourth places, respectively, with index values of 128 and 117.

“Mortgage fraud is a hallmark indicator of other trends,” said Ashley Woodworth, Interthinx vice president of business development and corporate strategy. “For example, traditional fraud hotspots in California, Nevada, and Florida were hardest hit by high rates of default, foreclosure, and underwater borrowers because of

Recommendations for fraud prevention

Use common sense and trust your gut instinct. If some aspect of the transaction or the parties’ behavior and manner of communication doesn’t quite “feel right,” stop, question, and re-examine the transaction for legitimacy.

Look for the red flags. Things that don’t belong, seem out of place or are improper, such as the examples discussed above.

Be proactive and educate your employees about identity theft. Encourage them to ask for ID before they notarize any documents and never notarize documents brought in by a client “for a relative.”

Verify Social Security numbers.

Request additional ID if necessary.

Beware of suspicious conduct. Intimidating or pushy customers always in a hurry causing you to overlook details or due diligence, customers who “dangle the carrot” with promises of other big or many future deals to come if this one gets pushed through, name-droppers who allude to famous players or potential deals, and those who give the impression of significant wealth to impress others.

Source: Lynn Wilburn, president of Wilburn Investigations, Inc., NATIC

www.TheLegalDescription.com
widespread fraud in loan originations during last decade’s boom. Furthermore, the dynamic rebound of markets where housing prices are rising shows a corresponding increase in fraud risk. While the market rebound is welcome, this report reminds us that fraud is much easier to commit in a rising market.”

LexisNexis

LexisNexis Risk Solutions’s 15th Annual Mortgage Fraud Report spotlights three economic indicators: mortgage fraud and misrepresentation activity involving industry professionals, potential collusion activity, and for the first time, new data showing the volume of properties in default. The report is based on data submitted to the LexisNexis Mortgage Industry Data Exchange (MIDEX).

“This year’s study suggests that the more shared problematic economic indicators a state has, the greater its financial challenges will be in the coming years,” said Tom Brown, senior vice president, financial services, LexisNexis. “With Consumer Financial Protection Bureau mortgage regulations going into effect in January 2014, and demanding new rules for quality loans, it will be interesting to see what impact this has on overall mortgage defaults.”

Analysis of all loans investigated in 2012 and submitted to MIDEX shows a five-year high of 69 percent of all reports received having some type of application misrepresentation or fraud. Similarly, when focusing on just those loans originated in 2012, 61 percent report application misrepresentation and/or fraud. This is up from 49 percent of loans originated in 2011 and 43 percent in 2010.

For the first time in the study, a nationwide aggregation of available LexisNexis property data was used to determine states most likely suffering from the largest percentage of properties in default. Florida and Nevada experienced the most dramatic decreases in properties in default even though they were ranked first and fourth, respectively, on the list for 2012.

Five states appear on both the Investigation and Origination Mortgage Fraud Indices (MFIs) and the newly established list of Property Default Rankings: Florida, Georgia, Illinois, Nevada and Ohio. New Jersey was the only state in the study that made it on all three top-10 lists for mortgage fraud and misrepresentation reported to MIDEX, potential collusion and property defaults.

Ohio, which ranked first on the Origination MFI list, with a ranking of 224, had more than two times the expected rate of fraud or misrepresentation based on origination volume.

Eight states — Alabama, Delaware, Iowa, Kentucky, Louisiana, Pennsylvania, New York and Vermont — rank highly on both Collusion Indicator Indices (CILs) as areas with high percentages of potential non-arm’s length transaction activity.

CoreLogic

CoreLogic reported that fraud risk among U.S. mortgage applications declined 5.6 percent year over year in the second quarter of 2013. Fraudulent residential mortgage loan applications totaled an estimated $5.3 billion nationally in the second quarter of 2013, down from $5.5 billion in the second quarter of 2012, but up slightly from $5.2 billion in the first quarter of 2013. Fraudulent loan applications reached a combined value of approximately $10.5 billion for the first half of 2013.

CoreLogic’s analysis indicated that during the second quarter of 2013 approximately 19,700, or 0.8 percent, of mortgage applications were identified as having a high risk of fraud, down from 20,900, or 0.7 percent, in the second quarter of 2012. Quarter over quarter, fraudulent application volume remained relatively flat.

The CoreLogic Mortgage Fraud Report examines the collective level of fraud risk among mortgage applications at the national, state and core based statistical area (CBSA) levels. Developed using the company’s proprietary mortgage fraud data and predictive scoring technology, the report measures overall fraud activity based on the CoreLogic Mortgage Application Fraud Risk Index, as well as within six specific indexes: income, occupancy, employment, identity, property and undisclosed debt.

Among these six indexes, intentional misrepresentation of income on a mortgage application showed the greatest year-over-year increase in the second quarter of 2013 at 13.3 percent. Quarter over quarter, income application fraud risk increased 7.5 percent. Property fraud risk, or deliberate over- or under-valuing of a home to achieve illegitimate gains, showed the greatest decrease at 20.8 percent in the second quarter of 2013 compared to a year ago. On a quarter-over-quarter basis, property fraud risk decreased 7.1 percent.

The total dollars of fraudulent mortgage loan applications increased in 27 states compared to a quarter ago. Ohio had the highest year-over-year growth in mortgage application fraud risk at 30.1 percent, followed by Hawaii (19.6 percent), Kentucky (16.6 percent), Connecticut (15 percent) and Alaska (13.8 percent).
Comptroller discusses cyber threats, solutions

During a speech to the Exchequer Club, Thomas Curry, comptroller of the currency, discussed the risks posed by cyber attacks, as well as ways bank regulators and the private sector can work together to curb this risk.

“From a vulnerability perspective, we are at increased risk due to our banking system’s significant reliance on technology and telecommunications, and the interconnections between these systems,” Curry said. “Banks not only operate their own networks, they also rely on third parties to support their systems and business activities. Some of these third parties have connections to other institutions and servicers. Each new relationship and connection provides potential access points to all of the connected networks and introduces different weaknesses into the system. Ultimately, these interconnected networks are vulnerable to attacks that may affect multiple organizations at one time. Moreover, the ubiquity of the Internet means that a large part of the systems used by banks and third parties ultimately rely on telecommunications and technology that is outside of their control.”

“Our title and settlement industry has typically thought of the Department of Housing and Urban Development, state insurance departments, etc., as the regulators that impact us most,” said Christopher Gulotta, founder and chief executive officer, The Gulotta Law Group PLLC, Paradigm Title Agency and Settlement LLC and Real Estate Data Shield. “But with the formation of the Consumer Financial Protection Bureau (CFPB) and its mandate to regulate financial institutions more closely and to hold them accountable for the compliance of their third-party service providers, our industry has been forced to now become aware of the regulators who our up-stream clients are most affected by. Lenders wrestle day-in and day-out with OCC compliance, and as the largest single-source of business for our industry, what affects lenders, affects us. So, when the comptroller of the currency speaks to the increasing cyber security threats, our industry must listen.

“The OCC is not alone in its increasing cyber security concerns that affect our industry,” Gulotta continued. “This past summer, the CFPB issued its Summer 2013 Supervisory Highlights Report, specifically noted that non-banks are more likely to lack a robust compliance management system and that many lack an adequate system for ensuring compliance with federal consumer laws.”

Curry said that while advances in technology have benefited consumers of financial services, they also expand the industry’s exposure to cyber attacks.

“All of these trends pose special challenges at a difficult time for the industry,” Curry said. “While the cost of attacking bank systems is going down, the resources needed to identify, monitor and mitigate against vulnerabilities and potential attacks are increasing. It’s not easy to demonstrate a return on investment for implementing strong security that prevents systemic cyber attacks. How does an institution know whether its defenses are sufficient? Or what costs might have been incurred from an attack had it not been successfully thwarted? The fact is that cyber attackers need only limited resources to influence or breach of a lender’s

 Common schemes and fraud red flags

The following are some of the most common schemes we have seen in the title industry in recent years; this is not meant to be an exhaustive list. There are, to be sure, new schemes surfacing all the time and title professionals are encouraged to follow current governmental or industry efforts to prevent fraud and identity theft.

FALSE LOAN DOCUMENTATION

This was one of the principal causes of the recent collapse of the subprime mortgage industry. In many “no doc” loans processed over the past 25 years, mortgage brokers and applicants became very “creative” with their purchase and refinance loan applications.

PURCHASES/REFINANCES BASED ON INFLATED APPRAISALS

This typically happens when a disreputable licensed appraiser furnishes an appraisal containing misleading information about the property’s attributes, or an inflated appraisal based on fraudulent or inapplicable comps to bolster a value that matches, approximates or is in the range of the desired loan amount.

REMOTE CLOSINGS

With the increase in mortgage fraud today, any closings that take place outside of a title company office should only be handled by experienced closers who can spot potential fraud and/or forgery scenarios.

RELATED TRANSACTIONS

Family transactions, where one family member is conveying to another, present a number of possibilities for fraudulent activity ranging from forgery to identity theft to a garden variety of fraud, such as undue influence or breach of a lender’s
Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”

The OCC is also stressing certain lessons and fundamental processes that need to be in place to ensure that banks are secure and resilient.

“It’s important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them,” Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”

The OCC is also stressing certain lessons and fundamental processes that need to be in place to ensure that banks are secure and resilient.

“It’s important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them,” Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”

The OCC is also stressing certain lessons and fundamental processes that need to be in place to ensure that banks are secure and resilient.

“It’s important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them,” Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”

The OCC is also stressing certain lessons and fundamental processes that need to be in place to ensure that banks are secure and resilient.

“It’s important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them,” Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”

The OCC is also stressing certain lessons and fundamental processes that need to be in place to ensure that banks are secure and resilient.

“It’s important that financial institutions, at the board and senior management level, are aware and engaged, and that they understand the risks posed by these threats and the security measures needed to address them,” Curry said. “Whether offering a new product or making a strategic business decision, most bank activities have the potential to introduce vulnerabilities into the system, and it’s vital that senior management appropriately evaluate risks and develop prudent implementation and contingency plans.

“Senior level engagement shouldn’t stop at the bank walls,” he continued. “To deal with cyber security effectively, institutions both large and small need to communicate with each other, as well as with relevant government agencies. The financial services community has a robust public-private sector partnership, which can be leveraged even more for the benefit of the system. For example, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is an information sharing non-profit organization run by financial institutions, includes the OCC and other public-sector agencies as members.”

Curry said that effective information sharing will help increase awareness within individual institutions and throughout the industry, as well as enable the sharing of best practices and collective response to wide-scale events.

“If you read the OCC Interagency Guidelines Establishing Standards for Safeguarding Customer Information (12 CFR 30, Appendix B), you can see the similarities in the regulator expectations of banks in connection with the safeguarding of customer information and how the OCC back in 2001, identified the increased cyber security risks in the context of banks working with and through third-party service providers,” Gulotta said. “Specifically, banks are required to: identify such risks; exercise appropriate due diligence in selecting such service providers; review controls of such service providers to ensure that such vendors are capable of meeting the compliance requirements; oversee these service providers; and monitor such service providers through, for example, audits.”
**Title Insurance Task Force finalizes escrow theft white paper**

The Title Insurance Task Force of the National Association of Insurance Commissioners (NAIC) met on Oct. 1 with one mission — finalizing the Title Escrow Theft and Title Insurance Fraud White Paper. The Escrow Theft White Paper Subgroup worked for more than a year to develop a toolkit that regulators and title industry members could use to prevent escrow theft and the group completed their work in August.

It was then the task force’s job to finalize and adopt the paper. While the group did not have a quorum to adopt the paper that day, the NAIC was going to email the task force’s members to get a final vote to adopt before sending it to the Property and Casualty Committee for approval.

**Purpose and history**

In the introduction, the subgroup said the paper is intended to raise awareness and to be available as a tool for regulators to research methods for combating and preventing escrow theft, title insurance premium theft and other forms of fraud associated with title insurance and closing services. It stated that industry members can use it when evaluating their own enterprise risk management and auditing guidelines for combating escrow and title insurance premium theft.

“This paper points out that no single remedy exists to address the problems relating to escrow and title insurance premium theft,” the paper stated. “The goal of the paper is to raise the level of awareness and discuss some potential safeguards to reduce or prevent the occurrence of such problems.

“The ability to reduce or diminish opportunities for such misappropriations lies jointly with regulators, title underwriters, trade associations, title agency owners and individual title agents and escrow service providers. Consumer education can also play a role in helping to identify potential problems,” the group continued.

“While the methods outlined in this paper are by no means exhaustive, it is the goal of the NAIC Title Escrow Theft White Paper (C) Subgroup that the paper will serve as an initial tool for addressing the problem, promoting discussion and improving consumer protection,” it stated.

**Identified schemes**

“Title insurance and closing services have historically been a labor-intensive process with few opportunities for centralization of services within a title underwriter,” the group stated. “Although direct services have grown due to increased availability of digitized courthouse records, title underwriters rely on a large number of licensed and unlicensed individuals who are not directly employed by the title underwriter for title searches, issuance of commitments and policies, handling of premium and escrow funds, providing closing services and post-closing services.

Injunction regarding the sale of marital assets, so consent of a spouse may be required whether or not he/she is in the title. A final divorce decree is an official judgment of record, the terms of which may be binding on the parties and the title company or lender (even though not a party thereto) in financial transactions involving the property.

**QUIT CLAIM DEEDS OR UNRECORDED RELEASES PRODUCED ON REQUEST** These are usually title “clearance” issues that arise during a review of the special exceptions, “wild deeds” and prior, unreleased liens or mortgages shown on Schedule B of the title commitment. Whenever an unrecorded release is presented at closing, it deserves scrutiny to ensure that it is authentic and was simply mislaid and not fraudulent.

**DISBURSEMENTS TO PARTIES WITH NO APPARENT INTEREST IN THE SUBJECT PROPERTY**

This has been a favorite of unscrupulous brokers and attorneys who create a corporation or LLC to pull another $40,000 or $50,000 out of the deal as a contractor that allegedly performed valuable services in getting the property “ready for market.” The FBI has identified these entities as major players in the mortgage fraud field.

**SIGNATURE DISCREPANCIES**

Major differences between current and old signatures of record often indicate forged documents in the chain of title or identity fraud.

**WILD DEEDS IN THE CHAIN OF TITLE** These appear frequently in the case of deceased or delinquent landowners in foreclosure and are usually forged deeds to relatives or insiders to create the appearance of a legitimate conveyance to such
This decentralization, along with the large number of individuals and large number of financial transactions, increases the opportunities for those that decide to operate in a dishonest or untrustworthy manner."

The paper identified several methods by which escrow theft is perpetrated. They include:

- Misappropriation of closing funds for use other than as provided for in the closing instructions;
- Failure to pay off existing mortgage loans in full, diverting closing funds for personal use while attempting to make periodic payments on the existing loans;
- Misappropriation of title insurance premium with failure to report and issue title insurance policies;
- Failure to perform all services specified in the closing instructions or HUD form;
- Fraudulent activity by unlicensed or unauthorized entities;
- Engaging in check-kiting or other banking-related fraudulent schemes with title agency accounts;
- Acceptance of funds that are not “good funds” for the purpose of closing transactions;
- Intentional or fraudulent misrepresentation of title defects or failure to disclose title defects with the intention of burdening the title underwriter with subsequent losses;
- Participation or complacency in mortgage or real estate fraud schemes such as flipping and flopping (reverse staging), phony appraisals or rushed escrow closings; and
- Cyber fraud aimed at identity theft or misdirection of escrow funds to the accounts of unrelated parties, typically via fraudulently obtained online banking credentials of the title company.

The paper also identified several practices of concern “that may not rise to the level of fraud, but may be non-compliant in many jurisdictions, contrary to title underwriter requirements, contrary to contractual obligations or potentially indicative of fraudulent acts.” They include:

- Mingling of escrow funds with personal or operational funds,
- Inappropriate investment of escrow funds in unsound or non-guaranteed accounts,
- Delays in issuing title policies and premium remittance,
- Failure to fulfill closing obligations (deed filings),
- Mishandling resulting from confusing or poorly written closing instructions, and
- Inadequate prevention of fraud against title underwriters and cyber crime that is initiated by unrelated parties aimed at identity theft, obtaining fraudulent remittances or misdirection of funds.

Regulator tools

The group identified several ways to detect and prevent escrow theft and misappropriation, characterized by which type of entity is potentially best suited to implement them, beginning with those best implemented by regulators.

First, the group noted that the NAIC created two model acts, the Title Insurance Agent Model Act and the Title Insurers Model Act, which have provisions to help curb escrow theft.

“Although not comprehensive, the above outlined provisions of these two NAIC models can provide added protection against mishandling of escrow, settlement funds and title insurance premiums,” the group stated. “For jurisdictions that have not adopted NAIC Model Law No. 230 and No. 628, but wish to incorporate specific provisions intended to address proper handling of escrows and title insurance premiums, the models can be a source for legislative language.”

The group noted that regulators can begin addressing escrow theft at the licensing stage.

“Licensing standards established by a combination of regulatory
rules and statutory provisions can alert a regulator to potential escrow theft requiring intense scrutiny of the licensee’s involvement with an escrow account,” the white paper stated. “Enhanced initial audits or due diligence investigations of title insurance agents or agencies by regulators at the time a title insurance agent is licensed may enable regulators to identify prospective title insurance agents with past legal or regulatory issues, or with backgrounds not indicative of trustworthiness.”

“The amount of money that potentially moves through a real estate escrow account is considerable,” it continued. “This can make escrow theft tempting to those who find themselves in a situation where they perceive an ability to misappropriate escrow funds without being discovered. Thought and further consideration should be given to setting initial licensing standards that strengthen consumer protections, therefore, being less attractive to those with illegal intentions.”

Right now, licensing standards vary among states. Some require escrow settlement service providers to be licensed with departments of financial institutions or departments of insurance and some require no such license for performing escrow services. In drawing up new licensing standards, the group does not want them to be so unrealistic that they end up discouraging growth and expansion in the industry when the economy is booming.

The group also put forth information regarding statutory or regulator-required independent audits.

“On an annual basis, independent audit laws and regulations may require title insurance agents or settlement service providers that handle escrow, settlement, closing or security deposit accounts to submit a filing to their regulator which would require an independent review of their escrow, settlement, closing and security deposit accounts,” the group stated. “Independent audits of title insurance agents and settlement service providers’ depository accounts can be a useful tool for regulators to monitor to determine if title agents are performing best practices within their agency. In addition, these audits provide useful data to the regulator that may indicate that a problem exists or an early warning sign of potential problems within the accounts. Statutory guidelines for the completion of the audits ensure the audits are completed in a timely and concise manner. In addition to the audit, the filing would require supplementary information to be submitted to the regulator.”

The group also identified ways to mitigate escrow theft once it has occurred. For example, some states allow for closing protection letters. A few states have adopted requirements that hold title underwriters responsible for the escrow and settlement activities of their appointed title insurance agents.

The group also floated around the idea of establishing escrow theft reserves to be used to reimburse victims of escrow theft.

“Pre-funding such an account would most likely be accomplished through a per-policy or per-transaction fee, payable into a state-operated fund,” the paper stated. “Attempting to establish an appropriate size fund may be difficult since the impact of escrow theft varies widely by incident. Currently, many escrow thefts are reimbursed by title underwriters. Depending upon the source of such a reserve fund, having such a fund could possibly also reduce incentives for title underwriters to closely monitor title agent and settlement service providers. In at least one state, title underwriters are required to hold reserves for losses independent of title insurance.”

The group also identified these tools:

• Insurance fraud prevention laws;
• Establishment of advisory committees;
• Encouragement of reporting suspected fraud;
• Consumer education;
• Prompt and complete communication between regulators, title agents and title underwriters;
• Time requirements for policy issuance and policy and premium remittance;
• Good funds requirements;
• Minimum capitalization requirements for title agents; and
• Enhanced regulatory oversight, including market conduct regulations and the coordination of regulatory efforts.

Industry tools

The paper recommends title underwriters and agencies consider adopting strict requirements for the handling of premium and escrow funds by their employees in accordance with the federal laws applicable to title related escrow transaction services.

“...in so doing, account review processes and oversight and internal control guidelines adopted by industry associations such as the American Land Title Association (ALTA), may be incorporated into the contracts between title underwriters and title insurance agents that define the business practices employed by these entities,” the group stated. “...By establishing strict requirements and requiring adherence thereto through underwriting or title insurance agent appointment contracts, premium and escrow losses should be more easily detected and losses minimized. Detailed contract provisions may facilitate loss prevention. Loss prevention is a sound business objective and also protects the
consumer from financial harm.” Even when audits are not required by law, underwriters generally audit title insurance agents as part of the agency agreement. The working group identified several audit procedures that underwriters, and regulators, can use to detect fraud or potential escrow theft. They include:

• Determine whether there is a backlog of unissued policies or if policy issuance is delayed because of cash flow problems.

• Require premium trust accounts to assist in preventing premium fraud.

• Evaluate the title agency’s handling of escrow accounts to make certain that funds are handled in a fiduciary capacity, dispersed in accordance with closing instructions and HUD forms, where applicable, and in a timely manner.

• Follow state requirements where applicable. Some states, such as Texas, have specific audit requirements and forms that must be used.

• Interview management and employees to assist in identifying risks and weak controls.

• Review the title agencies’ overall financial condition. It is an important part of determining whether the title agency has sufficient capacity to meet its ongoing obligations.

• Diligent efforts should be made to ensure that the title agency has provided access to all appropriate records and accounts.

• Employ adequate sampling techniques for escrow and file review.

• Evaluate the title agency’s personnel practices for hiring closing staff.

• Identify and follow-up on any signs or indicators of potential problematic or fraudulent activity.

• In general, effective audits can be a good deterrent to escrow and premium theft.

The paper noted that underwriters and IT providers have developed integrated software solutions that integrate several title and escrow activities. These software solutions can “help reduce administrative costs, improve record retention, reduce inadvertent mishandling of funds and provide a less expensive method for title underwriters to audit and oversee activities of title agents.”

State, regional and national title insurance and settlement provider trade organizations offer assistance through educational programs, vetting programs and best practice standard setting programs, such as ALTA’s Title Insurance and Settlement Company Best Practices.