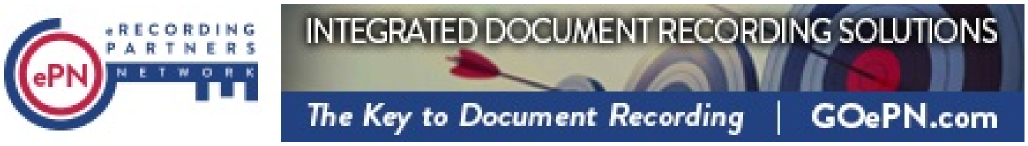
PRIA IN TOUCH

November 20, 2020



President's Message

Dear Members:

It’s an understatement to say there’s a lot going on at PRIA. Multiple work groups and sub-committees are busily engaged in projects and meeting regularly.

The eRecording Best Practices Work Group, which began meeting in early October, has, as the first phase of the project, been reviewing and editing the “2016 eRecording Best Practices for Recorders” paper. They will follow up with a separate project addressing “eRecording Best Practices for Submitters.”

The GIS Work Group, which recently published a “GIS Toolkit – How To Get Started” paper, is now gathering case studies from counties that have already integrated land records and GIS or are in the process of doing so.

The Interstate Notarization Work Group has been working on two different publications. The first, and recently published, is “Electronic Notary: How Does It Impact Recording?” and, as the name implies, addresses both the legal foundations of eNotarization along with practical applications for recorders.

The second project underway by the Interstate Notarization Work Group is an eNotarization and RON FAQs document. A sub-committee meets bi-weekly to outline a series of questions and answers that will guide recorders, primarily, through the details of this technology.

The Ransomware Work Group, which has already published a list of ransomware resources that can be found in PRIA’s Resource Library, is nearing completion of its educational paper on ransomware and cybersecurity. There will be an additional paper from this work group on sample Service Level Agreements (SLA).

The Redaction Work Group has generated a state-by-state list of redaction, confidential record shielding and address confidentiality laws around the country. This project is in the final review phase. At the same time, a sub-group is updating PRIA’s 2014 “Redaction Best Practices” paper. A separate paper on Social Security Numbers was extrapolated from the original best practices document and is now a stand-alone paper found in the Resource Library.

In addition to the current work group projects, there are two additional papers under development. The PRIA Board of Directors authorized an educational paper on “papering-out” to describe the background on this practice, when to use it and a PRIA position.

A sub-committee of the Governance Committee is undertaking the bi-annual review and updates to the PRIA Operating Rules, which define the day-to-day procedures of the association.

Do you have an operational challenge you would like PRIA to address? Or, perhaps you'd like to volunteer for one of the projects underway. Contact me and let's talk.

Have a good month,

Jerry Lewallen
President

In Case You Missed It…

Two new publications have been added to the PRIA Resource Library on the website. Click on the Resources menu and a dropdown menu will appear. Select Resource Library. Type in a key word, like "toolkit" or "electronic notarization," to locate these two additions to the library.

Or, click here to access the **"GIS Toolkit – How To Get Started"** for the how-to guide for implementing a land records and GIS integration. Or, here for **"Electronic Notarization: How Does It Impact Recording?"**, a quick read with general guidelines for recorders on electronic notarization and determining recordability.

If you missed the November 17 webinar, "Inside the Crystal Ball - How Will the Industry Respond to Forbearance," you can access the audio recording from this webinar here (members only). This webinar was an inside look at the difference between judicial and non-judicial foreclosures, the current forbearance percentage in the nation and its expected progression, how to differentiate between short payoffs and charge offs, the different types of loan modifications and how forbearance affects the recorder's office. Broaden your knowledge of how the industry functions.

This and all PRIA webinars are recorded and available to members, on-demand.

PRIA Board Approves New Work Project

During the October 21 Board of Directors Meeting, the board approved a new work project, "Disaster Preparedness - Natural Disasters and Pandemics." A timely topic for this year of COVID.

Natural disasters occur with amazing regularity. Examples of natural disasters include fires, floods, tornadoes, hurricanes and severe weather storms. The COVID-19 pandemic had organizations pivoting, exploring new options for getting the work done, broadening concepts of how work could and would be accomplished without actually being in the "standard" office setting. Each organization that has experienced a natural disaster or operated through the 2020 pandemic has learned hard and soft lessons. PRIA thrives on sharing first-hand knowledge and experience working across the government-business divide, learning from each other, from organizations of all different sizes and from different locations.

Both a business and government co-chair are needed before this project can gear up. Interested? No specific expertise or experience required, only a desire to dig into the topic and engage with a group of volunteers to produce a work product that will assist the PRIA membership in the event their organization experiences a disaster.

Contact Stevie Kernick for additional information or to volunteer.

Maricopa County Sees Increase in Recorded Documents

Maricopa County, AZ, recorded its millionth document for 2020 on October 19 with an electronically recorded document sent from Simplifile. In previous years, this milestone has been reached closer to December, reports LeeAnn Wade, recording director. “I expect this early milestone is because of the significant number of refinancing we are seeing in Arizona,” she said.

A Very Personal Ransomware Story

Trevor Ma, office manager, Viva Escrow

As the IT person for Viva Escrow, I am in charge of keeping our technology secure and in place. This means not only hardware but also software. Unfortunately, my responsibilities have significantly increased in the past few years because of the incessant fear of systems failures, email compromises and possible loss of trust funds through wire fraud.

Viva Escrow is a small, privately owned company. A few years ago, our company was hit with a system compromise and ransomware demand. This was even before ransomware became so prevalent. So let me tell you straightforwardly that, “Yes, it can happen, it is terrible and it could have ruined our business.”

Ransomware is a particular type of computer virus that locks your files away and leaves a message requiring payment to have your files unlocked. A number of health facilities and city government facilities were hit in 2019. This type of fraud has increased because the hacked entities are in distress, they pay, and it doesn’t take long for the perpetrators to realize that this is an effective way to make a lot of money illegally.

Here is the Viva Escrow story...

At the end of a workday, one of our staff came to me and told me that something was wrong with her computer. Errors kept coming up on her escrow software, some functions of the software also did not work and there was gibberish.

I confirmed that certain screens could not open and with a feeling of dread, I looked into the system file directory. To my horror, some of the files had been forcefully encrypted.

Think of it like this: you have a computer folder filled with pictures. Suddenly the pictures are renamed and completely converted into something barely resembling what they were before - no longer openable and inoperable.

Written in the HTML document was the ransomware demand: “Your files are encrypted. Go to the link below for further instructions.” I did not go further as I knew what our course of action was going to have to be.

This was the reality of the situation:

- I cannot decrypt the files myself. It would be comparable to looking for a key without even knowing what the lock looks like. It would be impossible.
- Going to the provided link would not give me any assurance of recovering my files. The link would tell me the ransom demand and provide a Bitcoin link to pay. What happens after? Do they take the payment and run or do they send me the decryption key? What if the key they send me is unsafe or contains some other hidden backdoor for them to infect us again?

- I had to make sure any traces of the ransomware or other virus were cleaned from that individual computer, as well as the whole network. How many computer stations were affected? What about our network? I would have to immediately contact our IT consultant to make sure we swept through the system and secured our network.
- I then knew there was only one way to recover the now encrypted unusable files: pull up and re-install using our backup files. Fortunately, our company IT protocol had us performing daily tape backups, as well as a comprehensive monthly backup. If we did not have the backups, the files that were encrypted and all that data would be lost forever.

Our workstations were not completely inoperable from this particular ransomware called **Locky**. The antivirus software was able to scan through the computer and quarantine the remaining unsafe files. Luckily, only one computer station was infected and only a few of the network files. Once we had removed all the infections, we restored the effected folders based on the backup tape. Regrettably, data entered between the last backup and the infection was permanently lost. The internal cleanup took hours and by the time this was all done, it was midnight. The next morning, a call was made to the escrow software company and our network files were properly replaced.

Ransomware has a specific goal in mind: to get money through nefarious means. While other viruses may haphazardly delete files, steal passwords and render computers inoperable, ransomware hits you where it hurts the most: your data, your access to it and your ability to conduct business. It can cripple you into submission so that you will pay up.

Going back to our experience, we put in six hours of work just to restore one affected computer station. Through good fortune and our strong existing network defenses, it did not spread rampantly through our network of 20 individual stations. Our other systems and drives did not need to be reformatted and all their programs reinstalled. Nevertheless, it was still painful and time-consuming. What if not only our escrow software failed, but other software or critical system programs failed? What if it had spread to every other computer station in the network and our servers? We would have been crippled for days or longer. We would not have been able to help our clients with their closing transactions. What if important client personal data had been accessed?

In our community, our reputation would have been destroyed.

In May 2019, ransomware crippled the City of Baltimore affecting their entire system and many municipal services. They were urged not to pay the $70,000 ransom by the FBI; the cleanup has cost them $18 million so far. If ransom was paid and the key given, the city would still have needed to scrub and replace systems, but the alleviation of the short term pain might have been worth the cost of the ransom.

Riviera Beach in Florida was also a target and paid $600,000. On August 16, 2019, at least 22 cities in Texas were hit with ransomware demands. If you were in their IT department, what would you do?

What if replacing the computers and equipment is possible, but the backups were not sufficient or there were no backups at all? We would not have been able to access our client data and we would have been out of business for an indeterminate amount of time. At that point, paying the ransom would have been the only recourse as we would have been desperate to free our files. This is what the perpetrators are counting on. Whether it is our precious family photos, our thesis paper, the company personnel and financial files, customer data, customer non-public personal information and files, or government records, at some point there is a price you would be willing to pay despite it being blackmail and a reward for nefarious acts.

Ransomware is a computer virus and the vast majority of computer viruses infect a device when the user of the computer opens an unsafe program or lets an unsafe script or macro run. One or two clicks in an unsafe site and the virus was planted and the user commits an action that causes infection to happen. This is the challenge of IT departments worldwide, from small companies to large multinational corporations, hospitals and governments. Competent IT departments have an underlying infrastructure in place to protect their networks, but the real key is continuous training for all users to ensure they understand their role in protecting the system.

To summarize, it comes down to three very important things:

- Invest in anti-malware and anti-ransomware software. Make sure it is properly set up and running in the background of all your end-users. Up-to-date software can be that final secure wall to prevent the infection from taking effect. Be sure your systems are scanned frequently.
- Commit to awareness and training about ransomware and safe online practices. This tends to be more labor and time-intensive than setting up anti-malware software, but is arguably more important. If your users are being responsible with their online and network connections, the risk of infection for the present and the future goes down considerably. Teach them to be continuously aware of emails, attachments and links.
- Maintain offline backups, and back up frequently. This can include dedicated flash drives, tape backups or disconnected hard drives. True backups should not be held on the same network they are backing up. The most destructive ransomware variants manage to corrupt backups that were held on the network itself. Store your backups somewhere safe and reliable so that they can be retrieved and usable in an emergency.

My company was lucky; the problem was isolated and solved relatively quickly. The worry-filled nights, however, are continuous. Now that we have had an attack, prevention has become our constant concern.

Find a Vendor in PRIA’s Membership Directory

A new feature has been added to PRIA’s online Member Directory. Business members of PRIA can indicate the services they offer, which will then display when a user clicks on the drop-down menu on the main page of the directory. Let other members know exactly the products or services you offer.

Log into the members-only side of the website and select the “My Membership” tile. Click the "Profile" link at the top and then the “Custom” tab. Select one or more "Services Offered" in the dropdown menu and click "Update."

If a service offered by your company is missing from the list, please contact Mallory Robinson and it will be added.

Need a Membership Certificate?

Now you can print a membership certificate to display in your office or at an industry event. Log into the members-only side of the website and select the “My Membership” tile.

Click to download a printable PDF membership certificate for the current year.

Welcome New Members

PRIA welcomed these new members in October.

Government
Joyce Mascena, retired, South Windsor, CT

Business
Idealogic PDS Inc., Toronto, Ontario, Canada

Total paid membership as of October 2020, is 623.

MAJOR CONTRIBUTORS 2020-21

PRESIDENT'S CIRCLE

CSC
eRecording Partners Network
Simplifile

NATIONAL ASSOCIATION

American Land Title Association

PLATINUM

Kofile Technologies
MERSCORP Holdings, Inc.
Pioneer Technology Group

GOLD MEMBERS

Avenu Insights and Analytics
Black Knight - Ernst Fee Service
Computing System Innovations
CoreLogic
Esri Inc.
Fidelity National Title Group
Granicus Inc.
Harris Recording Solutions
Nationwide Title Clearing
Rekon Technologies
Synrgo
Tyler Technologies
Westcor Land Title Insurance Co.

CONTENT DISCLAIMER

The views and opinions expressed in the media, articles, comments, or links in this publication are those of the speakers or authors and do not necessarily reflect or represent the views and opinions held by PRIA or its members. PRIA does not warrant the accuracy, timeliness or completeness of the information contained in this publication. If you have a complaint about something you have found in this publication, please contact PRIA by email at **info@pria.us**.

Property Records Industry Association
coordinator@pria.us
919.459.2081