


Data Security: Knowing the Dangers, Protecting Yourself and What's Next?

Rick Diamond
VP, I.T. Director
Rick.Diamond@fnf.com



@RDIAMONDFNF

Pamela Williams
AVP, Digital Solutions Manager
Pamela.Williams@fnf.com

A black and white photograph of a man with a beard and mustache, wearing a button-down shirt, sitting at a desk in an office. He is looking down at a tablet device in his hands. On the desk, there is a laptop and some papers. In the background, there are shelves with books and other office equipment, slightly out of focus.

The need for quick and easy access is largely driven by and fed by technology adoption and the security responsibility that comes with it.

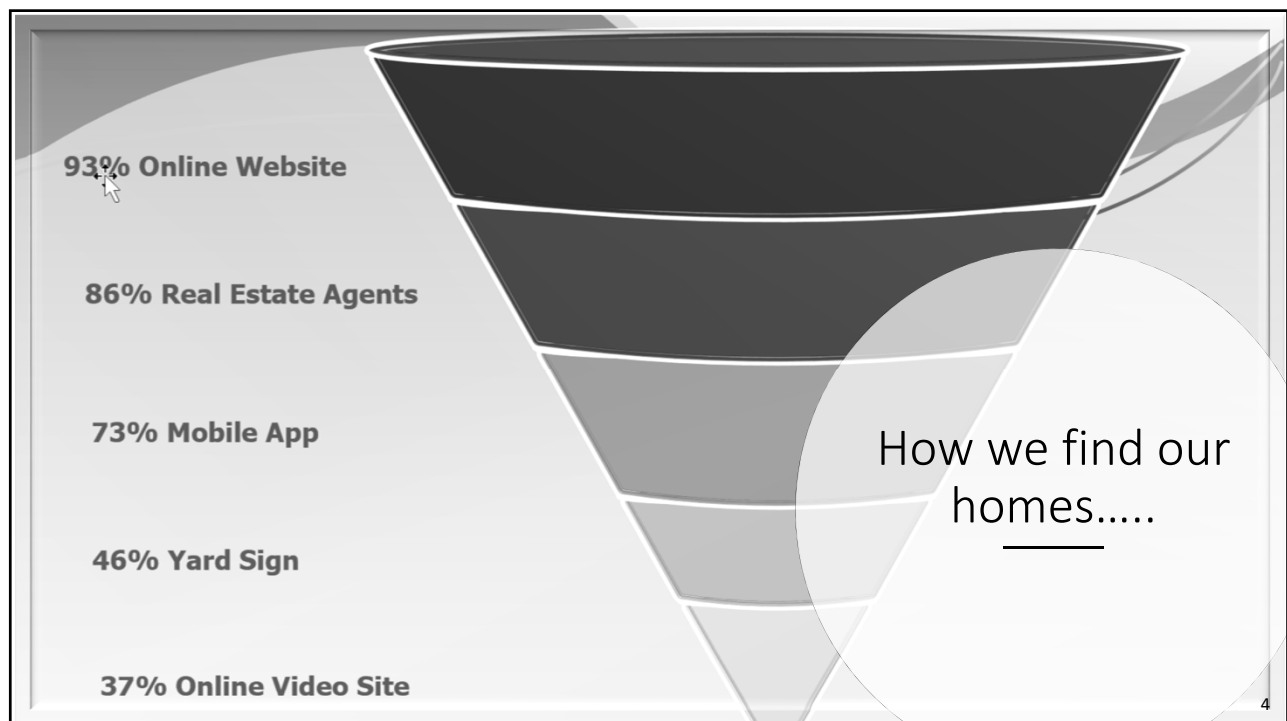
...and it is changing your customer's expectations.

90%

Lets first talk about Digital access

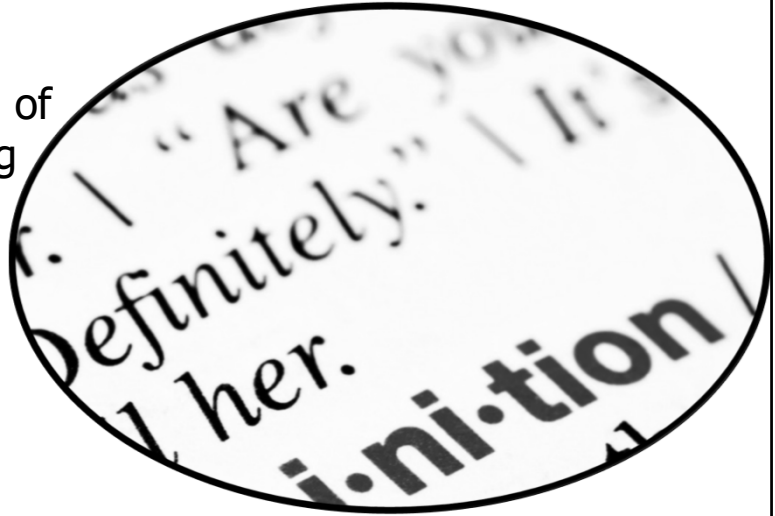
**46% of smartphone
owners say their
smartphone is
something
"they couldn't live
without"**

3



What is a Digital Transaction?

The electronic execution of some or all of the closing documents, which could include electronic signature, notarization, and recording.

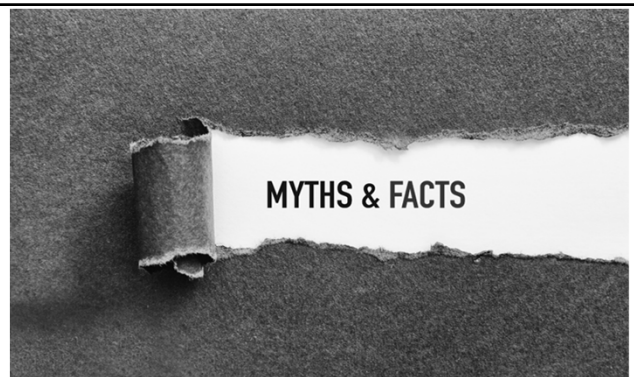


5

Two Common Myths:

Digital Closings are REMOTE

Digital Closings must be 100% paperless



One Important Fact:

Data Security is more critical than ever!

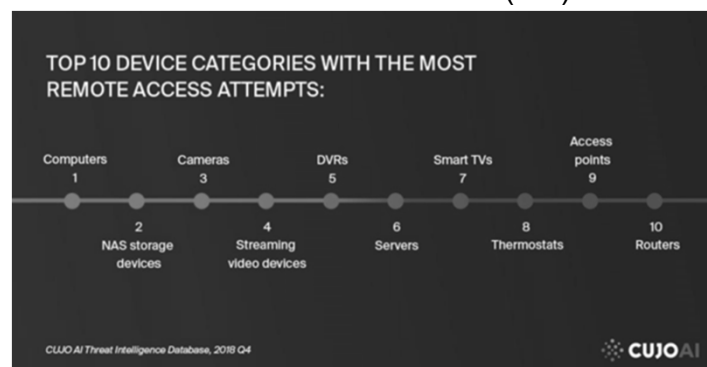
6

Top cybersecurity statistics for 2019

- Half of all Cyber attacks are targeted at small businesses
- Estimated \$6 trillion in damages by 2021 – more than all natural disasters and the sales of illegal drugs!
- \$76 billion of illegal activities involves bitcoin
- Only 10% of cybercrimes are reported in the U.S each year
- By the year 2024 that the cyber security market will be a \$300 billion industry!
- **Ransomware attack every 14 seconds!**
- Up to 200 billion IoT devices will need securing by 2020
- An IoT device could be attacked easily within the first five minutes of connecting to the internet!
- 95% of cybersecurity breaches due to human error.... *91%percent of attacks by cyber criminals start through email*
- Globally, Microsoft tracks nearly 6.5 trillion — yes, trillion — cybersecurity events per day.
- Globally, vents per day.
- *Cost for cybercrime globally was over \$1 trillion in 2018 – More in 2019!*

Cybercrime Trends of 2019

Remote Access Attacks (IoT)



Attacks via smartphones

One of the most common attack vectors to smartphones are related to unsafe browsing (phishing, spear phishing, malware). More than 60% of fraud online is accomplished through mobile platforms, according to RSA, and 80% of mobile fraud is achieved through mobile apps instead of mobile web browsers.

Top 5 Cybersecurity Predictions for 2020

- **Compliance fatigue will spread among security professionals** - insufficient cybersecurity skills and small budgets, and cybersecurity professionals may start to flatly disregarding a mountain of regulations.
- **Third-party data breaches will dominate the threat landscape** - IBM says the average time to identify a breach in 2019 was as high as 206 days. Such attacks are infrequently detected both due to their sophistication and lack of skills amid the victims.
- **External attacks will continue to expand without control** - 61% of organizations have experienced an IoT security incident in 2019. The global proliferation of IoT, connected devices and the usage of public cloud, allows for multiple access points. ***Don't forget them!***
- **Cloud misconfigurations will expose billions of records** - Gartner reports that around 95% of cloud security failures result as a fault of the customer, not vendors of public cloud infrastructure.
- **Password re-use- and phishing attacks will skyrocket – *Still think Passwords are not a problem?***

2020



Those darn Passwords!

- **Are you proactively managing your passwords?**
 - Use strong and complicated passphrases
 - Don't use the same passphrases for different accounts
 - Change your passphrases frequently (60-90 days)
 - Don't share your password with anyone (especially family!)
 - Use Multi Factor Authentication (MFA) to log in
- *Hackers know users cling to favorite passwords and weak passwords, resisting changing credentials regularly and make them stronger. It's why attackers reuse old passwords found on one account to try to break into other accounts of the same user.*
- You can check - <https://haveibeenpwned.com/>

A Password Manager can help

- DashLane - <https://www.dashlane.com/>
- LastPass - <https://lastpass.com/>
- KeePass - <http://keepass.info/>

2019



Those darn Passwords!

How about your Smartphone?



- Only real way to get in is with Brute Force because of strong encryption
- It takes on average this long to break into an iPhone when a passcode contains only the numbers 0-9
 - **Four digits: 7 minutes**
 - **Six digits: 11 hours**
 - **Eight digits: 46 days**
 - **Ten digits: 12.5 years**



2020

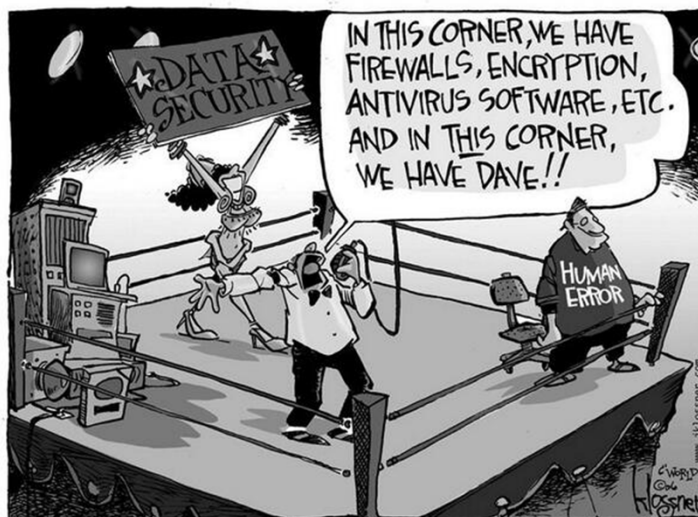


Growth of Ransomware in 2018-2019

- According to Cybersecurity Ventures, ransomware damages were predicted to exceed \$8 billion in 2018. (Source: Cybersecurity Ventures)
- Ransomware downtime costs organizations more than \$64,000 on average. (Source: Coveware)
- Ransomware is costing businesses more than \$75 billion per year. (Source: Datto)
- The FBI suggests ransomware payments are totaling around \$1 billion. (Source: Datto)
- A tenth of all businesses reporting stated their ransom demand was \$5,000 or more. (Source: Datto)
- Nearly 40 percent of ransomware victims paid the ransom!
- ***Backups are extremely important!***
- ***Remember this stat? 91%percent of attacks by cyber criminals start through email***

2019

comparitech



Hacking a human is by far the easiest way to get into a network!

Take this opportunity to educate your Realtors and clients!

Ransomware – What to expect in 2020

- Enterprise ransomware attacks have seen a more than 300% increase in the last year...The rate of detections within businesses rose from 2.8 million in the first quarter of 2018 to 9.5 million in the first quarter of 2019. That's nearly a 340% increase in detections.
- Cybersecurity Ventures predicts ransomware will cost \$6 trillion annually by 2021. (Source: Cybersecurity Ventures)
- McAfee predicts some common ransomware targets will decrease. However, the company suggests cybercriminals will target less common and more vulnerable victims, such as individuals with high net values and connected devices (IoT). (Source: McAfee)
- Palo Alto Networks predicts a noticeable increase in Mac ransomware this year. (Source: Palo Alto Networks)
- MIT predicts cloud computing companies will see increased attacks against their systems. (Source: Computer Weekly)
- Mobile malware attacks will increase in 2020. Malicious mobile will mimic reputable apps, a key problem that's on the rise, which will mean both consumers and app stores will have to vet apps more carefully in 2020.

2019

FBI IC3: EAC and BEC Statistics

- BEC Fraud Losses Grew to \$1.3 Billion in 2018: **FBI**
- The 2018 Internet Crime Report (ICR) shows that both the incidence and cost of internet crime continues to escalate. Complaints rose 14.3% from 2017 to **351,937** in 2018
- The greatest financial loss to internet crime came from business email compromise (BEC) and email account compromise (EAC) scams. 20,373 victims lost a total of \$1.298 billion.
- BEC and EAC are constantly evolving as scammers become more sophisticated. The scam has seen personal eW-2 information, and mails compromised, vendor emails compromised, spoofed lawyer email accounts, requests for the targeting of the real estate sector.
- Greater losses occurred in the over-60 age bracket. 62,085 over-60 victims lost just under \$650 million compared to 48,642 victims aged 50-59 losing just under \$495 million.
- **You must stay vigilant!**

2020

So what can you do to protect yourself and your business?

Professional email Solutions

- GoDaddy Professional email - <https://www.godaddy.com/email/professional-email>
- Google email for your Business - <https://www.google.com/work/apps/business/>
- *This is also a good opportunity to review any E&O or professional liability insurance to confirm it covers cybercrime and data breach.*

Backups, Business Continuity

- What are your backup procedures?
- What is your Business Continuity plan?
- Are they documented and tested?
- Infrascale – <https://www.infrascale.com>
- Carbonite – <https://www.carbonite.com>

So what can you do to protect yourself and your business?

- 1. STOP Dave from clicking on everything!
- 2. Don't let anyone access their personal email on your network!
- 3. Do not allow the use of removable devices like flash drives!
- 4. Destroy old hard drives of computers and copiers!
- 5. Proactively manage your passwords!
- 6. Use Passphrases & long Smartphone passwords
- 7. Use Multi Factor Authentication (MFA) to log in
- 8. Encrypt email! Or use a Secure Portal
- 9. Create a White List of web sites used in your business
- 10. Don't let anyone access their personal Social Media on your network!
- 11. Enable Multi-Factor Authentication on your personal email accounts
- 12. Conduct Background checks
- 13. Use secure messaging apps
- 14. Patch! Patch! Patch! All your systems!
- 15. Update older programs and Operating Systems! – *As of January 14, 2020, Microsoft no longer provides security updates or supports PCs running Windows 7!*
- 16. Update Printer Firmware and update older Printers!
- 17. Educate employees on their security responsibilities
- 18. Have a business continuity plan and test your backups!

Ok, so now that you have your Data Security House in order...

Components of a
Digital
Transaction:

19

Electronic Signature

a sound, symbol, or process
attached to or associated with
an electronic document



20

Hybrid Digital Close:

Hybrid Digital Closing
(In person)

All documents signed electronically, except for notarized documents.

The promissory note may or may not be created and signed digitally.



21

Full Digital Closing I

Electronic Notarization
In Person

All documents, including note and security instrument, are electronically created, signed, notarized (as required) and recorded



22

Electronic Notarization:

Notaries are able to electronically sign and seal documents with the signer and notary public physically present in the same location.



23

Full Digital Closing II

Remote Online Notarization
Audio/Video via webcam

All documents, including note and security instruments, are electronically created, signed, notarized (as required) and recorded



24



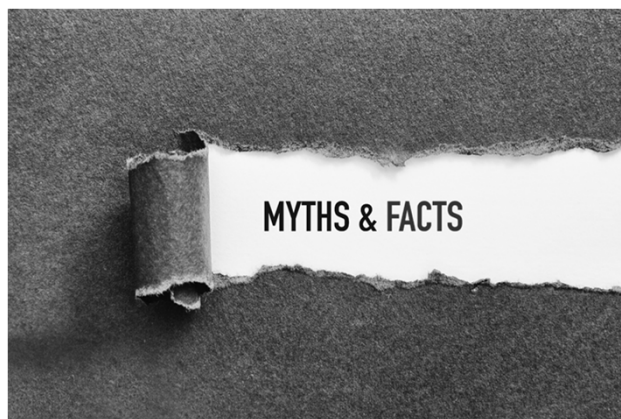
Remote Online Notarization: documents are notarized as the signer electronic appears before the notary using online audio-video technology.

25

Authentication for a RON transaction

Allows for review a state- or government-issued photo ID for visual validation while using software to provide the notary with assurance the ID is valid

Use of Dynamic versus Static Knowledge-Based Questions



26

Hello

my name is

Proven Method Authentication:

- What the signer possesses (i.e. driver's license, US passport)
- What the signer knows (knowledge-based authentication)
- Who the signer is (fingerprint recognition, eye scan)

27

Digital Closing: Work Process

If RON Notarization:

Closing is Scheduled with Signers and Notary via Audio/Video **Approved** Vendor

Signer passes Authentication to Sign Remotely: Government issued ID, KBA questions, Notary

Signer Electronically Signs the Documents

Notary Electronically Signs the Documents and affixes Electronic Notary Seal

28

What We've Learned So Far

Remote Online Notarization

- Thoroughly understand the law and the administrative rules before starting the process of offering online/Remote Online Notarization
- Online notarization preparedness can be a large investment
- Investigate and evaluate the costs of offering Online and/or Remote Online Notarization
 - Training
 - Technology Hardware
 - Technology Software
 - Ongoing support
- To help manage costs and keep per/transaction costs low
 - Do not use the “if we build it they will come” philosophy when starting out
 - Don't provide every existing Notary with online notarization capability at the beginning of the process
 - Try to forecast and anticipate online notarization volume and trends
- Once setup and trained, practice, practice, practice, prior to conducting first “live” online or RON transaction
- Stay informed of online notarization technology changes and introductions

29

Remote Online Notarization

- Identify customers who are good candidates for RON eligible for eNotary
 - Buy equipment:
 - Camera
 - Headset
 - Send a Practice link at least 48 hours in advance
 - Be prepared and know where you will store a copy of the video.
 - Partner with a great vendor
- Request lender instructions state “the documents “may” be electronically signed

30



31

How Agents Prepare for Digital Transformation in the Settlement Industry:

More than technology

Culture and teams that understand the Process, Technology

Ready to serve your customer's digital preferences



Blockchain

What is it?

- New network and database hybrid technology designed to support Bitcoin
- Ledger shared information without a 3rd party
- Immutable Record - data can never be changed
 - Prevents corrupt county governments from going back and deleting or changing land records
- Digital Hash of Documents
 - Digital Fingerprint / Tamper Seal for Documents & Data
 - Ensures Recorded Documents we never altered

33



Blockchain

Blockchain will support, not replace, title insurance according to a commentary published by A.M. Best.

- Here's the problem
- "In order to realize the value of the Blockchain, current title systems and land records will need to be converted into distributed ledger systems, the theme, 'garbage in, garbage out' is still valid, and any fraudulent or erroneous records would be transferred as such. The due diligence process would be as necessary as before."
- Equally important will be the dialogue with regulators and state and county officials as to the protection mechanisms and plans for dealing with privacy issues.
- GDPR - General Data Protection Regulation
- *And now... CALIFORNIA CONSUMER PRIVACY ACT (CCPA) - The CCPA applies to **any company that operates in California** and either makes at least \$25 million in annual revenue, gathers data on more than 50,000 users, or makes more than half its money off of user data. **The Consumer will be able to see what data companies have gathered about them, have that data deleted, and opt out of those companies selling it to third parties from now on.***

34

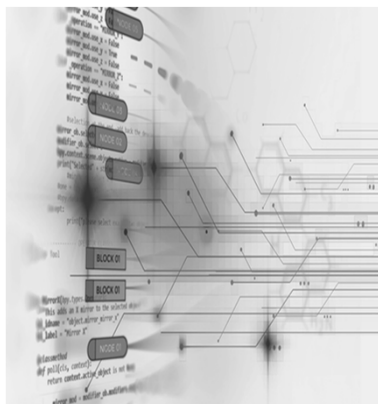
Title Policy vs. Blockchain

Cause of Claim	Title Insurance	Blockchain
Errors in Public Records	✓	X
Unknown Lien	✓	X
Illegal Deeds	✓	X
Missing Heirs	✓	X
Forgeries	✓	X
Undiscovered Encumbrances	✓	X
Unknown Easements	✓	X
Boundary / Survey Disputes	✓	X
Undiscovered Wills	✓	X
Corrupt Country Recorders	😬	X
Bribes to Change Country Data	😬	✓
Hacked Country Recorder Databases	😬	✓

35

Digital Definitions

Blockchain



• Technology Innovation fills gaps

- The Printing Press filled the Knowledge Gap
- Combustion Engine filled the Power Gap
- The Internet filled the Distance Gap
- Blockchain fills the Trust Gap
 - Today we use a Ledger, easy to add and easy to delete
- But does it really?

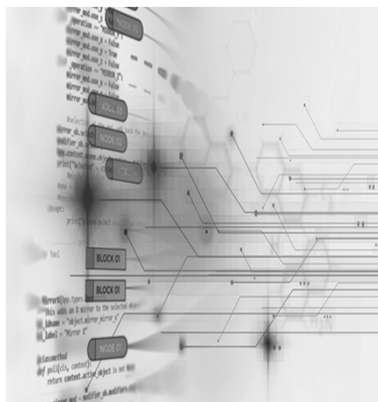
36

Blockchain



- **Trust is the fundamental Currency in Commerce**
- **Trust Gap is expanding**
- **In today's ledgers, 30% of all Titles have an error**
- **One record depends on all others before it with a Crypto Key**
- **A distributed ledger around the world**

Blockchain



- **Can you actually trust that the data in a**
- **Can you actually trust that the data in a BlockChain is true?**
- **Security is still an issue in this new technology**
- **Scalability is still an issue**
- **How do you go backwards?**
- **What about privacy?**
- **An important aspect of GDPR (General Data Protection Regulation) on Blockchain is the fact that personal data is not to leave the EU. This is a major problem with public Blockchains, since there is no control on who hosts a node**

Will it really change our industry today?

- Certainly not in the near term
- The technology is still extremely immature
- How do we know the information is actually true?
- Blockchain applications will have to be integrated to the current legacy systems. The cost of replacing current systems along with the disruption that a project like that would cause can be overwhelming for almost any company.
- Should you still pay attention?



Resources:

American Land Title Association

1800 M Street, NW, Suite 300S

Washington, D.C. 20036-5828

<https://www.alta.org>

Electronic Signature and Records Association

<https://esignrecords.org>

Mortgage Bankers Association

<https://www.mba.org>

41



2018 19,000
eNotes for the
entire year

Q1 of 2019, 17,000
eNotes were
recorded

42

Digital Closing: Work Process



43

Digital Closing Work Process

If Hybrid Digital Closing:

Documents are
Electronically
Signed; Documents are
also Printed and
Traditionally Signed/
Notarized

Signer Electronically
Signs Documents

Signer Traditionally
Signs Printed
Documents

Notary Traditionally
Signs/Notarizes
Printed Documents

44