American Land Title Association
Protect your property rights

ALTA inSIGHTS

REAL TIME | ON-DEMAND

Develop a Cybersecurity Risk Management Plan

Today's ALTA Insights Featured Sponsor

Speakers

- **Moderator - Linda Grahovec**
  SVP, Director of Education & Marketing | FNF Family of Companies

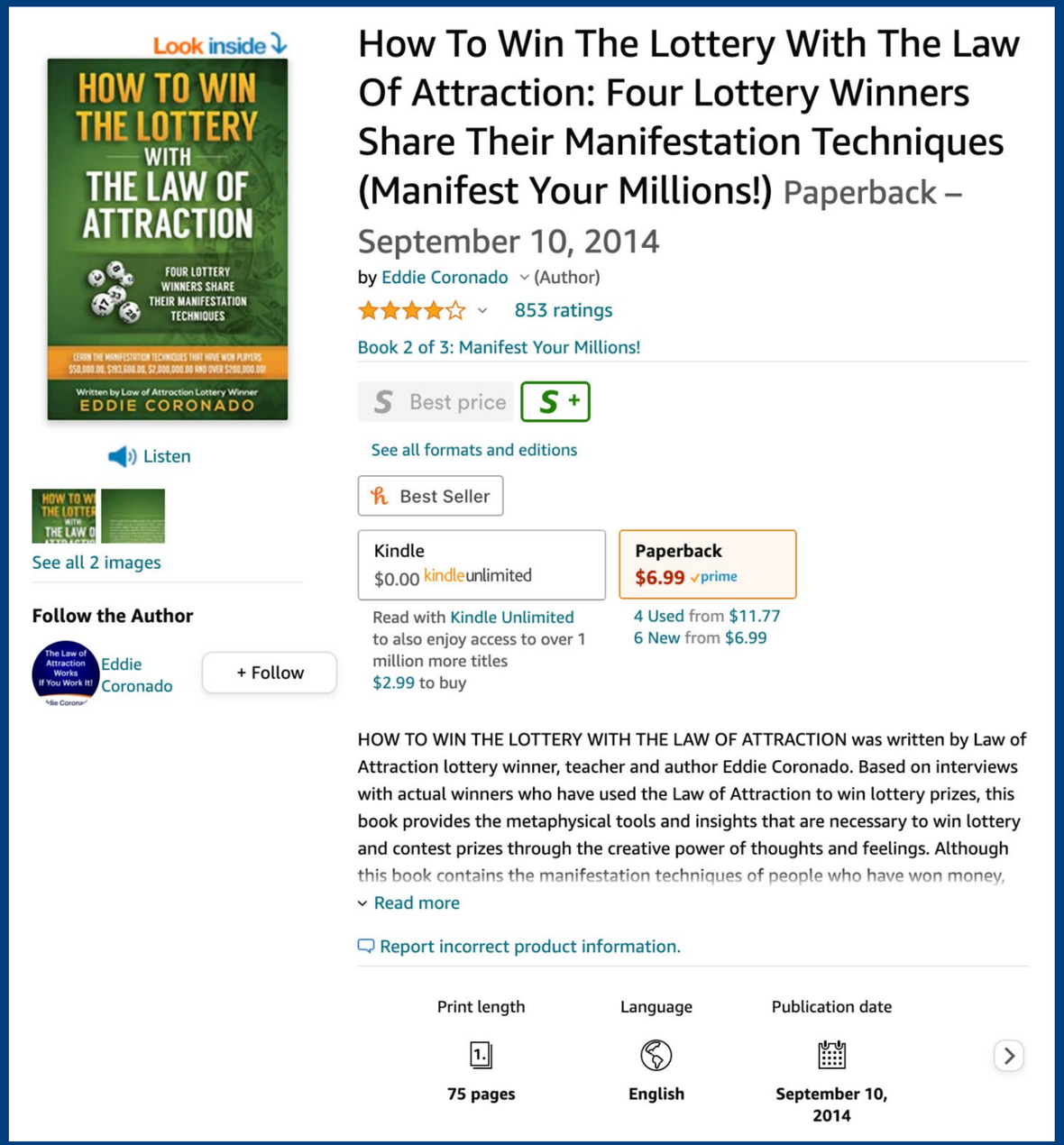
- **Presenter - Andy White, Ph.D.**
  Chief Executive Officer | Closinglock

- **Presenter – Brian Freedman**
  Global Manager Solutions Engineering | QOMPLX Inc.

Closinglock

QOMPLX:

Develop a Cybersecurity Risk Management Plan



Silver Bullet Solution

Four Lottery Winners Share Their Manifestation Techniques (Manifest Your Millions!)

HOW TO WIN THE LOTTERY WITH THE LAW OF ATTRACTION was written by Law of Attraction lottery winner, teacher and author Eddie Coronado. Based on interviews with actual winners who have used the Law of Attraction to win lottery prizes, this book provides the metaphysical tools and insights that are necessary to win lottery and contest prizes through the creative power of thoughts and feelings.

Outline

- Cybersecurity Statistics
- Tangible Risk Mitigation
- ALTA resources
  - Incident Response Plan Template
  - Employee Training
  - What You Can Do Today

Cybersecurity Statistics

Cyber Losses Mount

- **Cyber attacks are escalating**
  Attackers often go undetected with forged and falsified authentication to compromise identity and their key target is Identity such as Active Directory
- **Service disruptions are mounting**
  Ransomware groups and breaches are impacting reliable service delivery
- **Targeting financial flows**
  Growing focus on real-estate and title given the large amounts of money moving and frequent changes in counterparties

Rising cyber attacks leave more victims in their wake

- Attackers go undetected with forged and falsified authentication which serves to compromise identity and target active directory which can lead to breaches, ransomware, and loss of control.

85% CYBER BREACHES TARGET ACTIVE DIRECTORY

Attack Name | Cyber Gang | Victim

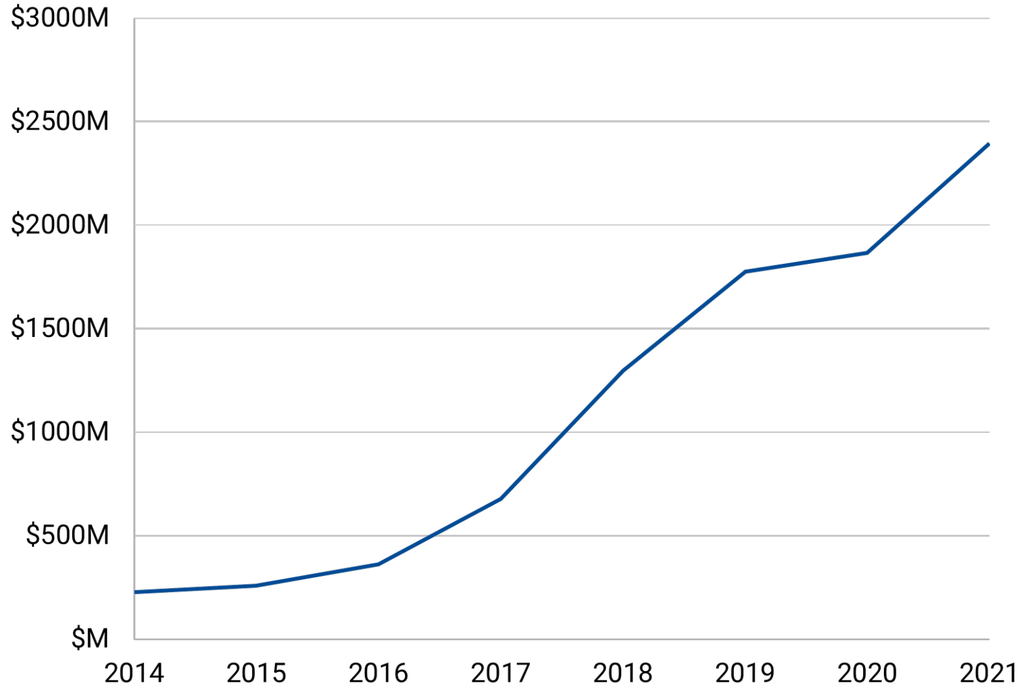
Cybersecurity Statistics

$6,000,000,000+
Lost in US to BEC/EAC from Jan 2019 to Dec 2021

$2,235,000
Average cost of cyber attacks on small and medium-sized businesses

$120,000
Average loss per business email compromise event

Business Email Compromise Losses



Cybersecurity Statistics

$6.9 billion lost to cybercrime in 2021

In 2021, a cybercrime was reported every 37 seconds

58% of malware attack victims are small businesses

1 in 13 web requests lead to malware

Email is the primary conduit

35% of cybercrime losses as a result of Business Email Compromise

92.4% of malware is delivered via email

34% increase in phishing attacks from 2020 to 2021

Real estate transactions are complex and risky.

Fragmented Communications

The real estate industry still relies on email, phone, mail, and fax for exchanging transaction documents and payment information

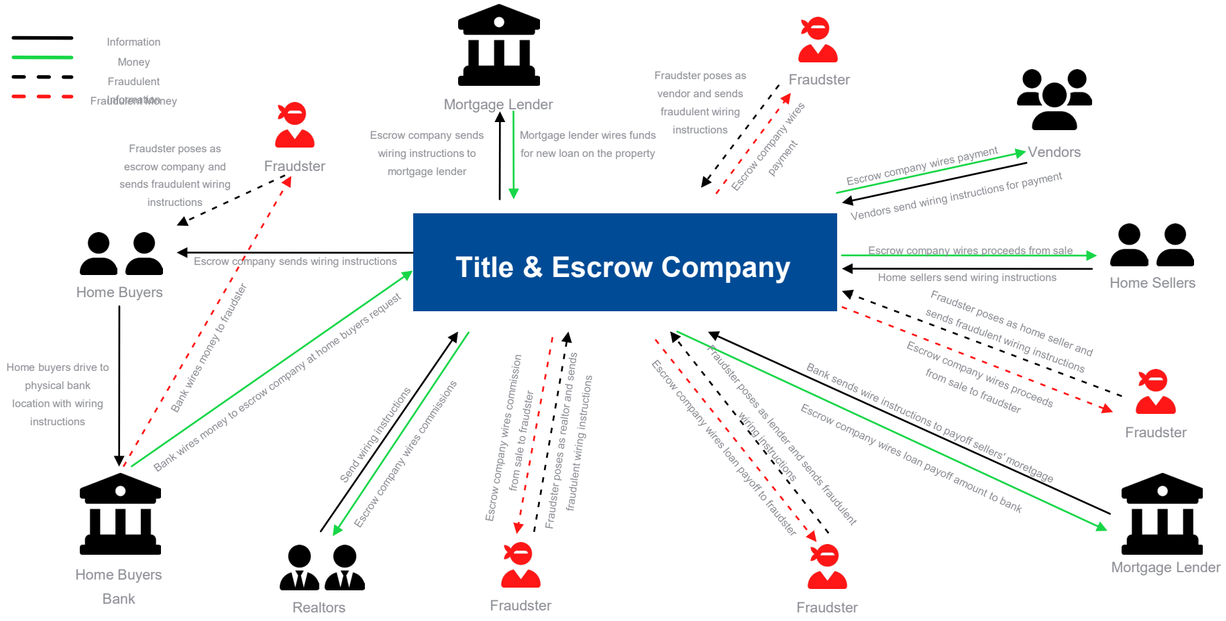
Complicated Flow of Funds

Each real estate transaction requires multiple incoming and outgoing payments, with different parties on every transaction

Growing Fraud Risk

$350M+ in reported annual real estate wire fraud losses, with $2B+ estimated as lost

Flow of Funds in Real Estate Transactions



FRAUD DATA FROM 2021 FBI IC3 REPORT, AMERICAN LAND TITLE ASSOCIATION

Tangible
Risk Mitigation

Don’t be the slowest kid when the bear comes to camp

1. Use multi-factor authentication
2. Do not reuse passwords
3. Use a password keeper / password generator app
4. Change the default credentials on all software and devices
5. Update software regularly
6. Keep a consistent backup schedule and maintain offline backups
7. Manage your vendors and business partners to make sure they are doing what you are doing to protect your environment
8. Turn the firewall ON for all user devices
9. Use antivirus software on all devices
10. Don’t click on anything unsolicited in an email or text
11. Set up an out-of-band protocol for wires and make everyone adhere to it
12. Have a computer dedicated for accessing your banking/escrow account(s). Do not use this computer for anything else (e.g. social or email)
13. Use email services that provide phishing and pretexting defenses
14. Use a web browser that warns you when a website may be spoofed. Stop using Internet Explorer!

Protect Your Connection

PROBLEM

Public WiFi is shared

Viruses / malware are communicable

SOLUTIONS

VPN

PrivateTunnel NordVPN®

Tethering

COST

$6 per month for VPN

Free for tethering*

Update Your Software

PROBLEM

Software is developed by people

SOLUTIONS

Patch / update regularly

COST

Free

Password Managers

PROBLEM

Same password

Shared passwords

Weak passwords

SOLUTIONS

Password manager

Unique passwords on every site

Allows family sharing

COST

Free - $5/month

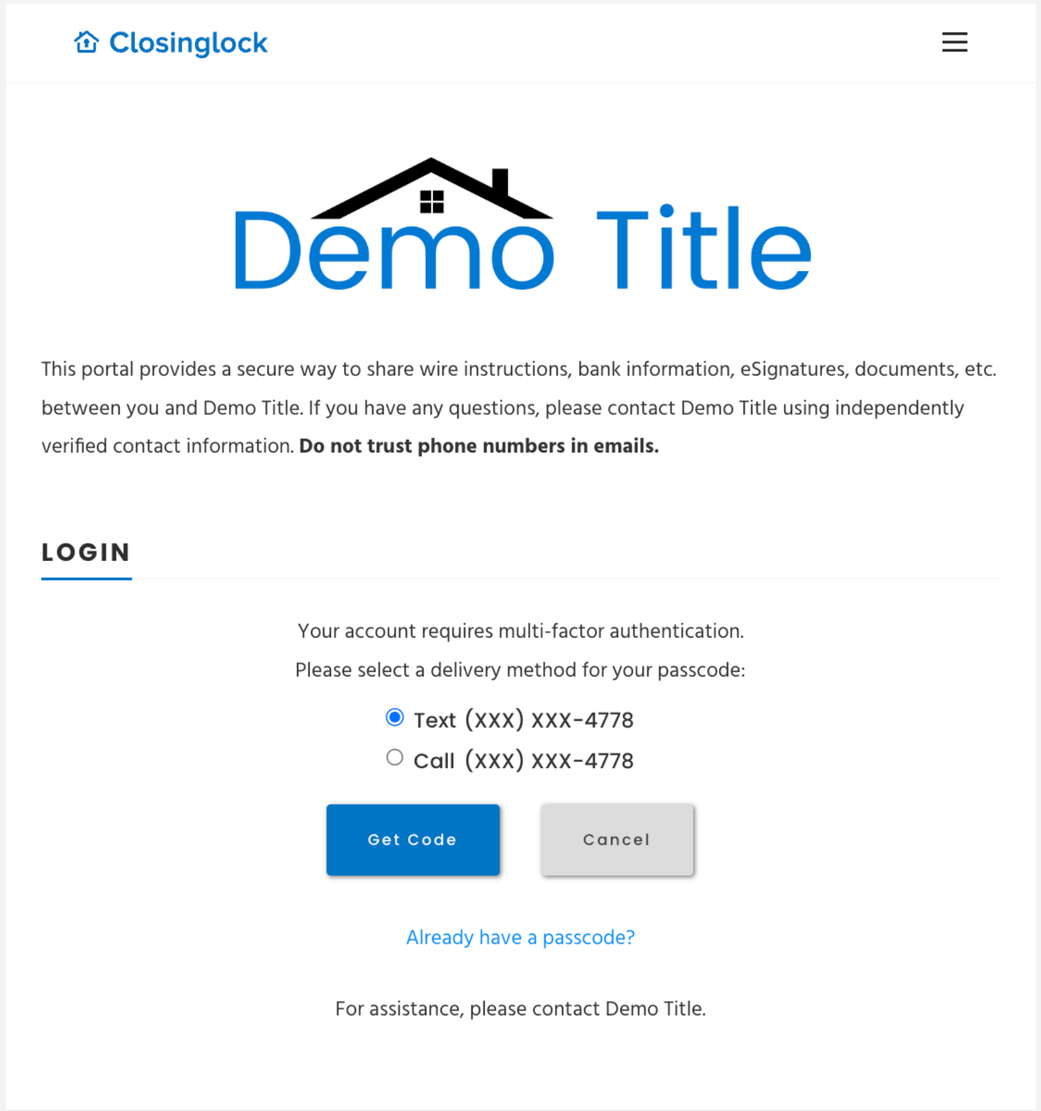
LastPass •••|

1Password

Multi-Factor Authentication (MFA)

Passwords are weak. Multi-factor authentication (2+) allows:

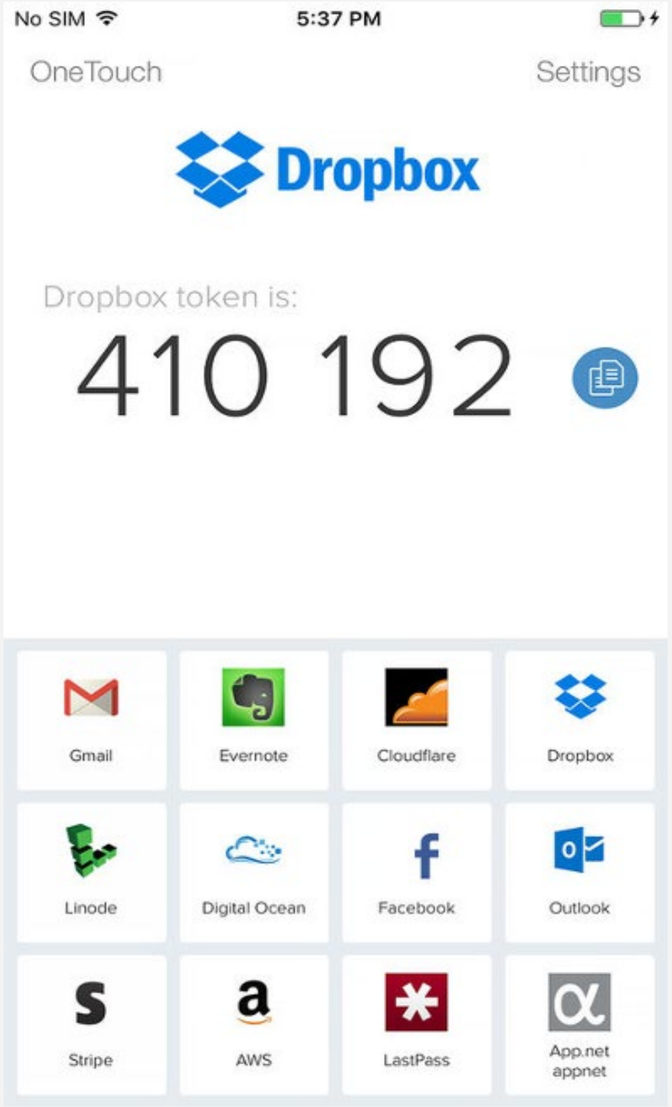
- Knowledge
- Possession
- Inherence



Two-Factor Authentication (2FA)

Password + text message

Cost: FREE



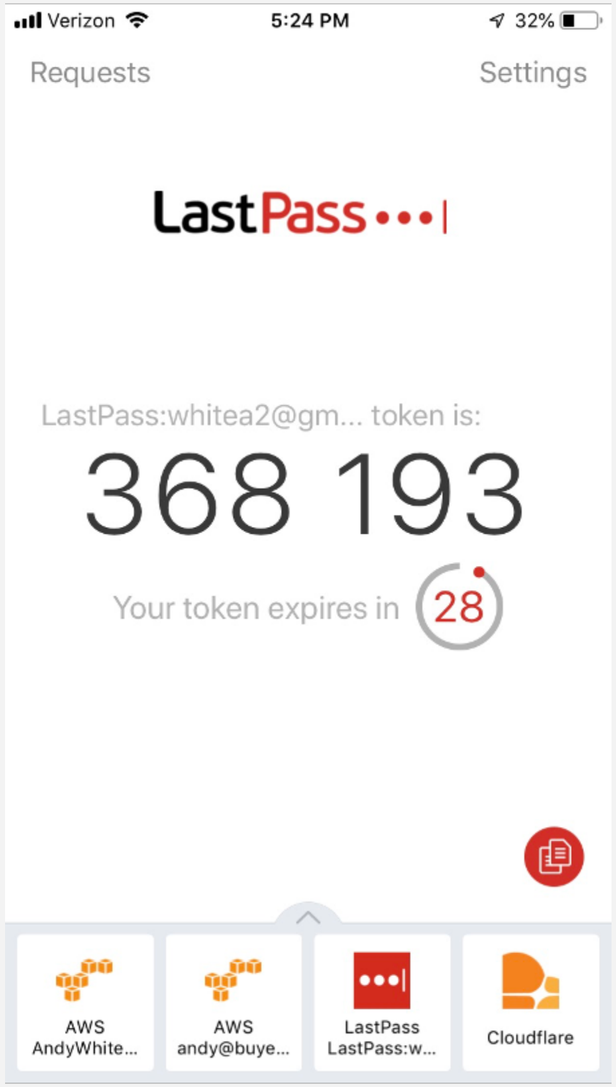
Two-Factor Authentication (2FA)

Password + software token

Make sure you have backup access!

Cost: FREE

AUTHY



Layering

PROBLEM

No one-size fits all solution

SOLUTION

Layer individual solutions

- Secure your connection
- Update
- Password manager + 2FA

Cost: FREE

Q:SCAN

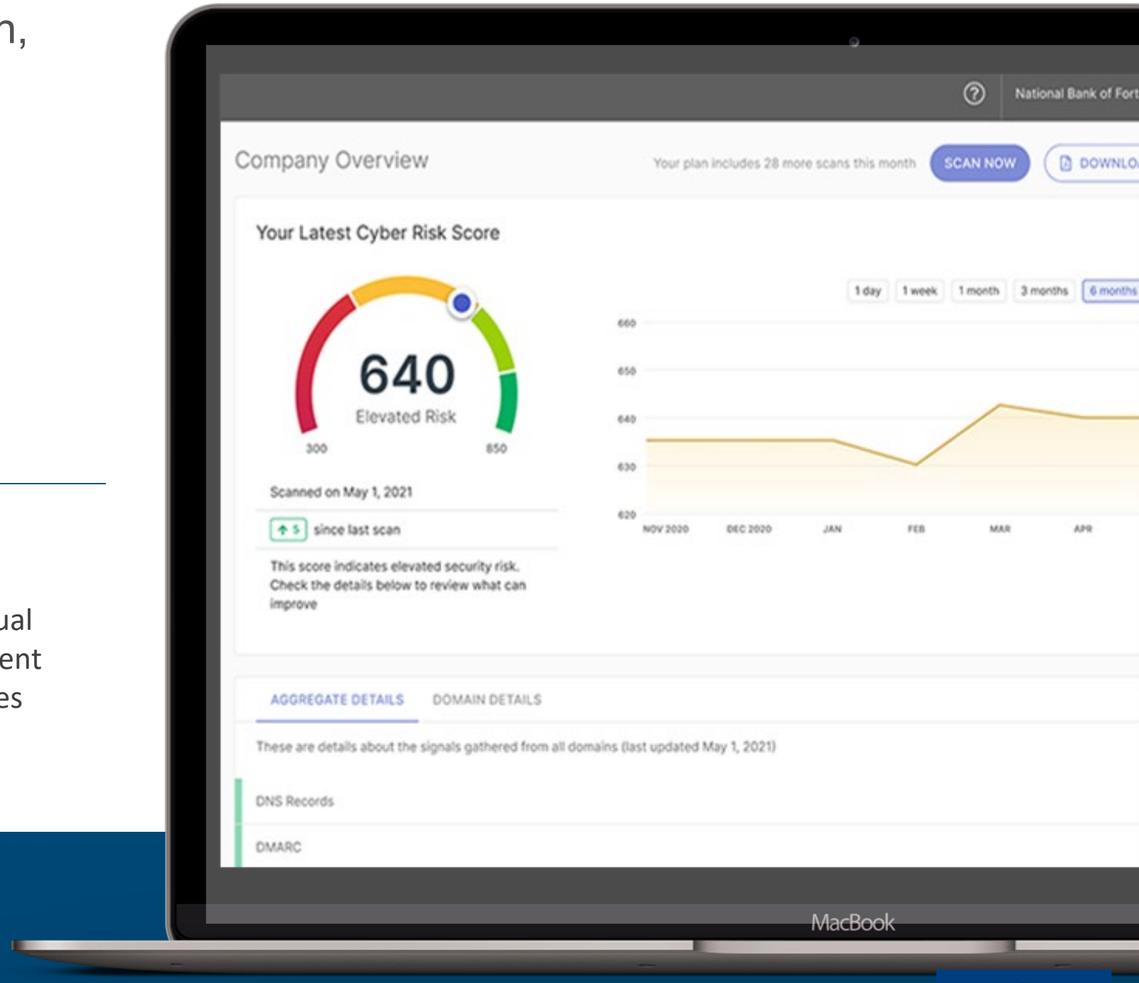
•Q:SCAN is a cloud-based, scalable platform that identifies customers' key security exposures. It can be used standalone for risk identification, or it can complement existing vulnerability scanning efforts.

KEY FEATURES

- Credit-score style enterprise cyber risk scoring and threshold monitoring
- Risk score trend reporting for ongoing risk analysis
- Domain level signal details
- Risk exposure alerts including breach data citations, observed malware DBs, externally visible vulnerabilities and exposed ports

SIGNALS COLLECTED

- Domains
- Sub domains
- DNS records
- DMARC
- SPF
- Zone transfers
- Open ports
- Exposed services
- Web application headers
- Breached email addresses
- TLS certificate health
- Malware indicators
- Contextual enrichment databases



Q:SCAN uses open-source intelligence techniques to identify customers' and suppliers' external attack surfaces

vCISO – Phone a Security Friend

vCISO (fractional virtual CISO)

Advisory Services (vCISO)

- A named Security Advisor will work in concert with the customer to help establish and maintain the customer's security vision, strategy, and programs.
- QOMPLX will provide expert guidance by understanding the customer's goals and business environment, anticipating future security and compliance challenges, and working with IT and Security teams to identify current security risks to the business-critical systems.
- Senior consultants advise the CIO, management team, and board to build security program strategies, prioritize areas for investment or uplift, perform due diligence, or sustain appropriate security capabilities.

vCISO + Q:SCAN (+Insights) ...become boring to a hacker or fraudster

vCISO + QSCAN

- vCISO - Same as above
- Analyst insights w/ attack surface reduction (how does your company look to a hacker)

QOMPLX
MDR capabilities

Detection

- Intelligence-fed threat hunting
- Custom detection rules
- Data source ingestion
- Enriched alerting
- QOMPLX Managed Assurance

Response

- Validation and notification
- Remote response
- Containment and remediation actions
- Incident response experts'

Reporting

- Metric-driven dashboard
- Attack surface monitoring
- Security Improvement and resilience
- Recommendations
- Intelligence and threat advisories
- Custom reporting per incident

Collaboration

- Phone/Slack/email
- Visibility Custom incident response plans
- Extended team

Investigation

- Correlated analysis
- Alert prioritisation
- Detailed results

ALTA Resources

Topics

https://www.alta.org/business-tools/information-security.cfm

- Incident Response Plan Template
- Employee Training
- Wire Fraud

Incident Response Plan Template

ALTA Cybersecurity Incident Response Plan

- Make a list of Systems (software vendors, where is data, computers, mobile devices)
- Identify IT Personnel - who is in charge of what computer systems?
- Business Impact Analysis / BCP
- Review Cyber Coverage
- Breach Notification and Reporting Requirements
- Disaster Recovery Plan
- Roles & Responsibilities
- Crisis Communication Plan

Employee Training and Awareness

- QOMPLX, PhishMe, KnowBe4, etc.
- Webinars
- Educational Opportunities

Wire Fraud

- ALTA
  - Outgoing Wire Preparation Checklist
  - Rapid Response Plan and Worksheet
  - Report to FBI (IC3 Report)
  - Videos & infographics
- Silver Bullet: stop emailing/texting wire instructions
- Payoff fraud

Wire Fraud Statistics

$2.4B

20K BEC/EAC Complaints with Reported Losses

$350M

Reported Lost From Consumers in Real Estate

15%

FBI Estimate of Losses that are Reported

FBI ESTIMATES 10-15% OF LOSSES ARE REPORTED.

$245

Average amount lost to wire fraud per real estate transaction

FRAUD DATA FROM 2021 FBI IC3 REPORT, AMERICAN LAND TITLE ASSOCIATION

PAYOFF FRAUD

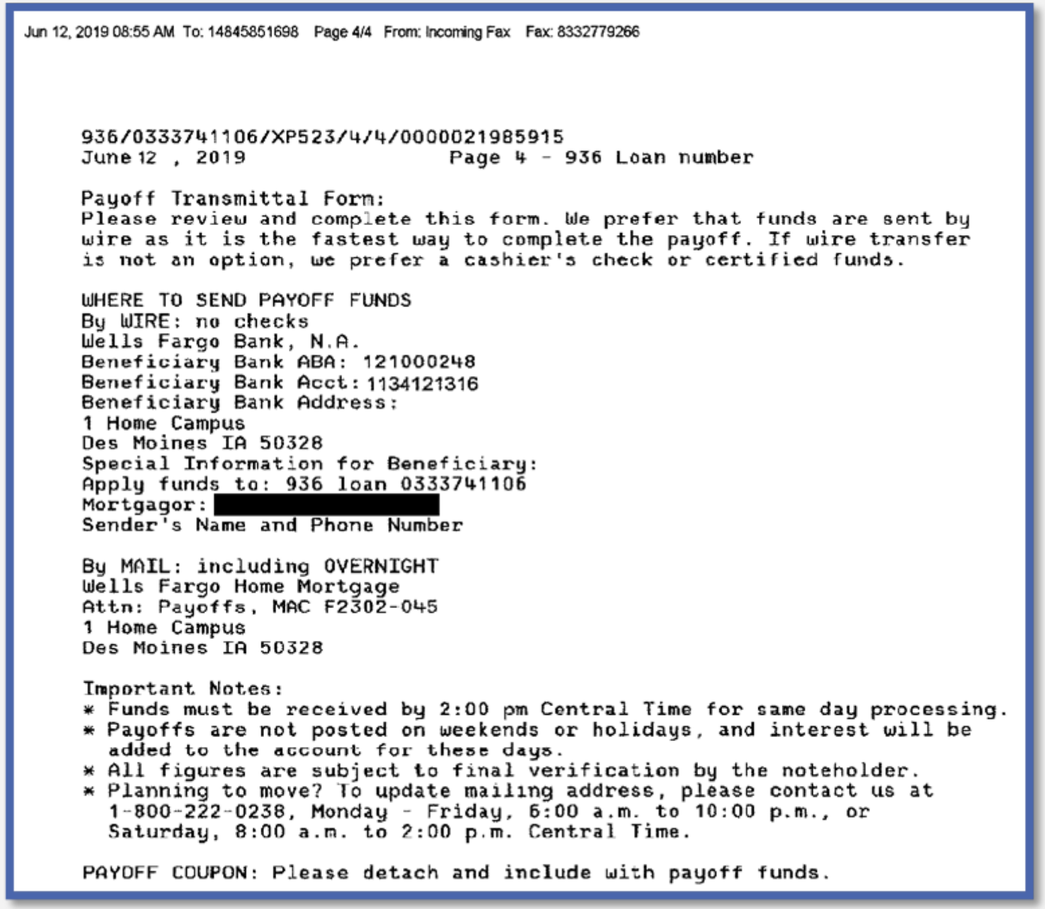
Problem

What

Fraudster tricks escrow company into wiring mortgage payoff funds

How

- Request payoff quote
- Insert fraudster’s account number
- Send encrypted email and secure fax to escrow company
- Send follow up from Realtor
- Profit



Jun 12, 2019 08:55 AM To: 14845851698 Page 4/4 From: Incoming Fax Fax: 8332779266

936/0333741106/XP523/4/4/0000021985915
June 12 , 2019 Page 4 - 936 Loan number

Payoff Transmittal Form:
Please review and complete this form. We prefer that funds are sent by wire as it is the fastest way to complete the payoff. If wire transfer is not an option, we prefer a cashier's check or certified funds.

WHERE TO SEND PAYOFF FUNDS
By WIRE: no checks
Wells Fargo Bank, N.A.
Beneficiary Bank ABA: 121000248
Beneficiary Bank Acct: 1134121316
Beneficiary Bank Address:
1 Home Campus
Des Moines IA 50328
Special Information for Beneficiary:
Apply funds to: 936 loan 0333741106
Mortgagor: [redacted]
Sender's Name and Phone Number

By MAIL: including OVERNIGHT
Wells Fargo Home Mortgage
Attn: Payoffs, MAC F2302-045
1 Home Campus
Des Moines IA 50328

Important Notes:
* Funds must be received by 2:00 pm Central Time for same day processing.
* Payoffs are not posted on weekends or holidays, and interest will be added to the account for these days.
* All figures are subject to final verification by the noteholder.
* Planning to move? To update mailing address, please contact us at 1-800-222-0238, Monday - Friday, 6:00 a.m. to 10:00 p.m., or Saturday, 8:00 a.m. to 2:00 p.m. Central Time.

PAYOFF COUPON: Please detach and include with payoff funds.

PAYOFF FRAUD

Solutions

~~Ignore it~~

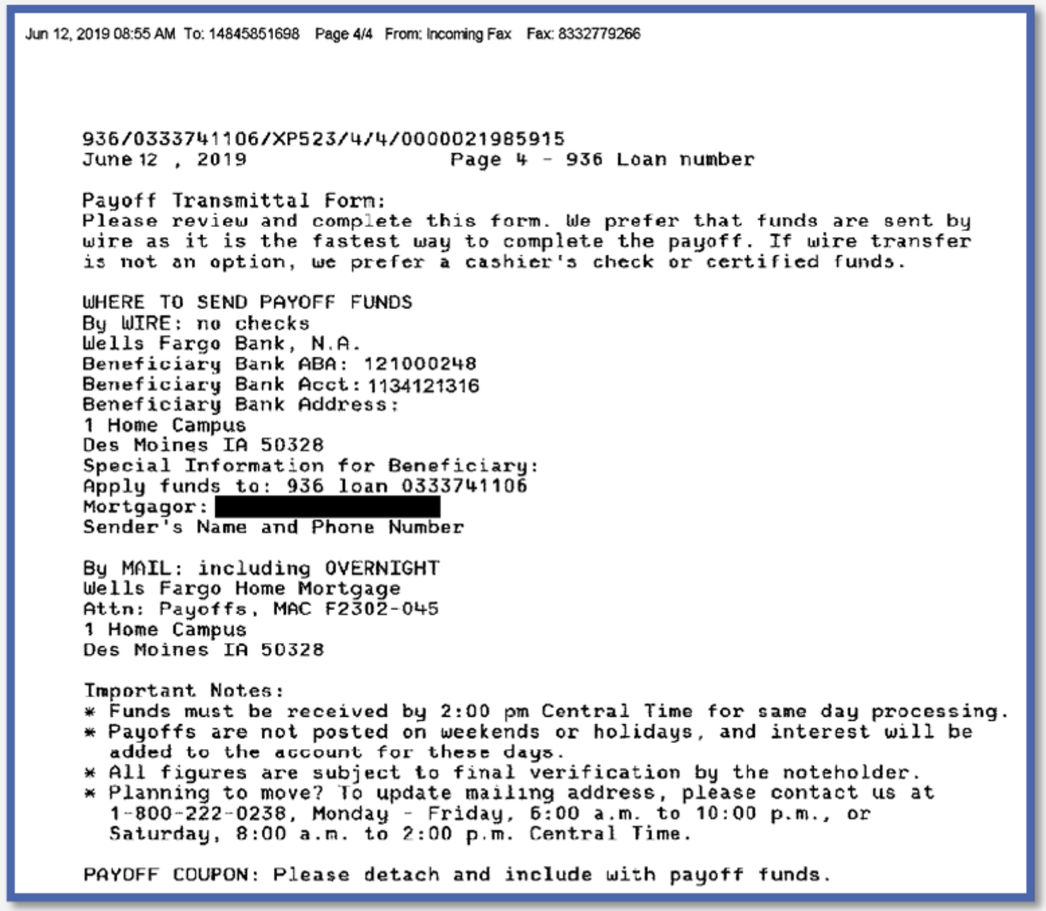
Call bank every time

Use a verified number

Maintain a list of valid payoffs

- Lock it down!
- Handle dynamic accounts

Use a payoff verification service



Jun 12, 2019 08:55 AM To: 14845851698 Page 4/4 From: Incoming Fax Fax: 8332779266

936/0333741106/XP523/4/4/0000021985915
June 12 , 2019 Page 4 - 936 Loan number

Payoff Transmittal Form:
Please review and complete this form. We prefer that funds are sent by wire as it is the fastest way to complete the payoff. If wire transfer is not an option, we prefer a cashier's check or certified funds.

WHERE TO SEND PAYOFF FUNDS
By WIRE: no checks
Wells Fargo Bank, N.A.
Beneficiary Bank ABA: 121000248
Beneficiary Bank Acct: 1134121316
Beneficiary Bank Address:
1 Home Campus
Des Moines IA 50328
Special Information for Beneficiary:
Apply funds to: 936 loan 0333741106
Mortgagor: [redacted]
Sender's Name and Phone Number

By MAIL: including OVERNIGHT
Wells Fargo Home Mortgage
Attn: Payoffs, MAC F2302-045
1 Home Campus
Des Moines IA 50328

Important Notes:
* Funds must be received by 2:00 pm Central Time for same day processing.
* Payoffs are not posted on weekends or holidays, and interest will be added to the account for these days.
* All figures are subject to final verification by the noteholder.
* Planning to move? To update mailing address, please contact us at 1-800-222-0238, Monday - Friday, 6:00 a.m. to 10:00 p.m., or Saturday, 8:00 a.m. to 2:00 p.m. Central Time.

PAYOFF COUPON: Please detach and include with payoff funds.

Wire Fraud Response Plan

Inspect links before clicking

- ALTA Response Plan
- ALTA Response Worksheet

Contact FBI's Internet Crime Complaint Center

- 10-15% is reported
- FBI's Financial Fraud Kill Chain, Recovery Assets Team
  82% success rate in 2020 …
  of 11% of the losses = ???
- File Complaint

Ensure the documented plan is comprehensive

Inbound, outbound, payoff

Wire fraud solution.

INBOUND | OUTBOUND | PAYOFF

Trusted by thousands of title professionals

Protected $100B+ from wire fraud

Closinglock

closinglock.com

How to stop Ransomware and the disruption of services

Ransomware and forged identity

- In the case of the Colonial pipeline cyber attack, a compromised password was the entryway to the legacy VPN from which lateral movement and privilege escalation ultimately took place(1)
- The most devastating ransomware attacks often rely on forged and falsified authentication. Attackers take over the core authentication services and gain control
- Identity forgeries (on premise and in the cloud) provide unfettered access and unlimited time to find, exploit and take control of critical infrastructure… then move to demand ransom, steal information, or abuse payments/accesses

The QOMPLX solution is core to stopping it

- ‘Highly sophisticated’ ransomware attack sidelines Cloudstar(1)
- QOMPLX:CYBER solutions include capabilities to analyze vulnerabilities and assure identity as well as detect and mitigate breaches
- Global ransomware damage costs predicted to exceed $265 billion by 2031(2)
- Q:CYBER solutions are critical in the fight to stop attackers before ransomware can impact a target’s network

(1) The Title Report, Highly sophisticated’ ransomware attack sidelines Cloudstar, July 21, 2021.
(2) Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Exceed $265 Billion By 2031, June 3,2021

QOMPLX
MDR capabilities

Detection

- Intelligence-fed threat hunting
- Custom detection rules
- Data source ingestion
- Enriched alerting
- QOMPLX Managed Assurance

Response

- Validation and notification
- Remote response
- Containment and remediation actions
- Incident response experts'

Reporting

- Metric-driven dashboard
- Attack surface monitoring
- Security Improvement and resilience
- Recommendations
- Intelligence and threat advisories
- Custom reporting per incident

Collaboration

- Phone/Slack/email
- Visibility Custom incident response plans
- Extended team

Investigation

- Correlated analysis
- Alert prioritisation
- Detailed results

Client case study

CHALLENGE

60% of businesses that suffer a data breach close within six months. Why? The cost to repair the breach plus the loss in customers is catastrophic.

One QOMPLX client, a North American-based manufacturer, knew it needed to avoid such a disaster.

- The client worried that unauthorized access to user information might negatively affect its reputation
- The client was concerned about ransomware attacks and data leaks
- The client had limited IT resources

With a small IT staff and significant IT assets to secure, one North American beverage manufacturer knew they'd need a cybersecurity solution that would Increase their defenses without driving up costs.

For less than the cost of one full time cybersecurity employee, QOMPLX watches 24x7 for any signs of malicious activity across the client's entire identity infrastructure.

SOLUTION

To keep their cyber risks well-controlled, QOMPLX engaged with the client in a multi-year program in three phases:

Critical infrastructure protection

The client deployed QOMPLX Identity Assurance software to map their entire on-prem and cloud-identity environment (including hundreds of Domain Controllers), validate all authentication traffic, and protect against loading attack techniques.

Managed detection and response services

The client used QOMPLX MD) software-as-a-service to ingest, parse, normalize, monitor, and correlate logs source and security tools to detect cyber threats in real-time.

Acquisition diligence

The client retained QOMPLX Special Solutions Advisory team to perform pre-acquisition assessments on three targets, producing three "red flags letters that identified key weaknesses and recommended strategic uplift initiatives.

Additional Free Resources

https://nationalagency.fnf.com/FNF-Guidance/Risk-Management

2022 Cybersecurity Awareness Month

Wire (Diversion) Fraud

Mortgage Payoff Fraud

Cybersecurity Resources

FNF FAMILY OF COMPANIES

American Land Title Association
Protect your property rights

Q&A

FNF FAMILY OF COMPANIES

Contact Us

Linda Grahovec | FNF Family of Companies
linda.grahovec@fnf.com | Phone 630-222-0778

Adam Lampl | Closinglock
adam@closinglock.com | Phone 512-434-0075

Jason Kirkland | QOMPLX
jason.kirkland@qomplx.com | Phone 214-906-4778

American Land Title Association
Protect your property rights

FNF FAMILY OF COMPANIES