A Fund Roundtable:

Cyber-Hygiene Tips You Need to Adopt Today

Presented By:
Michael Rothman, Esq.
Linda Monaco, Esq.
Robert Rohan, Esq.
John St. Lawrence, Esq.

The Fund ALWAYS DRIVEN

1

October is National Cyber Security Awareness Month

Fund live programming:

- **Tues., Oct. 15 @ noon** – *Third Party Security Vetting for Law Firms,* presented by Ron Frechette of Goldsky Security
- **Tues., Oct. 29 @ noon** – *Computer Security in the Age of Computer Crime*, presented by The Fund's Darrell Marsh

Fund Website:

- www.thefund.com/information-center/information-security.aspx

The Fund ALWAYS DRIVEN

2

Topics of Discussion

- Litigation Exposure (Michael Rothman)
- Passwords (Linda Monaco)
- Website Management (Robert Rohan)
- Deterrence (Robert Rohan)
- Red Flags/ Servers/ Software (John St. Lawrence)
- Insurance Considerations (Michael Rothman)
- Wire Transfer (Linda Monaco)
- Staff Development (Robert Rohan)

The Fund ALWAYS DRIVEN

3

Litigation Exposure

The Fund ALWAYS DRIVEN

4

Litigation Exposure

- Consider investing in a Security Risk Assessment
  - But ensure that all office practices recommended by the SRA are followed
    - Same holds for adherence to your firm's Best Practices Manual
    - GoldSkySecurity.com
    - KnowBe4.com

The Fund ALWAYS DRIVEN

5

Litigation Exposure

- Avoid making statements on your website or social media about your firm's "security," "trust," "experience," etc.

The Fund ALWAYS DRIVEN

6

Litigation Exposure

- Understand the obligations imposed by FIPA, Sec. 501.171, F.S. (Florida Information Protection Act of 2014)
  - Required notice to affected persons for data breach
  - Move closed files containing private data off your server

The Fund ALWAYS DRIVEN

7

Litigation Exposure

- Did you obtain a signed Acknowledgement from the parties of your warning about wire fraud and your office practices?

The Fund ALWAYS DRIVEN

8

Litigation Exposure

- Are you taking commercially reasonable care
  - in controlling, securing and disbursing client funds?
  - in the manner by which you inform clients of the expected closing procedure, such as when and how to wire closing funds?
  - in safekeeping client NPI?

The Fund ALWAYS DRIVEN

9

Litigation Exposure

- Does your firm have a written Incident Response Policy to identify, report and cure any breach of data or loss of funds via wire transfer?
  - Know who to call! Your bank's Chief of Security – not the branch manager or your account manager

The Fund ALWAYS DRIVEN

10

Passwords

Passwords – Facts

- Most common passwords: Password or 123456
  - Easy to remember
- Easy to hack
  - Easy passwords – 111111
  - Passwords that relate to your life – Monaco1982
  - Posted passwords are available to everyone
  - Identical passwords
- Hard passwords hard to remember
- Passwords you cannot remember are useless

Passwords – Unique to each site

- If your common password is discovered
  - Will have access to all accounts which use that password

Passwords – Change Often . . . or Not

- Old rule – change often
  - Led to issues, writing & posting, easy, re-used, month & date
- New rule – have stronger passwords & less changes
  - More compliance
  - Long passwords are strong passwords

The Fund ALWAYS DRIVEN

13

Passwords – Use a Strong Password

- 12 characters minimum – the longer the better
- Mix it up – letters, numbers, symbols, uppercase, lowercase
- Don't use dictionary word or combination

Too Simple	Better
H0use	BigHouse$123
Cat in the Hat	Correct horse battery staple
My beautiful red house	Seashell glaring molasses invisible

- www.Diceware.com provides list of words
  - Roll your dice and create your passphrase

14

Password Manager

- Encrypted vault for login credentials
  - May also save
    - Notes
    - Insurance cards
    - Credit card information
- Issue security alerts
- Generate passwords
- Streamlines logins
- Break bad habits
  - Unique passwords
  - Change passwords

The Fund ALWAYS DRIVEN

15

Password Managers

- LastPass
- Dashlane
- 1Password
- Keeper
- Sticky password
- Intel's True Key
- RoboForm
- Iolo Technologies
- EveryKey
- My PassLock

Remember there is NO FREE LUNCH!

The Fund ALWAYS DRIVEN

16

Password Managers

- Demonstration

Remember there is NO FREE LUNCH!

The Fund ALWAYS DRIVEN

17

Password Generator

- Random password generators
- Random may not be random
  - Based on an algorithm
  - Better if based on a random factor – key strokes
- Long passwords are strong passwords

Remember there is NO FREE LUNCH!

18

Password Multipart Authentication Your Best Friend

- Process – How to know it's really you
- Five common authentication factors
  - 1 Something you know
    - Password, address, other names, first car, etc.
  - 2 Something you have
    - Site sends a code or token which expires within a short time
  - 3 Something you are
    - Fingerprint, retina, iris, voice, fact, etc.
  - 4 Somewhere you are
    - IP address – it knows your computer
  - 5 Something you do
    - Gestures or touches

The Fund ALWAYS DRIVEN

19

Passwords – Tips

- **LONG PASSWORDS ARE STRONG PASSWORDS**
- Use unique password for each site
- Use password manager
- Change your password regularly, or
  - Indication that you have been hacked
- Use multi-factor authentication
  - Just turn it ON
- Don't use obvious personal information
- Don't re-use passwords
- Don't share your passwords – with ANYONE
  - Don't post your passwords

The Fund ALWAYS DRIVEN

20

Website Management

A valuable tool for promoting your business should not be a resource mined by bad actors

The Fund ALWAYS DRIVEN

21

Website Management

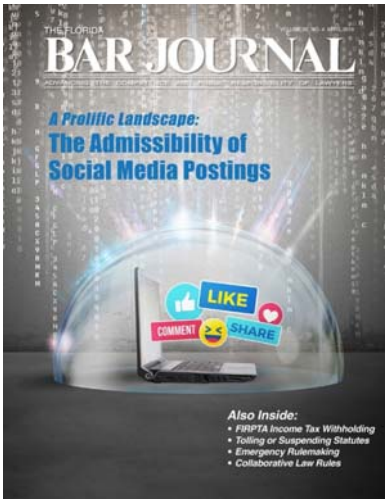
- Restrict company website content
  - Job descriptions
  - Internal phone directory

The Fund ALWAYS DRIVEN

22

Website Management

- Restrict company website content
  - Florida Bar
    - Quick Reference Checklist – Websites
    - Required Content (Rule 4-7.12)
    - Presumptively Valid Content (Rule 4-7.16)



The Fund ALWAYS DRIVEN

23

Website Management

- Restrict social media content
  - Personal v. business web pages
  - TMI (too much information)
    - Vacations
    - Business travel
    - Out of office details

The Fund ALWAYS DRIVEN

24

Deterrence

Shortcuts to accessibility create opportunities for good and bad alike

The Fund ALWAYS DRIVEN

25

Deterrence

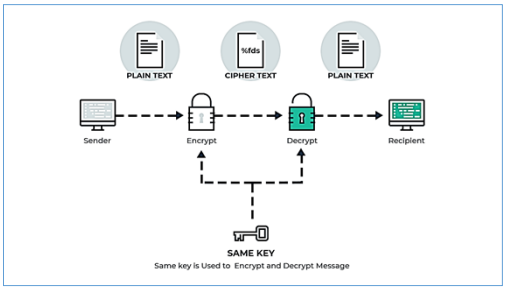
- Multi-factor authentication
  - a security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction

The Fund ALWAYS DRIVEN

26

Deterrence

- Encryption
  - the process of converting sensitive data or information into unintelligible data



The Fund ALWAYS DRIVEN

27

Red Flags / Server / Software

The Fund ALWAYS DRIVEN

28

Red Flags

"Phishing"

- Email seeks access to system by enticing user to "click" attachment or link to malicious site
- Now sophisticated; targeted to real estate professionals
- Forged messages appear to be from legitimate, real estate-related sources
  - "DocuSign"
  - "Dropbox"
  - "Real" underwriters, banks, title companies
  - Letterhead/signature blocks of actual parties reproduced
- Once "clicked," malware infects system; also "SPAMs" user contact list
- Once system infected, intruder can read/alter/redirect messages to defraud parties

The Fund ALWAYS DRIVEN

29

Red Flags

- Spoofed email addresses
  - Ex) rexrealtor@rexyourhome.com becomes
    - rexrealtor1a@rexyourhome.com
    - rexrealtor@rexy0urhome.com
- Spoofed domain addresses
  - Ex) upper-case domains
    - rexrealtor@REXYOURHOME.COM

- WARNING: Attacks can also come from a genuine email address if sender compromised
- Best Practice – Never open an attachment or link from an unverified source

The Fund ALWAYS DRIVEN

30

Red Flags

Preliminary CD and Contract

Kathy Hale <julia.beems@ucdenver.edu>

Sent: Thu 12/8/2016 8:57 AM

To: Renee Realtor, Tom Title Agent

Message | Preliminary CD.htm (12 KB)

Good Morning,

Attached is the initial CD for my client (based on preliminary fees that you sent over). Can you please advise on revised/added fees (tax prorations, HOA dues, etc)?

Preliminary CD and Contract is enclosed via encrypted secure OUTLOOK PDF format

Kathy Hale
Assistant
John E. Robinson
Key Financial, Inc.
161 Belle Forest Circle
Nashville, TN 37221
323-892-5021

From: Katie Bennett <kbennett@lawyersadvantages.com> Sent: Mon 3/5/2018 10:47 AM
To: John St. Lawrence
Cc:
Subject: Deed**Title Payoff Amount Update Needed**69 Union Street
Message | SCAN1606_000.pdf.htm (14 KB)

Hello,

Attached are the Statements, Deed, Title Commitment, and Payoff for 69 Union Street – scheduled to close on Monday, 3/9, at 4PM at Unity Real Estate. We will send the balance of the Real Estate Closing Documents upon completion.

Please let us know if you have any questions or need anything additional.

Have an Excellent day!

Katie Bennett | *Settlement Pre-Processor* | Lawyers Advantage Title Group

Phone: 410-480-2890 | Fax: 410-480-1575

8000 Main Street, Ellicott City, MD 21043

www.lawyersadvantages.com

***WIRE FRAUD TREND ALERT* We have seen an increase in fraudulent wire instructions received via email. Protect yourself by always verbally confirming wire instructions with your beneficiary directly on a substantiated phone number before wiring.**

31

Red Flags

From: ⁎Dropbox⁎ <svp@a-llaw.com>
To: no-reply@dropboxmail.co
Cc:
Subject: New Document "Distribution" -(Via ⁎Dropbox⁎)

Hi there,

A new Dropbox document titled "Distribution" has just been shared with you!

View Shared Document

"Please sign and return"

Dropbox also lets you easily share docs and photos, and collaborate with friends.

Thanks!
- The Dropbox Team

Want to stop getting invites from Dropbox? Unsubscribe
Dropbox, Inc., PO Box 77767, San Francisco, CA 94107

© 2018 Dropbox

If there are problems with how this message is displayed, click here to view it in a web browser.
From: Sadowski, Franciszka <SADOF002@hartford.gov> Sent: Wed 3/28/2018 5:08 PM
To: John St. Lawrence
Cc:
Subject: New Zix secure email message

New Zix secure email message from Hartford Finance

Open Message

To view the secure message, click Open Message.

Recipient - jst.lawrence@thefund.com

The secure message expires on Apr 08, 2018 @ 02:56 PM (PST).

Do not reply to this notification message; this message was auto-generated by the sender's security system. To reply to the sender, click Open Message.

If clicking Open Message does not work, copy and paste the link below into your Internet browser address bar.
https://web1.zixmail.net/s/3e3r3r4?cdvdvds=vsvsv

32

Red Flags

Pressure Tactics – Beware manufactured urgency

- Can be a tactic to short-circuit critical thinking

- Beware sudden changes in business practices
  - Ex) Business contact suddenly asks to be contacted at personal email address

- "Emergency" phone calls/email
  - Fraudsters monitor social media for information on business travel; vacations
  - May strike when critical decision makers out of the office
  - Be wary of attacks on Fridays or near holidays
  - Now possible to "deep fake" voices through software

The Fund ALWAYS DRIVEN

33

Server Security

- Use a firewall
  - Blocks unauthorized network traffic
  - Blocks unauthorized software downloads

- Limit privileged and admin-level network access to those who need it

- Limit file, directory, and network permissions to appropriate users

The Fund ALWAYS DRIVEN

34

Server Security

- Utilize lengthy passwords
  - Time to crack with “brute force” software:
    - M0nK3Y 1 hour
    - 14monkeyswearhats 800,309,871 millennia
- Consider multi-factor authentication process for log-in
- Consider backing up data offsite
  - Ransomware can infect backups as well
  - Backup should not be connected directly to network
  - Encrypted tapes or disks can be stored remotely

The Fund ALWAYS DRIVEN

35

Software Security

- Use your own domain for email
- Use antivirus/antispyware software and keep it up to date
- Consider using software to filter content of inbound and outbound email
  - If no international business, why accept email from outside U.S.?
  - Block SSNs and wire instructions from outgoing messages
- Check/lock Outlook settings so email cannot be auto-forwarded

The Fund ALWAYS DRIVEN

36

Antivirus and Spam Filtering Software

(no Fund endorsement expressed or implied)

- Antivirus/Antispyware
  - Bitdefender
  - McAfee Total Protection
  - Webroot
  - Norton 360
  - Kaspersky
  - F-Secure

- Spam filtering (in/outbound)
  - SpamTitan
  - Vircom
  - Spambrella
  - Cyren
  - Mimecast
  - AppRiver

The Fund ALWAYS DRIVEN

37

Insurance Considerations

The Fund ALWAYS DRIVEN

38

Insurance Considerations

- What covers what?
  - Errors & Omissions covers your acts of negligence
  - Cyber covers ransomware, data breaches
  - Crime covers third party theft (traditionally, hacking)
    - "Funds transfer fraud" = unauthorized instruction to wire out
    - A "Social Engineering Fraud Endorsement" to Crime, Cyber or E&O, which might cover BEC, is getting more expensive, harder to find, with lower sub-limits (now typically $100k -$250k)
    - TIP = rely on experienced insurance broker who can reduce premiums by bundling policies

The Fund ALWAYS DRIVEN

39

Insurance Considerations

- Identify the policies that cover the type of wire fraud seen in real estate
- Review whether the limits of coverage for that exposure is adequate
- Review the claim triggers under which a loss will be covered by each policy
- Coordinate the various policies so that it is clear what will happen if a claim arises

The Fund ALWAYS DRIVEN

40

Insurance Considerations

- Ask what does the insurance policy include? Does it have a SEF endorsement?
- What are the applicable limits? Check on sub-limits and separate retention amounts for business email compromise
- Ask if a social engineering endorsement can be added to an E&O policy at time of renewal

The Fund ALWAYS DRIVEN

41

Insurance Considerations

- Negotiate Exclusions
- You don't get if you don't ask!
  - Call Back v. No Call Back

The Fund ALWAYS DRIVEN

42

Insurance Considerations

- Consider using third party vendors such as;
  - CertifID (www.certified.com)
  - Vialok (www.vialok.com)
  - These companies offer upwards of $1m of insurance against a misappropriated wire under certain circumstances

The Fund ALWAYS DRIVEN

43

Wire Transfer

The Fund ALWAYS DRIVEN

44

Wire Transfer – Facts

- Wire transfer fraud in US Real Estate only – 2018 statistics
  - $149,457,144.00 in 2018
  - $12,454,759.50 per month!
  - $409,471.63 EVERY DAY! And growing
  - 9,600 victims in 2017
- FBI – labeled the scams as “business email compromise” or BEC
- Fraudsters create urgency – MUST BE DONE NOW!!!
- 2018 - Florida national ranking for BEC fraud
  - Number of victims – 3rd
  - Amount of funds lost – 4th

The Fund ALWAYS DRIVEN

45

Wire Transfer

- Warn, warn, warn clients; then warn again
  - Websites
  - Communications – emails etc.
  - Send separate notice to clients & real estate agents
- Call for verification – let client know ahead of time
- Verify account holder information with receiving bank prior to initiating the wire transfer!

The Fund ALWAYS DRIVEN

46

Wire Transfers – Warning Verbiage

- Be aware! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS call us immediately to verify the information prior to sending funds.
- Due to increased fraud, buyers, sellers and lenders should confirm all wiring instructions by phone directly with our office before transferring funds.
- WARNING! WIRE FRAUD ADVISORY: Wire fraud and email hacking/phishing attacks are on the increase! If you have an escrow or closing transaction with us and you receive an email containing Wire Transfer Instructions, DO NOT RESPOND TO THE EMAIL! Instead, call your escrow officer/closer immediately, using previously known contact information and NOT information provided in the email, to verify the information prior to sending funds.

47

Wire Transfers – Use Outgoing Wire Checklist

ALTA Information Security Committee
Outgoing Wire Preparation Checklist
V.2.0 08-19-2019

ALTA Outgoing Wire Preparation Checklist

Visit the ALTA Website: https://www.alta.org/business-tools/information-security.cfm

Date: _____

File Number: _____

Company Name/Location: _____

48

Wire Transfers – Use Outgoing Wire Checklist

- Review the source of wiring instructions
  - Originally
  - Where they changes, if so what was the verification of the change
- Verify instruction received
  - How sent
  - When sent – how long to send out – each bank is different – may take a while to confirm
  - Call trusted number to ensure receipt
    - Read instructions to sender to confirm accuracy
  - List wire creator & authorizer
- Verify delivery of wired funds
  - Call to verify receipt

The Fund ALWAYS DRIVEN

49

Wire Transfers – Best Laid Plans of Mice & Men

- No matter how many warning or how careful you are – something will go wrong
- Review insurance to ensure proper coverage
  - Losses from wire fraud
    - Email is hacks and false information is sent out
    - Fraudster obtains information and uses it to defraud a party – information may have come from another party in the transaction
- Have a plan – TIME IS OF THE ESSENCE

The Fund ALWAYS DRIVEN

50

Wire Transfers – ALTA Rapid Response Plan

- Alert company management & internal wire fraud response team
- Report to sending & receiving banks
- Report to law enforcement
- Call sending bank to confirm recall request has been processed
- Inform parties in the transaction – using known numbers
- Check with your plan to see if you need to secure internally
- Consider contacting insurance carrier(s)
- If wired out of the US, hire attorney in that country to help recovery
  - The Fund does not allow foreign wire transfers
- Document you response
- File complaint with FBI

51

Wire Transfers TIPS

1. Call, don't email wire instructions
   - If you receive email instructions – do not use the number in the email to verify the instructions – read back instructions for accuracy
2. Use secure portals for communications
3. Verify all wire transfers instructions and portal invitations
   - Known numbers
4. Be suspicious
   - Be wary of email requesting changes in information
5. Forward, don't reply
   - If email came from look-a-like address it will then go to correct mail address

52

Wire Transfers TIPS

6. Confirm everything
   - Have bank confirm the name and account prior to sending the wire
   - Re-read instructions the same as meets and bounds legal description
7. Verify that the funds transferred immediately
8. Confirm receipt of wires
9. Sender of wire to initiate phone calls verifying information
10. Warn all parties of BEC and wire fraud

53

Staff Development

The weakest link in cyber defense is the human factor

The Fund ALWAYS DRIVEN

54

Staff Development

- Employee access to files, programs or websites
  - Office policy manual
  - Physical restriction

The Fund ALWAYS DRIVEN

55

Staff Development

- eMail Best Practices
  - "Forward" not "Reply" to business eMail
  - Unencrypted eMail content
  - Hot links and downloads

The Fund ALWAYS DRIVEN

56

Staff Development

- Encourage third-party product research and study
  - Identity and account credential verification
    - CERTIFID
    - evident
  - Encryption service providers
  - Free cyber webinars

57

Staff Development

- Conduct phishing tests

58

Cyber-Security Awareness Month

59