



Fraud Prevention 2024: Recognizing Red Flags in Legal Practice and Staying Ahead with Technology

Welcome!

Please make yourself comfortable, the session will start shortly.



Fraud Prevention 2024:
Recognizing Red Flags in Legal Practice
and Staying Ahead with Technology



Sharad Singh
Head
RS & CS Main Street Distribution



Marie Taylor
Director, National Underwriter
Legal, Risk and Compliance



John Tracy
Senior Legal Counsel
Claims



Twane Boettinger
Director
Information Security & IT Risk Governance

Agenda

Fraud in real estate transactions

- Types of fraud that are prevalent in real estate legal transactions
 1. Corporate ID fraud
 2. Internal office fraud
 3. Elder abuse
 4. Wire fraud
 5. Bad cheque fraud
- Red flags and best practices to keep in mind

Client identity and verification

- Overview of synthetic ID
- Deepfake scams
- Importance of digital ID verification tools for all deals

Information technology - protect your business

- Overview on phishing attacks; social engineering (SE) and business account takeover
- Resources to protect your business

Questions?

Please use the
interactive Zoom

Q&A

1) Fraud in Real Estate Transactions

A) Corporate ID Fraud

Corporate ID Fraud – What is it?

Multiple Variations

- A third party, real or fictitious, **poses as an existing officer** or director and mortgages or sells real estate owned by the corporation
- A third party, real or fictitious, **fraudulently installs him or herself as an officer** or director and mortgages or sells real estate owned by the corporation
- A related party **removes an existing officer** or director and sells or mortgages real estate owned by the corporation without the knowledge or consent of the legitimate officers or directors.



Corporate ID Fraud – Red Flags

- Vacant Land or other unoccupied Property
- Recent Changes in Officers and Directors
- Lack of Minute Book
- A Pristine Minute Book
- Property is Free and Clear
- Funds are being paid to anyone other than registered owners after payment of legitimate debts
- Rushed Closing



Corporate ID Fraud – Best Practices

- Ask questions regarding any recent changes in officers and directors
- Closely examine Minute Book – does it match the vintage of the Corporation? Ask questions
- Internet searches
- Ask questions about the transaction and/or property
- Disclose all information to your title insurer
- Never feel rushed

Corporate ID Fraud – Title Insurance Coverage?

Commercial Policies

- Owner (Policy Coverage and Post Policy Fraud Endorsement)
- Lender (Policy Coverage and Post Policy Fraud Endorsement)

Residential Policies

- Owner (Policy Coverage)
- Lender (Policy Coverage)

B) Internal Office Fraud

Internal Office Fraud – What is it?

- Employee or Independent Contractor of the Firm uses his or her insider position to commit fraud.



Internal Office Fraud – Red Flags

- Working long hours alone
- Family Problems
- Addictions
- Control Issues
- Refusal to take vacation
- Defensiveness
- Living beyond means



Internal Office Fraud – Best Practices

- Formal screening and background checks for all new staff/contract worker/freelancers
- Implement internal controls
- Never share electronic title registration passwords
- Practice proper bookkeeping
- Know your employees

Internal Office Fraud – Is it covered by Title Insurance ?

- Funds diverted to pay off mortgages
- Active participation in identity theft scams
- Plain and simple theft of client funds

C) Elder Abuse

Elder Abuse – What is it?

- financial abuse is the most common form of elder abuse
- any improper conduct done with or without informed consent of a senior that results in monetary or personal gain to the abuser and/or monetary or personal loss for the senior.
- misuse/fraudulent Power of Attorney
- theft, fraud, forgery
- undue influence



Elder Abuse – Red Flags

- elderly client you have never met before
- client is accompanied by an individual who is doing all the talking
- title search indicates numerous NOSI's and private mortgage is being registered to pay them off
- Power of Attorney recently prepared and now Donor has capacity issues
- the borrower is not personally benefitting from the proceeds of the mortgage
- elderly client has property free and clear of mortgages and now is obtaining a very large private mortgage





* CERTIFIED IN ACCORDANCE WITH THE LAND TITLES ACT * SUBJECT TO RESERVATIONS IN CROWN GRANT *

REG. NUM.	DATE	INSTRUMENT TYPE	AMOUNT	PARTIES FROM	PARTIES TO	CERT/CHKD
		REMARKS: P [REDACTED] 4.		[REDACTED]		
[REDACTED]	2019/08/27	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest #6 is registered in 2019	
[REDACTED] 6	2019/09/09	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest #7 is registered one month later	
[REDACTED]	2020/03/06	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest # 8 is registered a few months later	
[REDACTED]	2020/03/17	CHARGE		*** COMPLETELY DELETED *** [REDACTED]	[REDACTED] Private mortgage is registered	
[REDACTED]	2020/09/03	CHARGE		*** COMPLETELY DELETED *** [REDACTED]	[REDACTED] Six months later another private mortgage is registered	
[REDACTED]	2020/09/22	TRANSFER OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	[REDACTED] Second private mortgage is transferred to a private individual three weeks after it is registered	
[REDACTED]	[REDACTED]	[REDACTED]		[REDACTED]	Security Interest #9 is registered	
[REDACTED]	[REDACTED] 05	CHARGE		*** COMPLETELY DELETED *** [REDACTED]	[REDACTED] New private mortgage is registered	
[REDACTED]	2021/03/09	DISCH OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	Previous second private mortgage discharged	
[REDACTED]	2021/03/15	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest No. 7 is discharged	
[REDACTED]	2021/03/16	DISCH OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	First Private mortgage is discharged.	
[REDACTED]	2021/03/22	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest No. 2 is discharged	

NOTE: ADJOINING PROPERTIES SHOULD BE INVESTIGATED TO ASCERTAIN DESCRIPTIVE INCONSISTENCIES, IF ANY, WITH DESCRIPTION REPRESENTED FOR THIS PROPERTY.
NOTE: ENSURE THAT YOUR PRINTOUT STATES THE TOTAL NUMBER OF PAGES AND THAT YOU HAVE PICKED THEM ALL UP.



* CERTIFIED IN ACCORDANCE WITH THE LAND TITLES ACT * SUBJECT TO RESERVATIONS IN CROWN GRANT *

REG. NUM.	DATE	INSTRUMENT TYPE	AMOUNT	PARTIES FROM	PARTIES TO	CERT/CHKD
		REMARKS: A [REDACTED]				
A [REDACTED]	2021/03/30	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest No. 10 is registered	
[REDACTED]	2021/03/30	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Secursity Interest No. 9 discharged	
		REMARKS: [REDACTED].				
[REDACTED]	2021/04/14	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED] LP	Security Interst No. 11 is registered	
		REMARKS: [REDACTED]				
A [REDACTED]	2021/05/07	DISCHARGE INTEREST		*** COMPLETELY DELETED [REDACTED] [REDACTED].	Security Interest No. 3 is discharged	
		REMARKS: A [REDACTED]				
[REDACTED]	2021/05/21	CHARGE		*** COMPLETELY DELETED *** [REDACTED]	[REDACTED] Private Mortgage is registered.	
[REDACTED]	2021/06/25	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]		
		REMARKS: [REDACTED]				
[REDACTED]	2021/07/07	CHARGE	\$756,250	[REDACTED]	[REDACTED] New First Mortgage registered	C
[REDACTED]	2021/07/08	DISCH OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	Private mortgage is discharged	
		REMARKS: A [REDACTED]				
[REDACTED]	2021/07/28	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security Interest No. 6 ischarged.	
		REMARKS: [REDACTED]				
[REDACTED]	2021/08/20	DISCH OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	Private mortgage is discharged	
		REMARKS: A [REDACTED]				
[REDACTED]	2021/08/23	CHARGE		*** COMPLETELY DELETED *** [REDACTED] N [REDACTED]	[REDACTED] New Private 2nd mortgage registered	

NOTE: ADJOINING PROPERTIES SHOULD BE INVESTIGATED TO ASCERTAIN DESCRIPTIVE INCONSISTENCIES, IF ANY, WITH DESCRIPTION REPRESENTED FOR THIS PROPERTY.
NOTE: ENSURE THAT YOUR PRINTOUT STATES THE TOTAL NUMBER OF PAGES AND THAT YOU HAVE PICKED THEM ALL UP.



* CERTIFIED IN ACCORDANCE WITH THE LAND TITLES ACT * SUBJECT TO RESERVATIONS IN CROWN GRANT *

REG. NUM.	DATE	INSTRUMENT TYPE	AMOUNT	PARTIES FROM	PARTIES TO	CERT/CHKD
[REDACTED]	2021/11/23	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Notice of security Interest No. 12 is registered	
[REDACTED]	2021/11/23	NO SEC INTEREST	\$3,873	[REDACTED]	Notice of Security Interest No. 13 is registered	C
[REDACTED]	2022/05/20	NO SEC INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Notice of Securiry Interest No. 14 is registered	
[REDACTED]	2022/06/10	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Notice of Security Interest No. 10 is discharged	
[REDACTED]	REMARKS: P [REDACTED].					
[REDACTED]	2022/06/28	CHARGE	\$475,000	[REDACTED]	[REDACTED] New Private 2nd mortgage	C
[REDACTED]	2022/06/28	NO ASSGN RENT GEN		[REDACTED]	[REDACTED] Corresponding assignment of rents	C
[REDACTED]	REMARKS: ASSIGNS P [REDACTED]					
[REDACTED]	2022/06/29	DISCH OF CHARGE		*** COMPLETELY DELETED *** [REDACTED]	Old Private 2nd discharged	
[REDACTED]	REMARKS: P [REDACTED]					
[REDACTED]	2022/10/12	TRANSFER OF CHARGE		[REDACTED]	[REDACTED] New Private second transferred	C
[REDACTED]	REMARKS: [REDACTED]					
[REDACTED]	2022/10/12	TRANSFER OF CHARGE		[REDACTED]	[REDACTED] The second is transferred back to same mortgagee on same day	C
[REDACTED]	REMARKS: [REDACTED]. [REDACTED]					
[REDACTED]	2022/10/27	DISCHARGE INTEREST		*** COMPLETELY DELETED *** [REDACTED]	Security No. 11 discharged	
[REDACTED]	REMARKS: [REDACTED]					
[REDACTED]	2022/11/24	DISCHARGE INTEREST		*** COMPLETELY DELETED [REDACTED] [REDACTED]	Security Interest No. 13 is discharged	
[REDACTED]	REMARKS: [REDACTED]					
[REDACTED]	2023/03/21	NO SEC INTEREST	\$41,140	[REDACTED]	Security Interest No. 14 registered	C
[REDACTED]	2023/03/21	NO SEC INTEREST	\$41,140	[REDACTED]	Security Interest No. 15 registered	C

Elder Abuse – Best Practices

- document your conversations with your clients;
- meet with your clients alone where possible to insure they are not being influenced
- ask questions – why do they require a private mortgage, are they aware of the fees, rates, penalties
- if the mortgage is to assist a child, are there other children
- if there are Notices of Security Interests – was the equipment installed, are they aware of the lien
- trust your instincts

Elder Abuse – Is it covered by Insurance

- invalidity
- unenforceability
- Duty to defend

D) Wire Fraud

Wire Fraud– What is it?

- Use of trickery to divert the electronic transfer of funds.



Wire Fraud – Red Flags

- ANY kind of electronic communication asking that account details be changed or even set-up.



Wire Fraud– Best Practices

- Never change account details based on the strength of an email alone.
- In the days of “deep fakes” even be wary of telephone instructions.

Wire Fraud – Is it covered by title insurance?

- Funds diverted to pay off mortgages
- Check commercial policies for schedule b exceptions
- Plain and simple theft of client funds

E) Bad Cheque Scam

Bad Cheque Scam – How does it work?

- Fraudsters alter legitimate cheques or falsifies the cheques to scam a lawyer to send legitimate trust funds
- Divorce Settlement
- Debt Collection
- Employee Injury
- Real Estate



Bad Cheque Scam – Red flags

- New client
- Email address is typically from free service, Hotmail, Gmail – even if it is a business
- Email has typos
- Client is out of country - prefers email
- Rush transaction
- Willing to pay higher than normal legal fees because it is a rush
- You're instructed to wire funds quickly
- Some or all funds going to a third party not related to Transaction.



Bad Cheque Scam – Best practices

- Cross check and verify information provided to you
- Google Maps – street view
- Make sure funds have cleared
- Confirm Payee
- Contact Bank on cheque you receive
- Never feel rushed

Bad Cheque Scam – Is there coverage with title insurance?

- NO and YES

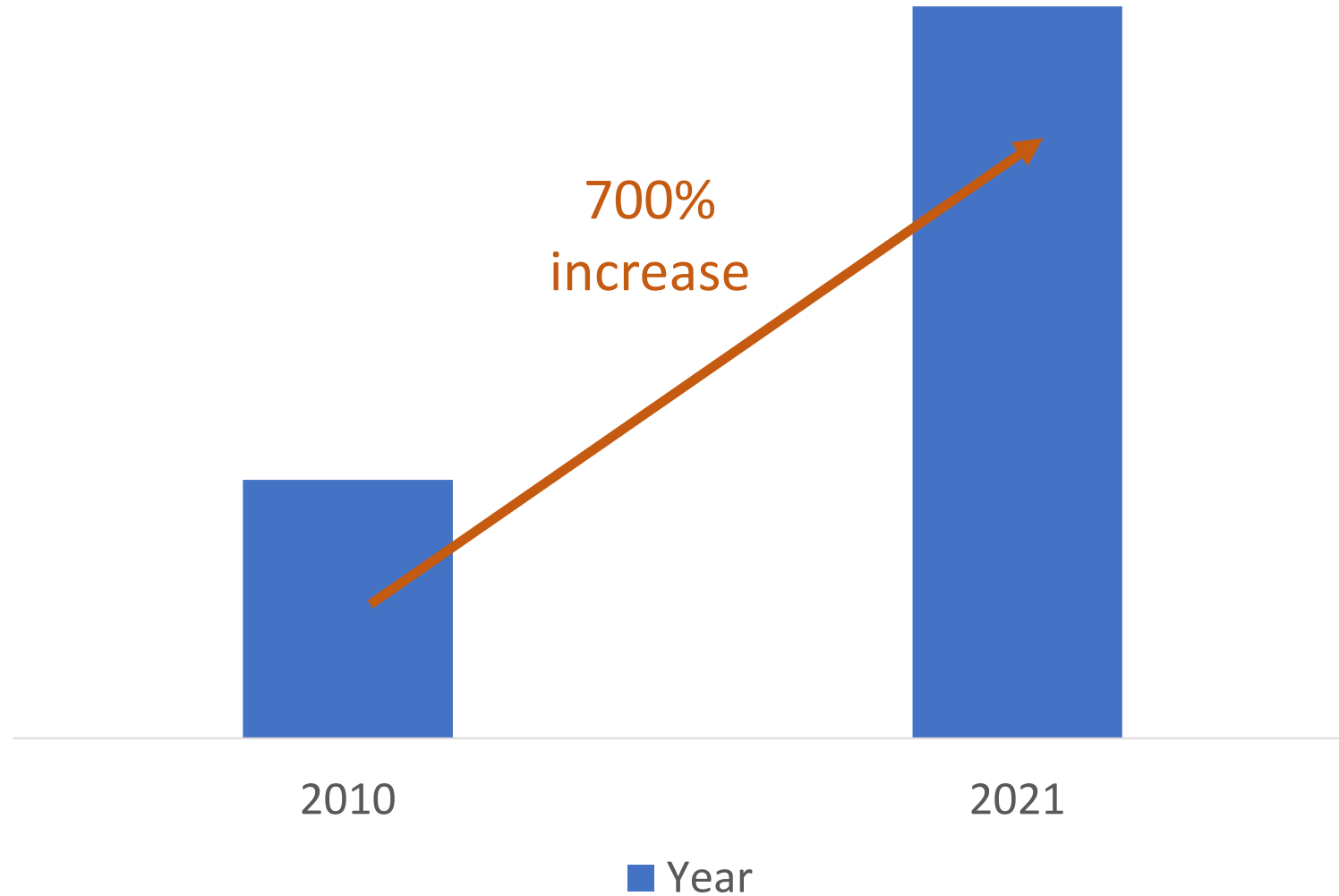
2) Client Identity and Verification



\$539,000,000

Suspicious transactions identified

The growing risk of technological sophistication: fake ID



New type of fraud: synthetic identity

- Create fake identities by combining fake information with actual ID data
- These fake IDs are perfect and impossible to spot without sophisticated technologies
- The process takes years but is highly lucrative, resulting in financial, emotional and reputational impact

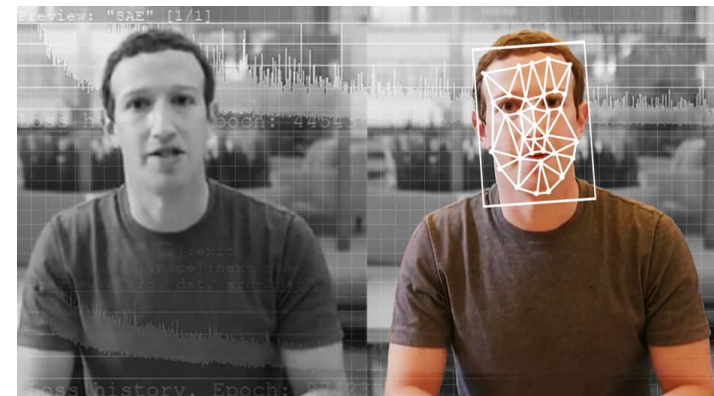
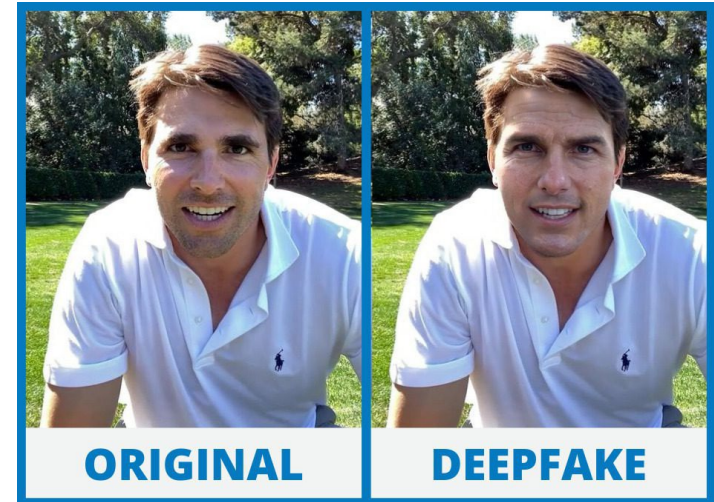


New type of fraud: Deepfake fraud



New type of fraud: Deepfake fraud

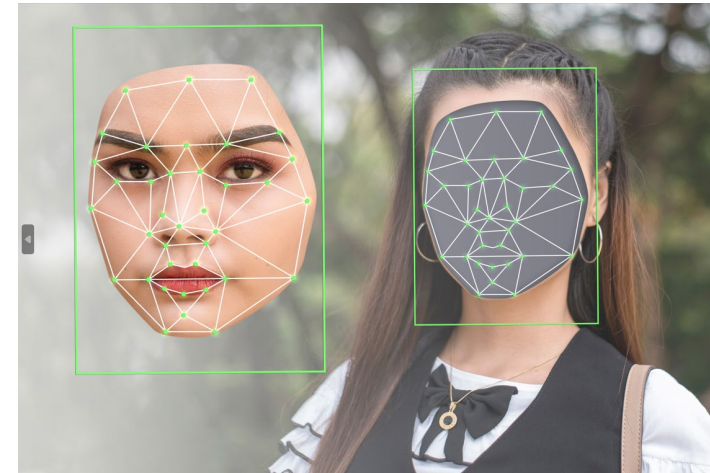
- There are several fake ID generation websites
- Deep fakes are highly realistic digital manipulations of audio, images, or video
- Highly accessible - the potential for mass scale, and potentially, mass destruction.
- Fraudsters are combining 3D printing with deepfake capability to produce high-quality physical IDs



New type of fraud: Deepfake fraud

\$25 MILLION STOLEN

- Fraudsters used deepfake technology to convince bank employee to execute multiple money wires
- Bank employee was on Zoom call with 15 participants – all deepfake avatars
- Bank employee even thought the CFO was on the call



Traditional identity verification methods are on their way out

- Government-issued ID cards: passports (without an encrypted chip), driver's licenses
- Utility bills or bank statements
- Knowledge based questions: a series of personal questions
- Credit checks: credit history



3) IT Security for a legal services practice

Key items

- Social engineering (SE)
- Business Account Take Over
- Resources

Impact of Fraud in 2023



\$554M+
AMOUNT LOST



62K+
NO. OF REPORTS



41K+
VICTIMS OF FRAUD



6.7M
FUNDS RECOVERED WITH
CAFC ASSISTANCE

Source: [Canadian Anti-Fraud Centre \(antifraudcentre-centreantifraude.ca\)](https://antifraudcentre-centreantifraude.ca)



Social Engineering In Action

- The art of manipulating, influencing or deceiving victims to gain control over computer systems.
- Three most common deceptive techniques; email-based phishing, text message based (SMS) smishing and voice-based vishing. Other common forms of SE described in this article by [CrowdStrike](#)¹.
- Understanding attack vectors can empower users to recognize the range of techniques employed by adversaries.
- SE, and email phishing specifically, remain the most successful attack vector.
- Educating staff, creating awareness and encouraging a culture of suspicion remain your best defense.

¹ 10 TYPES OF SOCIAL ENGINEERING ATTACKS AND HOW TO PREVENT THEM Bart Lenaerts-Bergmans - November 8, 2023

² Finance worker pays out \$25 million after video call with deepfake 'chief financial officer' Heather Chen and Kathleen Magramo, CNN. Published 2:31 AM EST, Sun February 4, 2024

What to do when faced with Social Engineering?

1) Report it internally

- IT/Security department
- Your email provider

2) Report it to authorities.

- If the email is asking you for personal or financial information or threatening you with legal action, blackmail or harm.
- Canadian Anti-Fraud Centre (CAFC)
- Local police



What to do when faced with Social Engineering?

3) Delete it

4) Build a playbook

- Work with your IT support to create a well defined, quickly actioned, repeatable set of steps immediately following a SE report
- Focus on email first, but don't stop there

* What about smishing messages?

- Report suspicious text messages to 7726 (SPAM)

What if staff “clicked the link”?

1) Immediate threat

- Ensure you are using the **latest version of antivirus** or antimalware in your devices.
- If the link takes the staff member to some input site, **do not provide any personal information.**
- **Close all browsers** immediately.
- **Disable the connection** to the internet (pull the ethernet cable, turn off Wi-Fi radio).



What if staff “clicked the link”?

2) Report the episode to IT/Cybersecurity Team immediately.

- Consider reporting to CAFC, CCS and/or local police.
- Scan your machine for malware.

3) Protect your identity

- Consider changing your passwords to sensitive accounts (corporate and personal) even if no information shared.
- Use a different device to change your passwords.
- Use unique credentials for each service to prevent access sprawl.
- Consider heightened security monitoring on your accounts and devices for a period of time.

Email Take Over (aka Business Email Compromised, BEC)

How to avoid email takeover?

- **Avoid clicking** on links or downloading attachments from unknown sources.
- Instead of using a short, complex password that is hard to remember, consider using a **passphrase**.
- Enable **Multi-Factor Authentication** wherever you can.
- **Avoid re-using passwords**. Cybercriminals use stolen credentials to automate attacks on multiple sites. Reused passwords make this easier.



Email Take Over (aka BEC)

How to avoid email takeover? - continued

- Use reputable antivirus and firewall software.
- Avoid using a corporate email address to register on social networks, online services, and other nonwork resources.

PRO-TIP

Consider multiple email accounts with purpose in mind:

- Friends and Family
- Corporate services outside your main corporate email
- Shopping services

Email Take Over (aka BEC) - continued

How do I know if my email is compromised?

- Inability to sign into your email account
- Receiving unexpected password reset emails.
- Unusual account activity
 - i.e. emails in Sent Folder that you didn't send
- Changes to email settings
 - i.e. forwarding rules, filters, or your signature



PRO-TIP

Check **haveibeenpwned.com** - allows you to search across multiple data breaches to see if your email address has been compromised.

Email Take Over (aka BEC) - continued

What are my next steps if I suspect my email is compromised?

1) If you no longer have access

- Contact your email provider and request that they issue a **temporary password** so you can regain access and change your password and security questions.

2) When you have access to your account, immediately

- change your password and security questions
- Implement 2FA
- Disable auto-forwarding and rules

Email Take Over (aka BEC) - continued

What are my next steps if I suspect my email is compromised? - continued

3) Take time to...

- Notify your contacts separately and caution them not to respond to any requests originating from your account.
- Address entities that use this email for billing or correspondence.
- Secure non-email accounts

Additional resources

- **NIST (National Institute of Standards and Technology)** – Free and low-cost online cybersecurity learning content



The image is a screenshot of a webpage from NIST. At the top left is the NIST logo, and at the top right is a link that says "View As Web Page". Below the header is a blue banner with various icons representing technology and security. Underneath the banner is a grey bar with the text "NIST Cybersecurity and Privacy Program". The main content area has a white background with the title "Overview of the NIST Cybersecurity Framework (CSF) 2.0 Small Business Quick Start Guide". Below this is a dark blue section for an "Upcoming Webinar". It features a calendar icon and the date "March 20, 2024" with the time "2:00 PM - 2:45 PM ET". To the right of the text is a circular diagram of the NIST Cybersecurity Framework, showing the five core functions: GOVERN (center), IDENTIFY (top), PROTECT (right), DETECT (bottom), and RESPOND (left). The NIST logo and full name are at the bottom left of the page.

Summary of Best Practices



Q&A



Fraud Prevention 2024:
Recognizing Red Flags in Legal Practice
and Staying Ahead with Technology

Thank you!