ESCROW BOOT CAMP 201

Fraud in the Escrow World

Cindy Immonen, NTP, CLTP, Solutions Provider
VP, Sr. Account Manager
P: 248-331-6860 |E: cindy.immonen@fnf.com

1

Fraud plays out in many various ways!

Let's review…

Cyber training every year - The Why

eFax / Faxing

Physical review

Packages and Mail

The Money

Impersonation Fraud

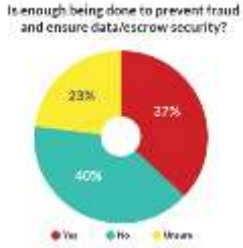
Adding up the RED FLAGS

One in 10 Americans are targeted for Real Estate FRAUD!

2

Fraud plays out in many various ways!

Fraud prevention remains a top concern for title agents.



3

Fraud plays out in many various ways!

4

Cyber training every year – The Why

Help STOP Fraud Before it Starts…

- Annual cybersecurity training is crucial for individuals and organizations to maintain a strong defense against cyber threats.
  - Awareness of evolving threats: Cybersecurity threats are constantly evolving, with new tactics and techniques emerging regularly.
  - Protection of sensitive information: Many cyberattacks aim to steal sensitive data, such as personal information or corporate intellectual property.
  - Prevention of social engineering attacks: Social engineering attacks rely on manipulating human psychology to gain unauthorized access or extract information from individuals.
  - Mitigation of internal risks: Employees can unintentionally pose security risks through actions such as weak passwords, sharing login credentials, or connecting unsecured devices to the company network.
  - Compliance with regulations: ALTA Best Practice #3

5

Cyber training every year – The Why

Help STOP Fraud Before it Starts…

The Biggest WHY????

Companies that we all use every day are HACKED

Bank of America warns customers of data breach after vendor hack

By Sergiu Gatlan

AT&T says data from 73M accounts leaked on dark web

AT&T Inc. said that personal data from about 7.6 million current account holders and 65.4 million former customers was leaked onto the dark web.

The data — leaked about two weeks ago — includes personal information such as Social Security numbers and appears to be from 2019 or earlier, the company said Saturday in a statement. The source of the data is still being investigated, according to AT&T, and it's not known whether it came from the company or a vendor.

200,000 Facebook Marketplace user records leaked on hacking forum

By Sergiu Gatlan

HEALTH INC.

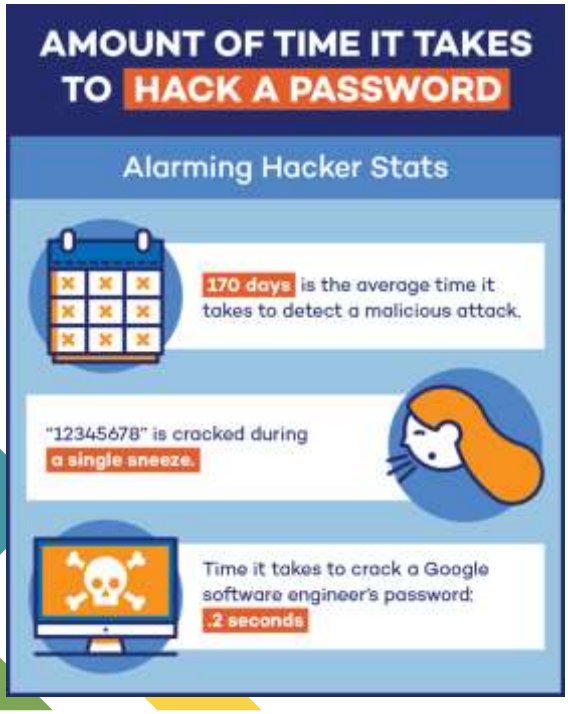
Health industry struggles to recover from cyberattack on a unit of UnitedHealth

A threat actor leaked 200,000 records on a hacker forum, claiming they contained the mobile phone numbers, email addresses, and other personal information of Facebook Marketplace users.

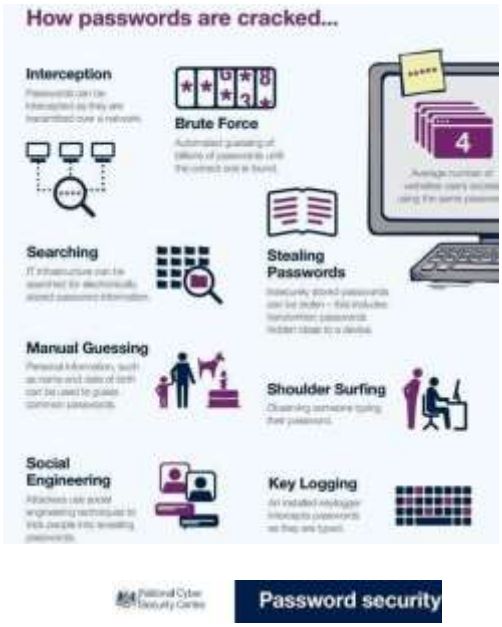
6


PASSWORDS ARE LIKE
UNDERPANTS
Change them often, keep them private and never share them with anyone.

7


AMOUNT OF TIME IT TAKES TO HACK A PASSWORD
Alarming Hacker Stats
170 days is the average time it takes to detect a malicious attack.
"12345678" is cracked during a single sneeze.
Time it takes to crack a Google software engineer's password: .2 seconds

8


How passwords are cracked...
Interception
Brute Force
Searching
Stealing Passwords
Manual Guessing
Shoulder Surfing
Social Engineering
Key Logging
Password security

When it comes to choosing a secure password, length is actually the most important component.

Each additional character in a password exponentially increases its security.

9

Go Long and Complicated

One of the best and easiest things to do is to create a long password out of an easy-to-remember phrase, then throw in some special characters.

For example: “1likeV@nilla1cecreaM”

Passphrases / Root Passphrase is made up of multiple random words, which are easier to memorize, easier to type, and tend to be even more secure than shorter, more complex passwords.

10

- Don’t reuse or recycle your passwords
- Don’t share your passwords with anyone
- Change your passwords using a randomly generated schedule
- Ensure that your passwords bear no resemblance to former passwords
- Consider using a secure password manager to help with creating unique passwords across multiple sites. This can be worrisome too…

11

Features you want with a password manager ~

- Cross-platform support to access and manage your saved passwords across any device or platform
- Multi-factor authentication to secure your password vault
- Offline access to ensure you keep your password even when you're not online
- Browser extension support to ensure you can access your password regardless of the web browser you use

'Zero-knowledge' encryption is important

Pick password managers with secure backups

Check for biometrics and other ways to log in

Don't forget your master password!

12

Be Cautious When Social

Be careful what you share and who you share it with.

This lesson was driven home by the revelation that **about 90 million Facebook users had their profile information and "likes" harvested—without permission—by researchers using a third-party quiz app.**

If you're going to post personal details about yourself (or your family), make sure your accounts are locked down and change your privacy settings to **restrict your posts to real-life "friends."**

Keep in mind that even if you think you have your account locked down, **think before you trade your privacy to play a Facebook game or take part in a what looks like a harmless quiz.**

13

You don't usually play these but,
why not…

Where did you grow up: STOP
Favorite color: GIVING
First pet's name: PEOPLE
Street you grew up on: YOUR
Favorite child's name: PERSONAL
Favorite sports team: INFO
High school mascot: TO
Favorite food: GUESS
What was your first car: YOUR
Mom's name before she was married: PASSWORD
First job: AND
Favorite brand: SECURITY
Favorite food: QUESTIONS

You should protect your information~

- Your birthdate
- Your street address
- **Geotagged photos**
- The time you're away on vacation

Protect Your Connection

PROBLEM

Public WiFi is shared

Viruses / malware are communicable

SOLUTIONS

VPN

Private Tunnel NordVPN

Tethering

COST

$6 per month for VPN

Free for tethering*

When working – Always use your employer's VPN

14

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

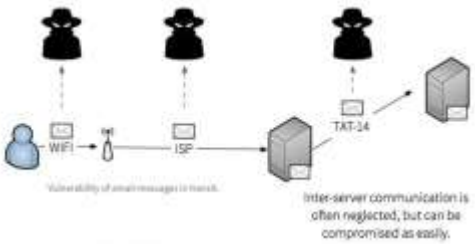
FRAUD DATA FROM 2021 FBI IC3 REPORT, AMERICAN LAND TITLE ASSOCIATION

Send all emails encrypted – **Yes, All Emails.** There are many safe easy services for encrypted emails. Don't bend to the presser of your clients to not send any email non-encrypted.

15

How Fraud Happens

Never conduct business over unsecured WiFi, don't use Free WiFi. Crooks have become wise to this and are hacking your system at this point. Then, hacking those weak email accounts and waiting for the opportunity to send a seller, buyer, real estate agent, or lender false wire instructions that are directed to a "Nigerian Prince".
Then, POOF, the money is gone. The closing doesn't happen, and everyone gets sued.



&

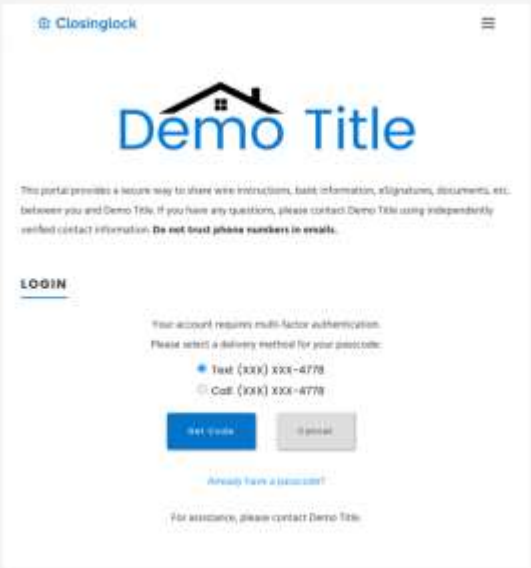
16

Multi-Factor Authentication (MFA)

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

- Knowledge
- Possession
- Inherence

17



Two-Factor Authentication (2FA)

Password + text message

Cost: FREE

18

Two-Factor Authentication (2FA)

Password + software token

Make sure you have backup access!

Cost: FREE

AUTHY

19

Some Tips for *Prevention*: Use Multiple Authentication Methods to prevent hacking…

"**Two Factor Authentication**" can help; you add an extra layer of security to your account by requiring two key elements:

1. Something you know - your password or pin
2. Something you physically have – a smart phone - most commonly a code sent to your phone
3. Something you are - fingerprints

Articles:

Two-factor authentication: What you need to know (FAQ)
https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

Free email services have Multiple Authentication Methods -

- Gmail (https://myaccount.google.com/security/signinoptions/two-step-verification/enroll-welcome)
- Yahoo (https://help.yahoo.com/kb/SLN5013.html)
- MSN (https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification)
- Apple (https://support.apple.com/en-us/HT204915)

Free email services - Check Auto-forwarding Fraudsters Use This Area and create a filter!
Disable Forwarding!!!

20

The average mortgage balance in the United States reached *$241,815* as of Q2 - 2023, making mortgage payoffs a top target for wire transfer fraud.

Mortgage payoff fraud is a financial crime where a fraudster impersonates a mortgage lender in a purchase or refinance transaction and manipulates bank account information on a mortgage payoff statement for the purpose of influencing a title or escrow company into sending a mortgage payoff payment to the fraudster's bank account.

- Sending phishing emails to real estate professionals such as title companies, real estate agents, or even buyers and sellers to gain unauthorized access to their email accounts.
- Collecting information about active and upcoming real estate transactions, including the mortgage payoff details such as account numbers, banking institutions, payoff amounts, parties to the transaction, and key dates.
- Intercepting the genuine mortgage payoff statement and changing the bank account details for the purpose of directing the payment to a criminal's bank account.
- Impersonating the mortgage company and sending the fraudulent payoff statement to the title company.
- Receiving and redirecting the payoff funds to alternative bank accounts to reduce the chance of recovery.

21

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

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: 1234127316
Beneficiary Bank Address:
1 Home Campus
Des Moines IA 50328
Special Information for Beneficiary:
Apply funds to: 936 loan 0312376116E
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 3:00 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 1-800-222-0230, Monday - Friday, 8:00 a.m. to 10:00 p.m., or Saturday, 8:00 a.m. to 3:00 p.m. Central Time.

PAYOFF COUPON: Please detach and include with payoff funds.

22

Foreclosure Payoffs / Foreclosure Timeline

When a Mortgage goes delinquent the lender will work with a law firm to facilitate the foreclosure process.

After the Sheriff Sale the Sheriff's Deed is recorded.
It will state the redemption period – ***Look and know this date***.

The property owner may pay the law firm to redeem the property.
The property owner may sell the property, and this must be done before the redemption period is up.

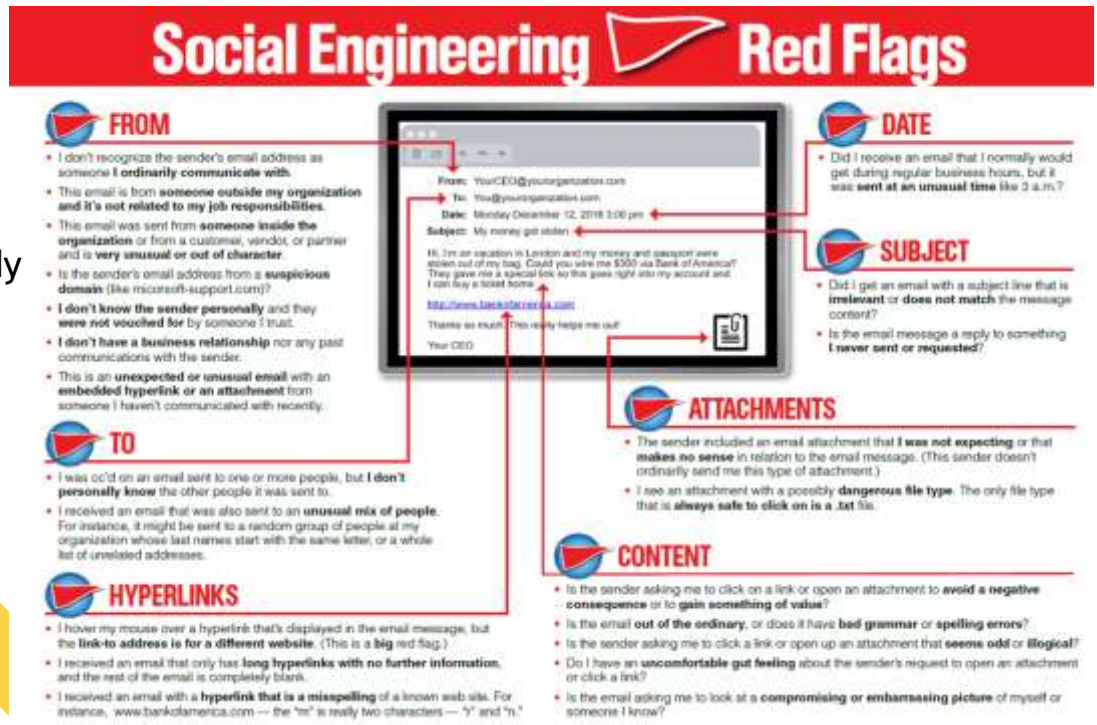
Warning…
There may be a 3-party bidder.

Be sure to read and re-read the payoff!!!
You must pay before the redemption time!

23

This is a handout

Keep handy



24

Security BUZZ as of the 1st of this month…
Beware of new cyber threat – 'Conversation Overflow'

In the ever-evolving world of cyber threats, a new tactic has emerged that's tricking even the smartest AI security systems. It's called "Conversation Overflow," a clever way cybercriminals are getting their phishing emails past our defenses.

Imagine an email that looks totally normal but hidden within it is a secret message designed to fool AI into thinking it's just another friendly chat. That's what's happening with Conversation Overflow attacks. These emails have two parts: one that we can see, asking us to click a link or share information and another hidden part filled with harmless text that makes AI think it's all good.

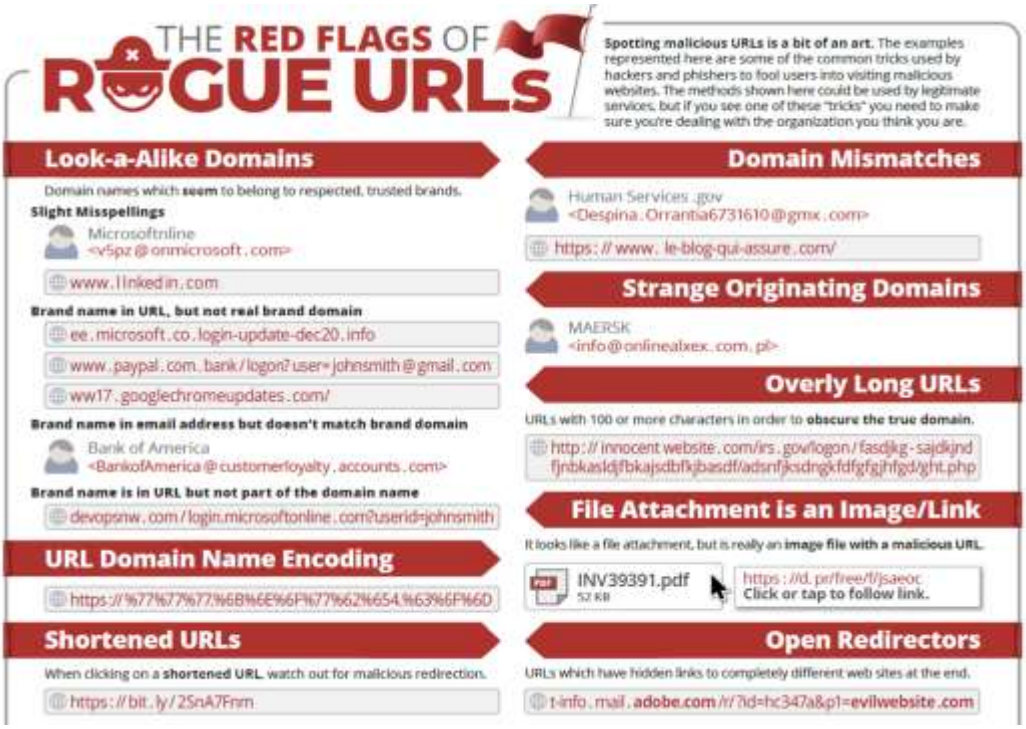
The alarming reality is that these emails specifically target executives and upper management with the highest access and authority level. Once these emails manage to bypass our defenses, they can stealthily request passwords and login details, leading to potential credential theft.

This new twist is our daily reminder to stay vigilant. Never enter credentials on the website you visited using the email link. **Always go to the source directly.**

25

This is a handout

Keep handy



26

This is a handout

Keep handy

27

A QR code, also known as a Quick Response Code, is a type of barcode that stores information in a quick-response format. A smartphone can read the data in a QR code using its camera, making storing and accessing information convenient. To use it, point your smartphone's camera at a QR code, and it will automatically direct you to a website.

Scammers place a ‘fake’ QR code over a real one to trick people into giving away their information!

… When you’re in a rush to process an EMD

When you’re in a rush to park for that closing…

28

QR codes are almost impossible to recognize as malicious by humans, so users must take extra precaution. When presented with a QR code, do all of the following:

•Treat QR codes with even more caution than direct links. If you receive a QR code from someone you know, contact them directly and verify they sent it before you interact with it.
•When scanning a QR code, your device should display a box containing the linked website. Pay close attention to that link and don't visit the website if not known to you and be very cautious of domains that use a URL shortener to hide the destination.
•Use the built-in scanner in your smartphone's camera to scan QR codes. There is no need to download any QR code scanner through the app store. QR code scanners from the app store may come bundled with dangerous or malicious extras.

We must all be vigilant to protect ourselves, your Company, and our customers.

⚠ IMPORTANT PRECAUTIONS

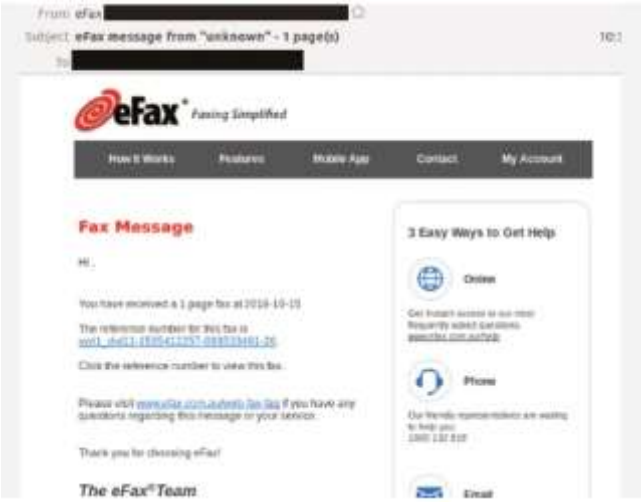
29

Your Devices… Computer | Tablet | Phone

- Always keep your device's software updated (use the latest operating system and browser versions available)
- Install security software and keep it up to date
- Download apps from trusted app stores
- Turnoff Wi-Fi/file sharing/ AirDrop options when not in use
- Avoid working with personal or sensitive data when you're using unsecured, public Wi-Fi
- Lock your devices and use biometric authentication (like face or fingerprint recognition)

30

eFax / Faxing



Be wary of your eFax system.

The fraudsters are intercepting the information and attachment(s) being sent to you via eFax. It safer to not have the eFax go into the inbox of your email system, i.e., opening the fraud link triggers a download of a malicious document that infiltrates trojan malware into your network. Set up your eFax for your staff to go out the 'eFax Portal' and pick up the eFax there. Still scour the information / the attachment(s) as it could have been intercepted and changed before it landed into your eFax portal.

- Yes, fraudsters can do that.

31

Physical review of the office and desks

Physical Security

Many data compromises happen the old-fashioned way—through lost or stolen paper documents. Often, the best defense is a locked door or an alert employee.

- Watch where you place mail & out going overnight.
- *Store* - put away and *Lock Up* paper documents / files.
- *Shred documents* containing personal/financial information.
- *Take Stock* of what you have and *Scale Down*.
- Implement appropriate access controls to your office building.
- Properly dispose of what is no longer needed.
- Create a plan for responding to security incidents.

32

Packages and Mail

Most likely you are overnighting or mailing sensitive information using outside carriers or contractors.

You need to encrypt the information – Do Not put Title Agency on your return address or anywhere on the package or envelope.

Use an overnight shipping service that will allow you to track the delivery of your information.

Do not send mail via a window envelope.

Keep an inventory of the information being shipped.

33

The Financial Crimes Enforcement Network (FinCEN) issued an alert to financial institutions on the nationwide surge in check fraud schemes targeting the U.S. Mail. Fraud, including check fraud, is the largest source of illicit proceeds in the United States and is one of the anti-money laundering/ countering the financing of terrorism National Priorities.

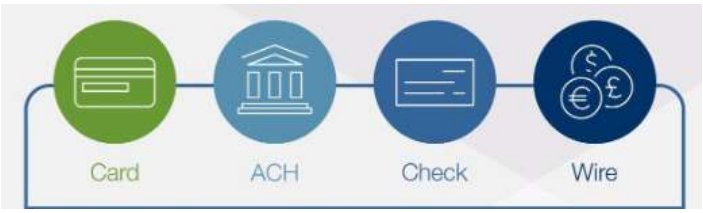
Victims of mail theft-related check fraud should contact the USPIS at 1-877-876-2455 or https://www.uspis.gov/report

The Money $$$

Payment rails are the infrastructure that allows money to transfer between a payor and a payee.

Just as the name suggests, you can think of a payment rail like the tracks for a railroad system. Without them, a train could not travel from Point A to Point B.

The rail allows money to move from one account to another.



34

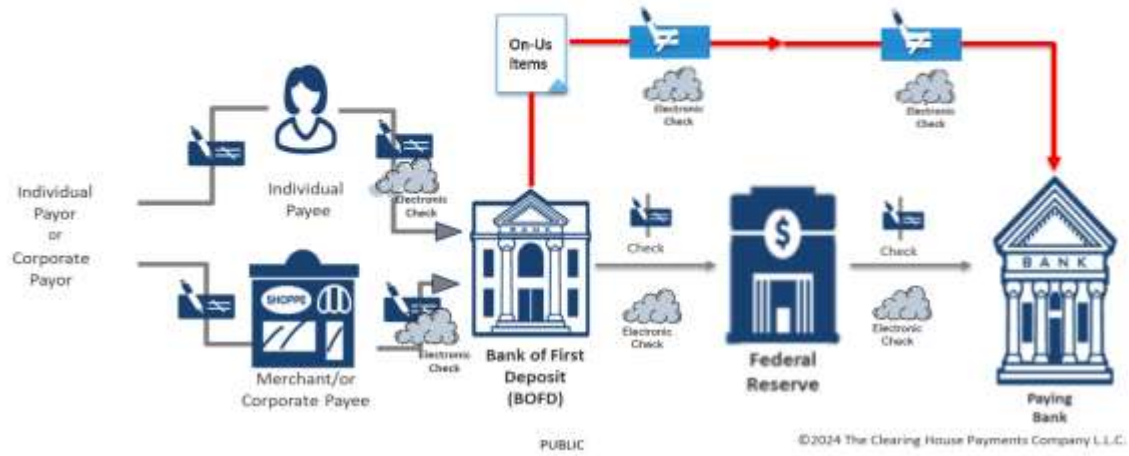
Check	Wire	Card	ACH
Payor	Originator	Card Holder	Originator
Paying/ Payor Bank	Originator's Bank	Issuing Bank (Issuer)	Originating Depository FI
Clearing House Bankers Bank FRB	Fedwire CHIPS	Payment Network	ACH Operator
Bank of First Deposit	Beneficiary's Bank	Acquirer	Receiving Depository FI
Payee	Beneficiary	Merchant	Receiver

Third Party Processors can be used in every payment system

35

Check Collection 101

- Check Payments System
  - Paper process flow shown from individual/corporate payor, to payee, through one or more channels, to the Paying Bank
  - Paper checks or electronic checks (general processes remain the same)



- Battling an increase in check ***fraud***
- Volume declining but not at expected pace

36

A **Cashier's Check** uses funds from a financial institution's account. Cashier's Checks usually include more security features than Certified Checks do.

A **Certified Check** uses funds from a customer's account. Thus, different then a Cashier's Check.

Inspect the check, look for signs that it could be fake (misspelled words or poor-quality paper without any security features). Inspect the check for additions, deletions, or other alterations. Inspect the watermarks.

Fraudsters will use routing numbers and account numbers that do not agree with one another. Ask the bank teller to provide you with their Routing Number and match it to your check. That bank may be willing to tell you whether the check is one they issued and is genuine. A genuine cashier's check always includes a phone number for the issuing bank. That number is often missing on a fake check. But don't use that phone number… Obtain the bank's telephone number from a reliable source.

Search the bank / credit union online for where the check is written on. Fake cashier checks have been known to be from a nonexistent banks / credit union.

37

Investigate if your check is drawn off a Federal Reserve District which is same District where the Bank Account is located. The fraudsters will use a different Federal Reserve District from where the Bank is located. Find & know your Federal Reserve District –

https://www.federalreserveeducation.org/about-the-fed/federal-reserve-districts/

The payee's name should already be printed on a check (this is done at the bank by the teller). If the payee line is blank, the check is fake.

Check to see that the routing number and / or the account number is not shiny in appearance.

Be very cautious when disbursing funds against an uncollected item – the check. If verifying that the funds have cleared… Ask your bank if the funds deposited have been "honored". This is different from "The Funds are Available". "Honored Funds" means that your bank has been paid by the account holder's bank. You need to wait 15 to 30 days for this confirmation.

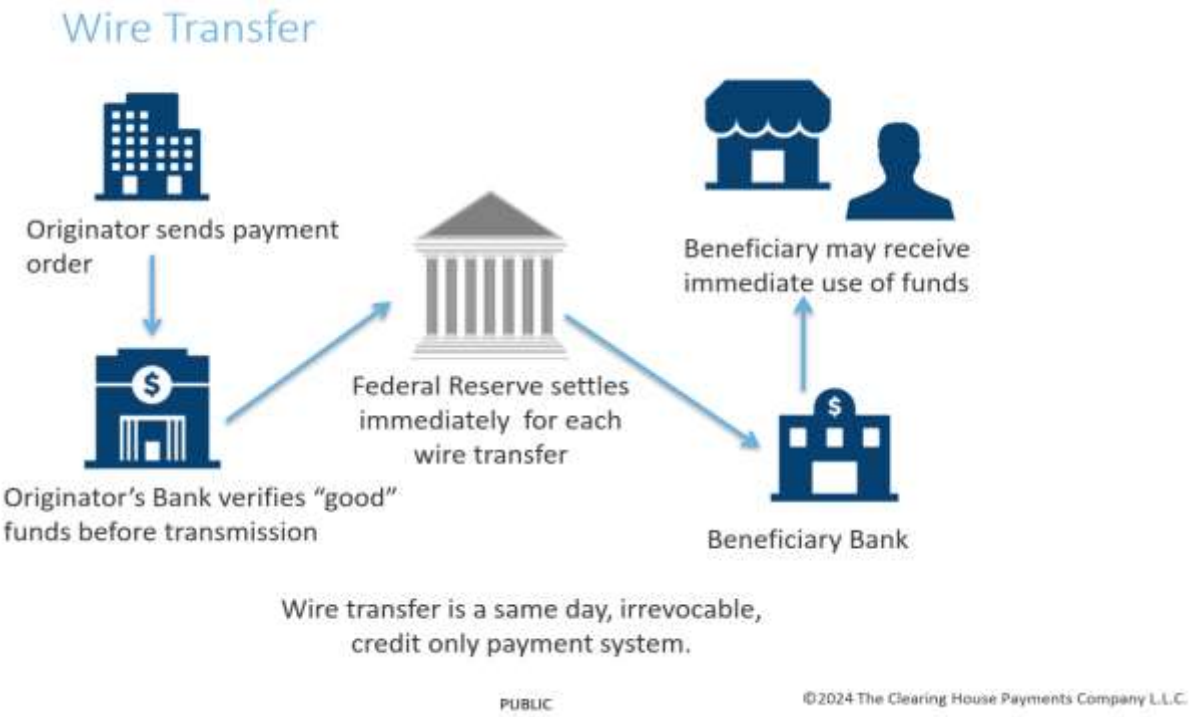
38

Cashier Checks / Certified Checks can be returned up for up to 30 days! Be careful returning funds from Cashier Checks / Certified Checks. Call your bank and confirm the funds have been collected with no return.

If worried… Ask your Bank / CU to have the check sent for collection. Your bank will not put any funds into your account until the check has been paid. You will likely be charged a fee by the bank and this process could potentially take as long as eight weeks.

Some fake checks look so real that bank tellers are reporting to be fooled. The scammers use high quality printers and scanners to make the checks look real. Some of the checks contain authentic-looking watermarks. These counterfeit checks are printed with the names and addresses of legitimate financial institutions. Even though the bank, account and routing numbers listed on a counterfeit check may be real, the check still can be a fake.

39



40

Card Networks

- Provides switching facilities for the routing of credit and debit card transactions between Acquirers and Issuers
- Facilitates the transmission of requests, transactions, approval, and denial messages between parties
- Performs settlement between Issuer and Acquirer accounts including fees
- Develops and administers transaction processing and operating rules
- Enforces compliance among participants

- Battling an increase in card **fraud**
- High fees to the merchant

41

ACH Network Participants and Workflow

42

ACH Return Time Frames For Consumers

Return Type	Return Time Frame
Standard Return	2 Banking Days
Extended Return	60 Calendar Days

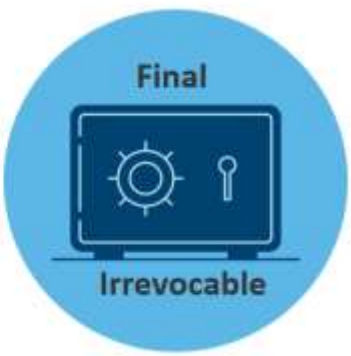
Other Provisions include:

- Return by ODFI request
- Late Permissible Return
- Breach of Warranty Claim

In fact, ACH can be recalled up to 24 months!

43

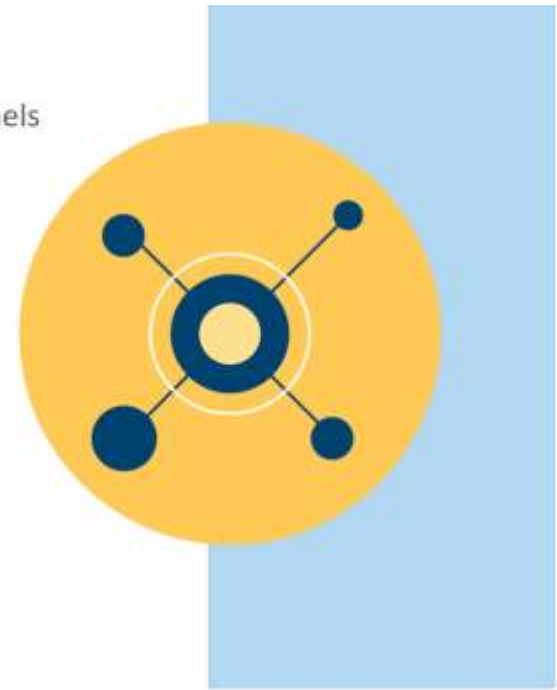
R|T|P Powering Smarter Payments | FedNow 24/7 INSTANT PAYMENTS



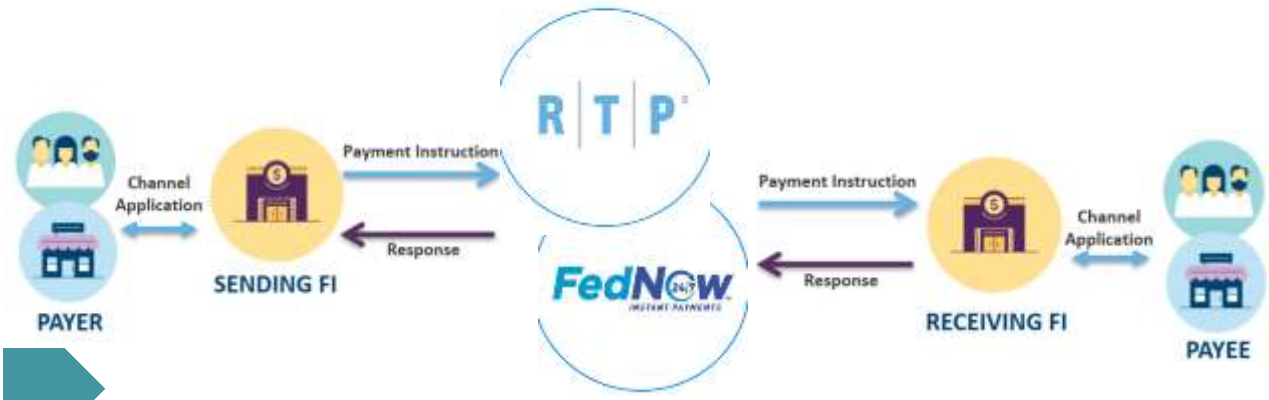
44

Instant Payments Workflow

- Customers initiate/receive through Digital Channels
- Sending Financial Institutions send a transaction through a Payment Message
- Receiving Financial Institution response
  - Accept the payment
  - Accept without Posting
  - Reject
- Messaging Standards: ISO20022



45



24x7x365

Credit Push Only

Final and Irrevocable

46

Crypto Rails
Crypto rails rely on a technology called blockchain – a decentralized, distributed database of encrypted records shared among several computers linked in a peer-to-peer network. Blockchain technology allows information to be recorded securely, ensuring that data cannot be manipulated or corrupted.

Despite some moves around the world to regulate cryptocurrencies, they remain less regulated than many other asset classes. If a platform that exchanges or holds your crypto assets goes bankrupt, there's a risk you could lose all your capital.

Cryptocurrency does not come with any protections!

Cryptocurrency is not safe from hackers.

47

Notary Impersonation Fraud

The Real Estate Agent brings you a document that you need for closing… It's been notarized.

A seemingly innocent document, stamped and signed by a trusted notary. Everything appears to be in order, but little do you know that a dastardly crime has taken place. Notary fraud is a deceptive act that can have far-reaching consequences.

Know that…. An ***Acknowledgement*** is a formal declaration before a duly authorized official (i.e., Notary Public) by a person who has executed an instrument, that such execution in his / her free act and deed – voluntary. The signer is of sound mind too.

Investigate… Ask Questions!

Look up the notary information at the public notary database for the State that the notary is from.

Do they work for a company with the Title Industry? Do you know them?

Ask questions:

- Find the notary's phone number… call and talk with them about the notary.
- Why can't the person signing come to your office or meet with one of your mobile closers / notary's… this is the best case!
- Can the signer sign using RON?

48

Power of Attorney Impersonation Fraud

Know that…. Power of Attorney Scams ~

Elderly People
Couples that are separated or not getting along

The Power of Attorney needs to be recorded

WHY

Two main reasons: ***Insurability and Revocability***

Is a Power of Attorney Assignable? NO

DO NOT ACCEPT Powers of Attorney for

The Executor of a Will and Testament

The Fiduciary Execute / The Estate Representatives

An Entity's Authorized Person

49

Investigate… Ask Questions!

Ask questions:

The signer should come to your office or meet with one of your mobile closers / notary's… this is the best case!

Can the signer sign using RON?

The Power of Attorney MUST

- provide an acceptable "power" referenced in the Attorney-in-Fact document authorizing such a signature for the purpose intended
- still be in effect
- the original grantor is still living
- he/she has not revoked the power

Seller / Buyer Impersonation Fraud

The U.S. Secret Service and ALTA has observed a **SHARP** increase in reports of real estate fraud associated with vacant land, residential property that is rented or a 2nd home, or commercial property that is unencumbered!

FRAUDSTERS are impersonating property owners to illegally sell the property. Sophisticated fraudsters are using the real property owner's Social Security and driver's license numbers in the transaction, as well as legitimate notary credentials, which may be applied without the notary's knowledge.

Fraudsters prefer to use email and text messages to communicate, allowing them to mask themselves and commit crime from anywhere.

50

Is It Too Good to be True? Ask Questions!

From romance to real estate, if it sounds too good to be true, it very well might be!

Ask questions if:

■ The property is a vacant lot or occupied by someone other than the actual owner, such as investment property, vacation property or rental property.

■ The property is for sale below market value.

■ The seller wants a quick sale, generally in less than three weeks, and may not negotiate fees.

■ The seller will only communicate by phone or email and won't meet in person.

The Scheme

- **The criminal searches public records to identify real estate that is free of mortgage or other liens and the identity of the property owner. These often include vacant lots or rental properties.**
- **The criminal poses as the property owner and contacts a real estate agent to list the targeted property for sale, and requests it being listed below current market value to generate immediate interest.**
- **The criminal, posing as the property owner, demonstrates preference for a cash buyer, and quickly accepts an offer.**
- **The criminal, posing as the property owner, refuses to sign closing documents in person, and requests a remote notary signing.**
- **The criminal (or co-conspirator) also impersonates the notary and provides falsified documents to title company or closing attorney.**
- **Title company or closing attorney unwittingly transfers the closing proceeds to criminal.**
- **All communication is electronic, not in person.**

51

Take Precautions

Contact the Seller / Buyer early in the transaction.

Ask the Real Estate Agent or the Lender for the Seller / Buyer contact information.

Confirm the contact information independently…

- Mail the seller at the address on tax records
- Ask the real estate agent if they have personal contact
- Use an ID verification system
- Run the seller email and phone number through a verification program
- Use the public records to compare the seller / buyer signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value
- Conduct additional due diligence as needed

52

WATCH FOR RED FLAGS

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property.
- Has a different address than the owner's address or tax mailing address.
- Refuses or is unable to complete multifactor authentication or identity verification.
- Has no outstanding mortgage or liens.
- The sales price is below market value.
- Purchaser found seller directly through Zillow or similar online real estate marketplace.
- Wants a quick closing, generally in less than a week or two, and may not negotiate fees.
- A cash transaction.

53

WATCH FOR RED FLAGS

- Funds wired to a different state or country than where the seller is purported to be located.
- Wants to use their own notary.
- Wants all documents sent to them at a completely different address that does not match anything in the file.
- Seller's ID photo seems "off, small or further from the camera" -- compare it to: https://www.driverslicenseguide.com/book-us.html
- Seller is only one of the vested owners and attempts to retain control of the closing and does not allow access to the other vested owners or only allows access via email.

54

Mortgage Fraud

United States v. Sterling Bancorp, Inc. (E.D. Mich.)
In April 2023, Sterling Bancorp, Inc., the holding company for its wholly owned subsidiary Sterling Bank & Trust F.S.B. (Sterling), pleaded guilty in the Eastern District of Michigan to one count of securities fraud for filing false securities statements relating to its 2017 initial public offering and 2018 and 2019 annual filings. According to the plea agreement, Sterling originated fraudulent residential mortgages under its Advantage Loan Program in a years-long scheme and then artificially inflated its revenues based upon the program as the bank went public. As part of the resolution, Sterling Bancorp., Inc. agreed that the misconduct caused more than $69 million in losses to non-insider victim-shareholders and agreed to pay more than $27.2 million in restitution. A former managing director of residential lending and two loan officers previously pleaded guilty in connection with the underlying Advantage Loan Program fraud. They currently await sentencing.

55

Report to help fight fraud!

https://www.ic3.gov/ FBI Internet Crime Complaint Center

Local law enforcement

State law enforcement, including the state bureau of investigation and state attorney general

Secretary of State for notary violations

Licensing and Regulatory Affairs – LARA

Forward phishing emails to reportphishing@apwg.org and https://reportfraud.ftc.gov/#/

Phishing text message, forward it to SPAM (7726)

56

FIGHT FRAUD WITH INDUSTRY PARTNERS

Educate real estate professionals in your community, such as county recorders, real estate agents, real estate listing platforms, banks, and lenders.

Host educational events at a local venue.

Alert your title insurance underwriters of fraud attempts.

57

FIGHT FRAUD WITH INDUSTRY PARTNERS

Many of our 83 counties here in Michigan have set up a free service for their property owners to set up an account that notifies them if a document is recorded against their name or property. It's free! Seek out the counties your doing business in to see if they have this product. Prepare a user-guide for your Buyers / Sellers to set this up.

This will help with future fraud and it's FREE.

Great way to market yourselves.

58

FIGHT FRAUD WITH INDUSTRY PARTNERS

Read your Underwriter Bulletins / Memos and Emails

59

MLTA est. 1901
MICHIGAN LAND TITLE ASSOCIATION
Integrity ◆ Responsibility ◆ Service

Thank you

Cindy Immonen, NTP, CLTP, Solutions Provider
VP, Sr. Account Manager
P: 248-331-6860 |E: cindy.immonen@fnf.com

60