

Banking Updates



ROBERT BERGFELD

VICE PRESIDENT & COMMERCIAL RELATIONSHIP MANAGER

ASSOCIATED BANK - NORTH CENTRAL WISCONSIN COMMUNITY MARKET

Discussion



HISTORICAL
RECESSIONS



2023 BANKING
UPDATES



FDIC INSURED
ACCOUNTS



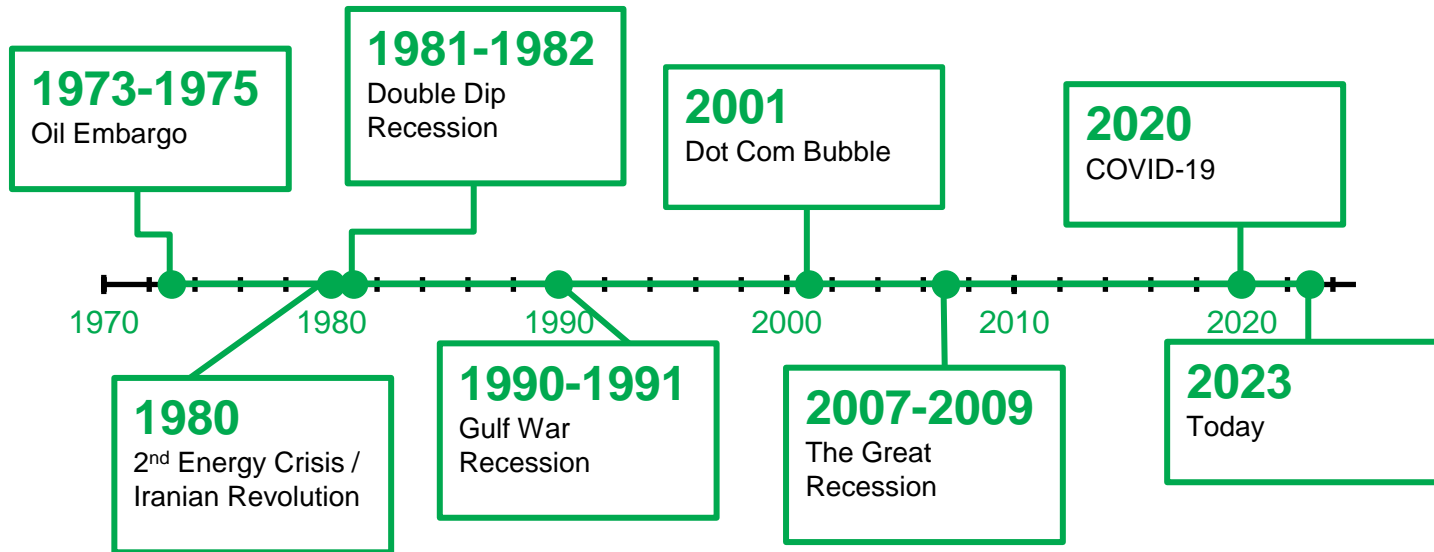
HISTORICAL
INTEREST /
INFLATION



WHAT'S NEXT



50 Year Timeline of Historical US Recessions

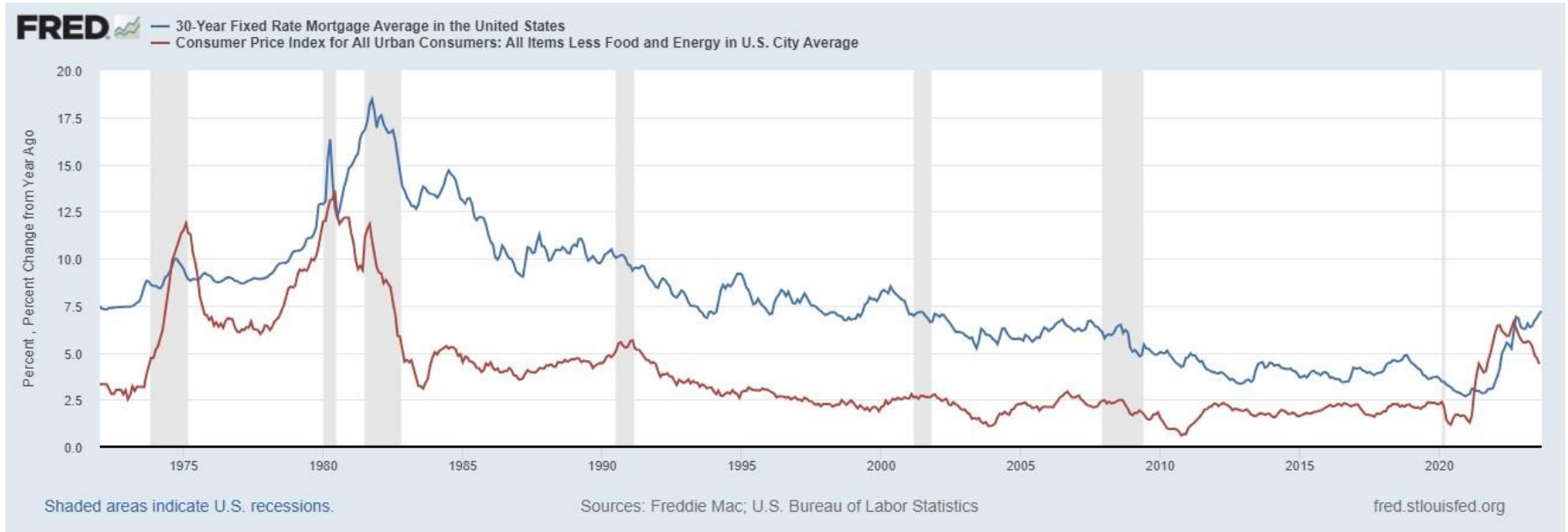


Banking News March 2023 – May 2023



- Silicon Valley Bank (SVB) 3/10/2023 – Impacted by rising rates. Acquired by First Citizens Bank.
- Signature Bank – 3/12/23 - Impacted by SVB. Acquired by New York Community Bank (aka Flagstar).
- Credit Suisse - 3/19/23 - Prior credit structure. Acquired by UBS.
- First Republic Bank – 5/1/23 - Impacted by rising rates. Acquired by JP Morgan Chase

Historical Interest Rates / Inflation

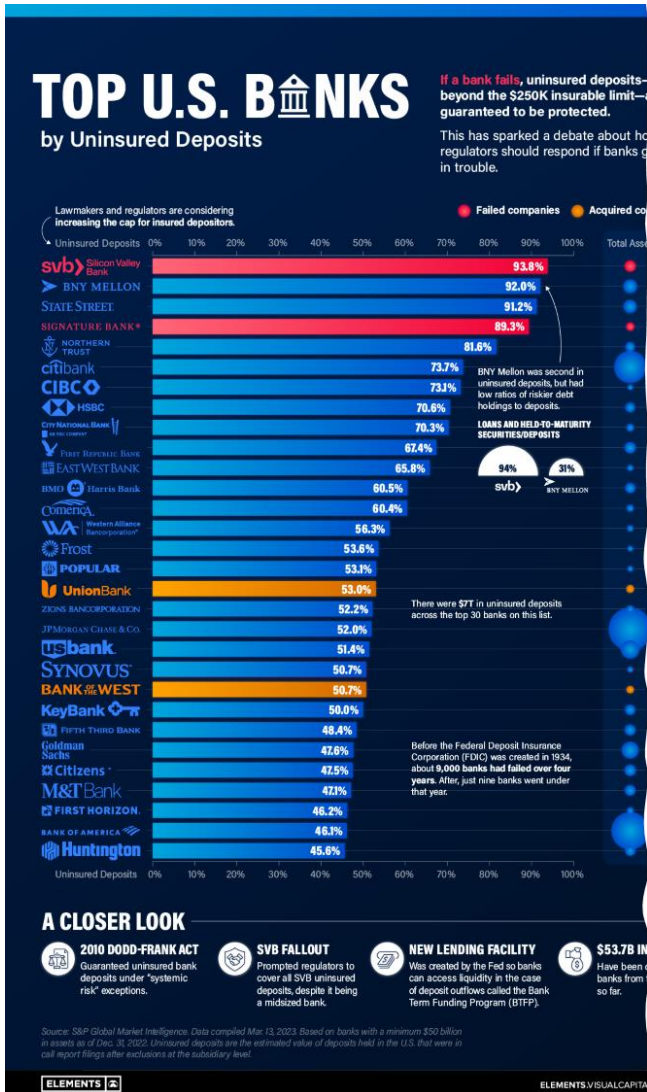


- Blue – 30-year Fixed Rate Mortgages
- Red – Consumer Price Index (CPI) measuring Inflation



What Can You Do?

FDIC – Insured Accounts



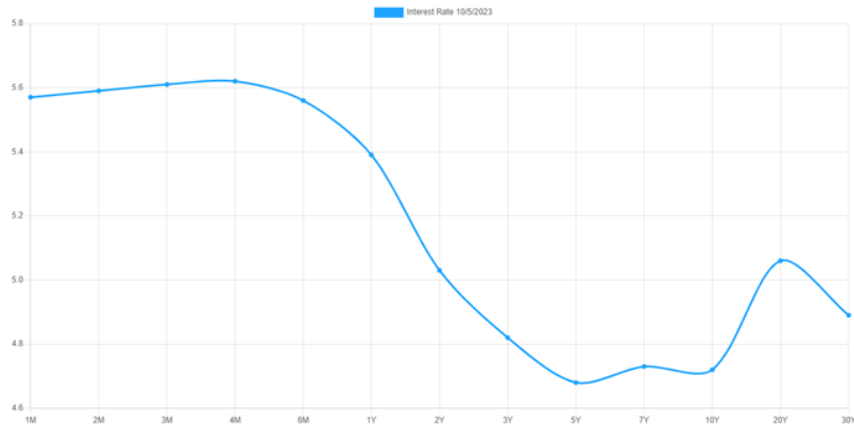
- FDIC Insured for Business Accounts is \$250,000
- Check investment policies
- Ask financial institution on options
 - Collateralized
 - Intra – Fi Sweeps
 - CDARs
- Investment options –
 - US Treasuries (T-Bills)



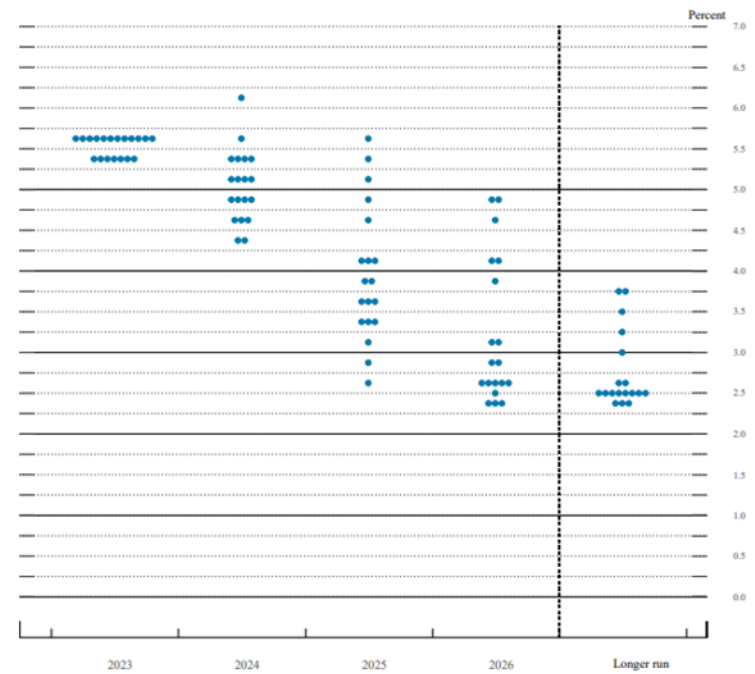
What's Next?



US Treasury Yield Curve – 10/5/23



Fed Dot Plots – 9/20/23





Questions?

Thank you

OPERATIONAL RISKS

FRAUD LOSS

SHELLY LAPOINT

VICE PRESIDENT & SENIOR COMMERCIAL TREASURY MANAGEMENT OFFICER
ASSOCIATED BANK - NORTH CENTRAL WISCONSIN COMMUNITY MARKET



Fraud Topics for Today's Discussion



1. Introduction
2. Fraud Landscape
 - a. Payment Fraud Prevalence by Type
 - b. Internet Crime Report Statistics
3. Types of Check Fraud and Best Practices to Protect Your Business From Fraud Loss
4. Fraud Protection Services Offered by Banks
5. Business Email Compromise and Cyber Fraud
6. Resources and Advice

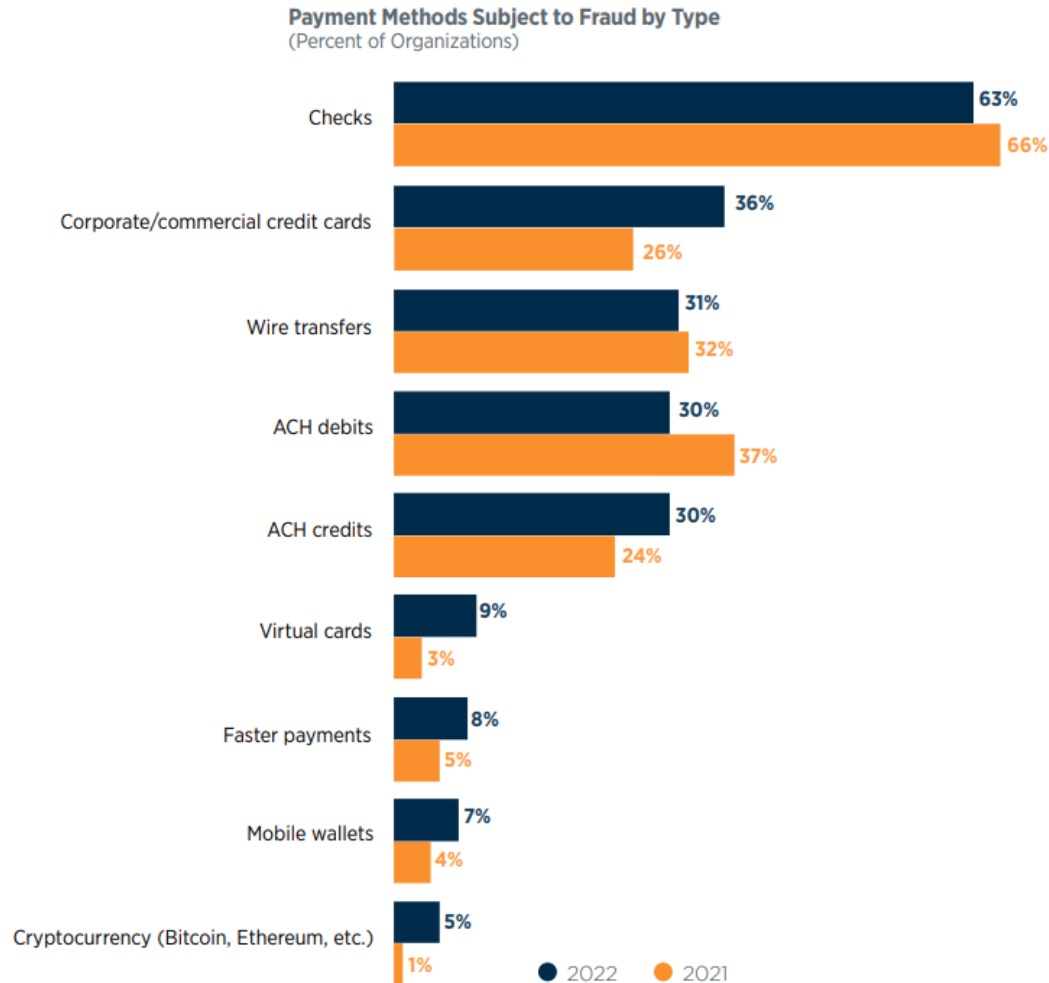


Fraud Landscape



Attempted/Actual Payment Fraud by Type

Checks continue to lead payment fraud attempts for organizations even though the number of checks being issued has declined.



Source: 2023 AFP® Payments Fraud and Control Report |

Internet Crime Report



2022 CRIME TYPES

By Victim Count	
Crime Type	Victims
Phishing	300,497
Personal Data Breach	58,859
Non-Payment/Non-Delivery	51,679
Extortion	39,416
Tech Support	32,538
Investment	30,529
Identity Theft	27,922
Credit Card/Check Fraud	22,985
BEC	21,832
Spoofing	20,649
Confidence/Romance	19,021
Employment	14,946
Harassment/Stalking	11,779
Real Estate	11,727

By Victim Loss	
Crime Type	Loss
Investment	\$3,311,742,206
BEC	\$2,742,354,049
Tech Support	\$806,551,993
Personal Data Breach	\$742,438,136
Confidence/Romance	\$735,882,192
Data Breach	\$459,321,859
Real Estate	\$396,932,821
Non-Payment/Non-Delivery	\$281,770,073
Credit Card/Check Fraud	\$264,148,905
Government Impersonation	\$240,553,091
Identity Theft	\$189,205,793
Other	\$117,686,789
Spoofing	\$107,926,252
Advanced Fee	\$104,325,444



Types of Check Fraud and How to Protect Your Account

Back to the Basics – Check Fraud



Problem

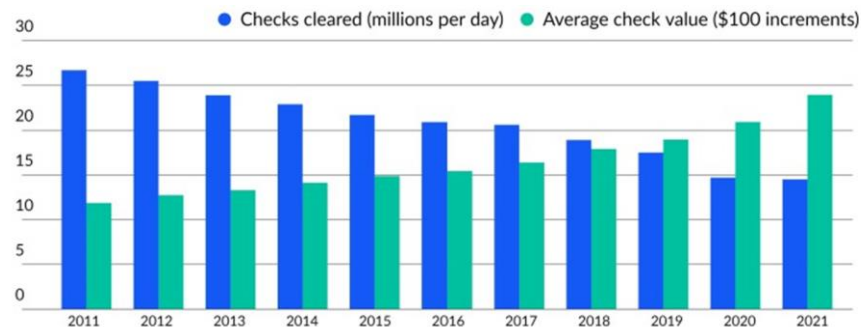
- Per Catalyst Corporate, who represents 1,400 Federal Credit Unions, Check fraud accounted for **66% of payment fraud**, followed by 39% for wire transfers in 2021

FinCEN SAR Statistics

Suspicious Activity Category	Suspicious Activity Type	2014	2020	2021	2022
Fraud	ACH	24,904	143,269	176,911	183,733
	Check	96,786	216,963	349,811	680,000
	Credit/Debit card	75,496	132,925	140,327	269,694

Challenges

- Creating backlogs in check warranty claims
- Availability of funds (Rec CC & Check 21)
- Average check value doubled last decade



Source: Federal Reserve

What's Happening on the Street



Theft of Arrow Key



UNITED STATES POSTAL INSPECTION SERVICE ABOUT CAREERS TIPS & PREVENTION NEWS REPORT

Scam Article

Check Washing

Last updated 05.01.2019 National

Have you ever sent a check that was cashed, but the recipient said it never arrived? You may be the victim of check washing. Check washing scams involve changing the payee names and often the dollar amounts on checks and fraudulently depositing them. Occasionally, these checks are stolen from mailboxes and washed in chemicals to remove the ink. Some scammers will even use copiers or scanners to print fake copies of a check. In fact, Postal Inspectors recover more than \$1 billion in counterfeit checks and money orders every year, but you can take steps to protect yourself.

Check Washing (Identity Theft)

A gang of scammers started an illegal check washing scam to bankroll their drug habit. Watch to learn more about check washing.



Types of Check Fraud

- **Counterfeit checks:** Criminals use printers and desktop publishing software to create counterfeit checks that look legitimate.
- **Altered/washed checks:** Criminals alter the amount or payee on a legitimate check.
 - **What is check washing and how is it used?** Fraudsters steal paper checks sent through the mail, for example, by fishing them from USPS mailboxes or by taking them out of your personal mailbox. They may even rob postal workers in search of checks. Once they have a check you wrote and mailed, for example, to a charity, they use chemicals to “wash” the check in order to change the amount or make themselves the payee. They then deposit your check and steal money from your account.
- **Forged, missing or improper endorsement:** Criminals forge the signature of the authorized signer or use a missing or improper endorsement.



Real Life and Typical Check Fraud Examples

- Check Fraud Example #1 - Non-profit organization who write an average of 10 checks per month
 - A check was confiscated somewhere, we believe in the mail, and altered/washed. The check was cashed/deposited by a fraudster.
 - The organization was not aware the intended payee did not cash the check until the payee called to say they had not received the money.
 - The check had been cashed/deposited by the fraudsters a month before and the money was gone.
 - The organization lost the full amount of the check which was over \$30,000
 - The organization did not have Positive Pay. Positive Pay was implemented after the check fraud loss. **Positive Pay would have prevented this loss.**
- Check Fraud Example #2 - Manufacturing organization writes an average of 200 checks per month
 - A check was confiscated somewhere, we believe in the mail, and altered/washed. The check was cashed/deposited by a fraudster.
 - The organization was not aware the intended payee did not cash the check until the payee called to say they had not received the money over 45 days later.
 - The organization lost the full amount of the check which was over \$15,000.
 - The organization did not have Positive Pay. Positive Pay was implemented after the check fraud loss. **Positive Pay would have prevented this loss.**
 - 30 days after the initial check fraud was discovered the organization experienced a second check fraud attempt. This time the fraudulent check was caught and stopped due to Positive Pay services being implemented. **Positive Pay saved the organization from another loss over \$20,000.**



Central Wisconsin Woman Charged With Mail and Wire Fraud

By Mike Leischner May 19, 2023 | 1:27 PM

A Marshfield woman is accused of stealing thousands of dollars in checks while using personal information to access unauthorized bank accounts.

Court records show Nacirema Frisch is facing 16 counts including mail fraud, bail jumping, wire fraud, and fraud against a financial institution. Investigators say she stole outgoing mail from a business, including checks. She's then accused of using personal information to access accounts that she wasn't authorized on.

Pair accused of stealing mail in third Northeast Wisconsin county

by Brian Kerhin, FOX 11 News
Monday, Jul 10th 2023

The pair are suspected of stealing more than \$600,000 from area businesses by stealing mail, then manipulating the checks and banking information to steal from those accounts.

Investigators find hundreds of stolen pieces of mail; two arrested

March 2022- KIMBERLY — The Outagamie County Sheriff's Office says they have recovered hundreds of pieces of mail with over 100 victims and arrested two people following an investigation into mail theft and financial fraud.



How can you protect your account?

- Understand and be Aware of the Risks
- Minimize the use of Checks
 - Move toward alternative payments
 - ACH & Credit Card
- Timely Reconciliation
 - Best Practiced Include Daily Reconciliation
- Enroll in Positive Pay Services (Prevention)
- The United States Postal Inspection Services also recommends that you:
 - Drop off mail in blue collection boxes before the last scheduled pick-up time or directly at your local Post Office
 - Regularly check your mail. Do not leave your mail in your mailbox overnight



Fraud Prevention Services Offered by Financial Institutions

Powerful Fraud Protection Services



Services Offered by Most Financial Institutions

Check Fraud Prevention

Check Block and Payee Positive Pay

- The Check Block service prevents all check transactions from posting to your accounts.
- Payee Positive Pay service matches information on checks presented to information the company provides their financial institution each time a check is issued. Typical information validated with positive pay service is payee name, check amount and check number.
 - How it works – Organizations provide a file or enter issued check information the banks online banking system. That information is used to match the checks presented for payment.

ACH Fraud Prevention

ACH Blocks and ACH Positive Pay

- The Block service prevents all ACH transactions from posting to your accounts.
- The ACH Positive Pay service then allows you to review all debits posting to an account, sending those previously authorized to be processed while having the ability to return any ACH payments that may have been unauthorized.



Business Email Compromise & Cyber Attacks

The lifecycle of a Business Email Compromise scam*



Business Email Compromise, (BEC), is when an attacker gains access to your company email account and spoofs the owner's identity to defraud.

Step 1

FINDING A LIKELY TARGET



Organized crime groups discern and hone in on a susceptible business. They search the internet for exploitable intel on the company and its executives.

Step 2

GROOMING



Scammers then focus on a company official, testing the waters with phishing emails and/or phone calls. Over a period of days or weeks, they patiently groom and manipulate the contact until they find an opportunity.

Step 3

TAKING THE BAIT



Finally convinced that the offer or opportunity is legitimate, the victim proceeds with the transaction, following the wiring instructions provided by the scammer—and unwittingly opens the door.

Step 4

WIRE TRANSFER



With these funds now in the organized crime group's account, there's a good chance the scammers will go back to their source for more.

*Source: Business E-mail Compromise, Federal Bureau of Investigation, <https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise>



Types of Cyber Attacks

Fraudsters are continuously finding new ways to attack systems, obtain information and/ or money through illicit means

Ransomware Attacks

- Encrypting data and holding it hostage
- Average cost of attack \$133,000, which does not include loss revenue

Phishing/ Social Engineering

- Trick users to provide personal/ private information
- People trick by pretending to be someone else

Malware Attacks

- Infiltrating a system either through email or loophole
- Once in a system, fraudsters can spy on users, block programs, etc

Insider Threats

- Employees leaving data behind on USB drives
- Utilizing same password for business and personal
- 95% of cybersecurity breaches are caused by human error

Additional Protection Services



Cyber Insurance

Cyber insurance is one option that can help protect your business against losses resulting from a cyber attack. If you're thinking about cyber insurance, discuss with your insurance agent what policy would best fit your company's needs,



Resources and Advice



Incident Response Plan

- Prepare for the incident in advance
 - Create your program
 - Provide executive approval
 - Define roles and responsibilities
 - Establish internal communication tree
 - Designate crisis leader with authority to act
- Test your incident response process periodically



Figure 1: Incident Response Lifecycle





Global Cyber Alliance

- Free resources for small business
- GCA Cybersecurity Toolkit for Small Business
 - Know what you have
 - Update your defenses
 - Beyond simple passwords
 - Prevent phishing and malware
 - Backup and recover
 - Protect your email and your reputation

- Find the toolkit at <https://gcatoolkit.org/smallbusiness/>



		4h 0min
TYPE	LEVEL	TIME

CIS Hardware and Software Asset Tracker

Use this spreadsheet to track your hardware, software, and sensitive information.

[View Tool](#) >



Additional Resources

- CISA has several resources:
<https://cisa.gov/cybersecurity>
<https://cisa.gov/stopransomware>
<https://www.cisa.gov/resources-tools/services/web-application-scanning>
- USSS Preparing for a Cyber Incident includes several resources:
<https://www.secretservice.gov/investigation/Preparing-for-a-Cyber-Incident>
- FBI IC3:
<https://www.ic3.gov/>
- FinCEN - Rapid Response Program (RRP):
<https://www.fincen.gov/sites/default/files/shared/RRP%20Fact%20Sheet%20Notice%20FINAL%20508.pdf>
- Associated Bank – Fraud White Paper
https://www.associatedbank.com/pdf/CDTM_White_Paper_Payments_Fraud.pdf

DISCLOSURES



Deposit and loan products are offered by Associated Bank, N.A. Loan products are subject to credit approval and involve interest and other costs. Please ask about details on fees and terms and conditions of these products. Relevant insurance coverage, if applicable, will be required on collateral.

Credit cards are subject to credit approval.

Associated Bank does not charge a fee to download our digital applications; however, transactional fees may apply. Carrier message and data rates may apply; check your carrier's plan for details. Visit AssociatedBank.com/disclosures for Terms and Conditions for your service.

Non-deposit investment products, insurance, and securities are NOT deposits or obligations of, insured or guaranteed by Associated Bank, N.A. or any bank or affiliate, are NOT insured by the FDIC or any agency of the United States, and involve INVESTMENT RISK, including POSSIBLE LOSS OF VALUE. Associated Banc-Corp and its affiliates do not give tax, legal or accounting advice. Please consult with your tax, legal, and accounting advisors regarding your individual situation.

Associated Bank and Associated Bank Private Wealth are marketing names AB-C uses for products and services offered by its affiliates. Securities and investment advisory services are offered by Associated Investment Services, Inc. (AIS), member FINRA/SIPC; insurance products are offered by licensed agents of AIS; deposit and loan products and services are offered through Associated Bank, N.A. (ABNA); investment management, fiduciary, administrative and planning services are offered through Associated Trust Company, N.A. (ATC); and Kellogg Asset Management, LLC® (KAM) provides investment management services to AB-C affiliates. AIS, ABNA, ATC, and KAM are all direct or indirect, wholly owned subsidiaries of ABC. AB-C and its affiliates do not provide tax, legal or accounting advice, please consult with those advisors regarding your individual situation.

Associated Bank has hundreds of locations throughout Illinois, Minnesota, and Wisconsin. Find a location near you. You can also bank with us 24/7 through digital and automated telephone banking and ATMs. Want to speak to a live representative? Call us at 800-236-8866 during our regular customer care hours. Commercial banking clients can call our dedicated business customer care line at 800-728-3501.

All trademarks, service marks and trade names referenced in this material are the property of their respective owners. (08/22) P06739
Investment, Securities, and Insurance Products: Image result for Equal Housing Lender Logo
Associated Bank, N.A. Member FDIC.

CONFIDENTIAL PROPERTY

These materials are the confidential, proprietary materials of Associated Banc-Corp and its affiliates and subsidiaries. External duplication or dissemination of these materials is strictly prohibited.