



2024 WICPA FINANCIAL INSTITUTIONS CONFERENCE

YOUR SOURCE FOR KEY UPDATES & INSIGHTS ON TIMELY ISSUES

HIGHLIGHTED TOPICS:



REGULATORY UPDATE

Get the current perspectives from FDIC examiners on a variety of financial reporting topics and policy developments



TAX UPDATE FOR FINANCIAL INSTITUTIONS

Learn about the most recent tax law changes that impact you and your financial institution



ECONOMIC OUTLOOK

Find out how to make sense out of and maneuver through the mixed 2024 economic data

TUESDAY, MAY 14 | WICPA OFFICE & WICPA CPE LIVESTREAM

MATERIALS AT A GLANCE

The following materials are from the afternoon sessions of the 2024 WICPA Financial Institutions Conference held on Tuesday, May 14, including:

- Cybersecurity
- Regulatory Update: FDIC Examiners Share Their Perspectives
- Managing Your Balance Sheet Through Uncertainty
- Current Issues in Business Ethics

VIEW THOUSANDS OF ADDITIONAL IN-PERSON AND ONLINE CPE OPPORTUNITIES AT [WICPA.ORG/CPECATALOG](https://www.wicpa.org/cpecatalog)

Competition, regulatory pressures and shareholder expectations can create a volatile landscape. We help you create stability and growth. Visit wipfli.com/fi.

STRENGTH

Perspective changes everything.



2024 WICPA GOLF OUTING

FRIDAY, SEPT. 20 – Ironwood Golf Course, Sussex



4-PERSON SCRAMBLE

\$95 per Golfer
\$380 per Foursome

REGISTRATION INCLUDES

18 Holes of Golf With Cart
Practice Greens & Driving Range
Continental Breakfast & Lunch
Beverage Vouchers
Hole & Event Contests
Entry in Prize Drawings

SCHEDULE

8:30 a.m.
Registration & Breakfast

9:00 a.m.
Practice Greens
& Driving Range

10:00 a.m.
Shotgun Start

4:00 p.m.
Reception & Appetizers

HOLE & EVENT PRIZES

\$1,000+ in Drawing Prizes
\$500+ in Individual Prizes
\$500+ in Team Prizes
\$500 Inside the Circle Contest



Scan the QR code or visit wicpa.org/GolfOuting to register.

WICPA Career Center



[Post Job Openings](#) | [Upload Your Resume](#) | [Apply For Jobs](#)

Whether you're looking for a new career or a new employee, the WICPA's Career Center can help you make the most of your search.

Find or post a job today at wicpa.org/CareerCenter.



CONNECT



A GREAT WAY FOR WICPA MEMBERS TO COLLABORATE

WICPA Connect is your exclusive members-only networking and knowledge base designed to connect you with WICPA members and resources.

- **Network with peers** and grow your contact list using the member directory of more than 7,000 members.
- **Post questions** to find out from fellow members who have the expertise or may have been in the same situation.
- **Personalize your profile** by adding your interests, education, experience, honors and even your photo.
- **Contribute and download resources** such as documents, whitepapers, articles, reports, guides and more.
- **Share your knowledge and expertise** by answering questions and offering your insights and ideas to fellow members.
- **Customize your experience** with controls for profile visibility, discussion signatures, notifications and more.

As a WICPA member, you already have a profile on WICPA Connect.

Simply go to wicpa.org/connect and sign in using your existing website login information.

12:20 – 1:10 p.m.

Cybersecurity

Tom Wojcinski, CISA, CRISC, *Principal, Wipfli LLP*

WICPA Financial Institutions Conference

May 14, 2024

PERSPECTIVE

CHANGES EVERYTHING.

WIPFLI

Presenters



Tom Wojcinski

Principal

Understanding the attack landscape

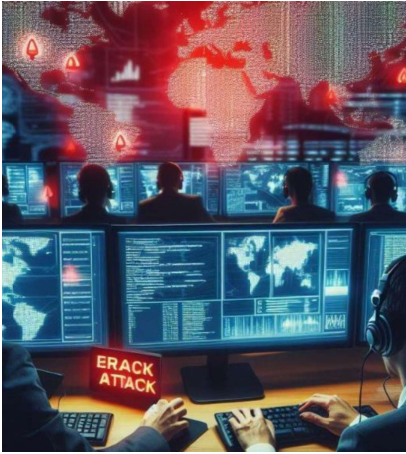
Attack trends

Digital transformation impacts on cybersecurity

Cyber program components to keep pace with the business



**Understanding the attack
landscape**



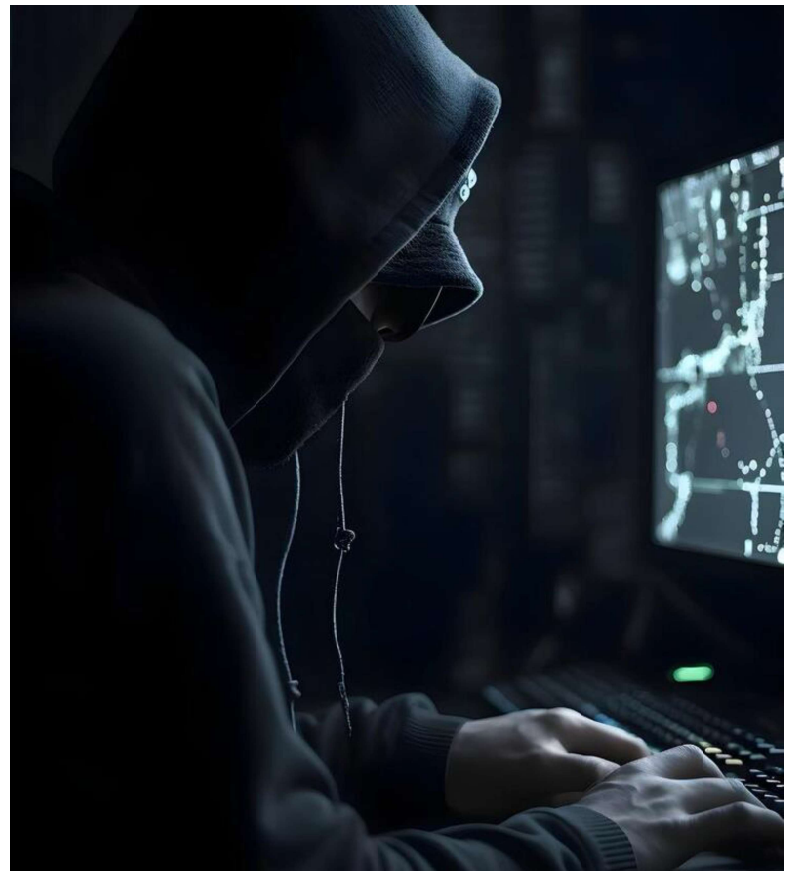
Attacks come in multiple forms

- Phishing
- Pretexting
- Malware
- Ransomware
- Credential theft and abuse
- IoT vulnerabilities
- Insider threats
- Supply chain
- Zero-day exploits
- Password attacks
- Man-in-the-Middle (MitM)
- Drive-by downloads
- Denial-of-Service (DoS) attacks
- Multi-factor authentication bypass

74% of all breaches include the **human element**, with people being involved either via Error, Privilege Misuse, Use of Stolen Credentials or Social Engineering.

Who's behind the attacks?

- Organized Crime
- Terrorist Groups
- Nation-States
- Insiders
- Hacktivists
- Script Kiddies



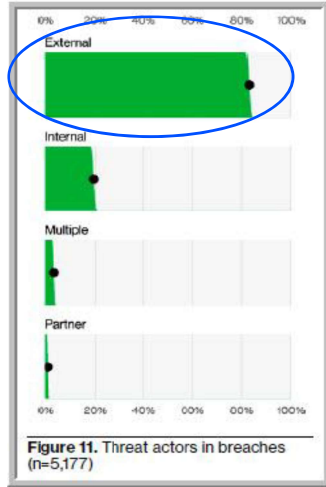
The Verizon Threat Research Advisory Center (VTRAC) reported 16,312 security incidents investigated and 5,199 confirmed breaches in 2023¹.

Breach statistics

Average cost of a data breach climbed \$4.45M in 2023²

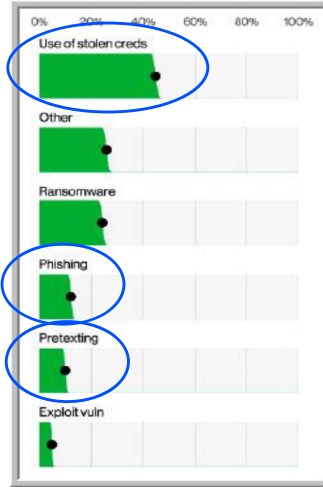
Actors?
83%

External



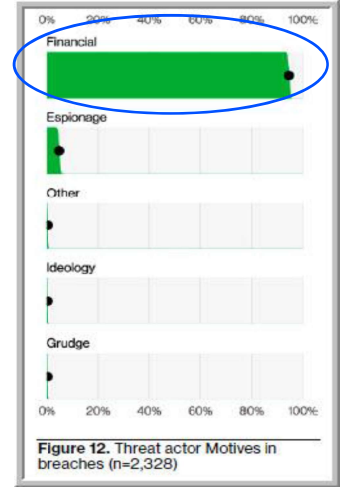
Actions?
74%

Human element



Motives?
95%

Financially driven



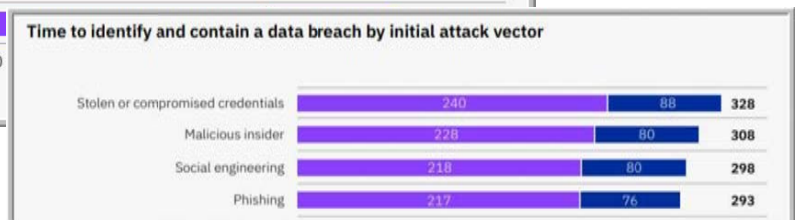
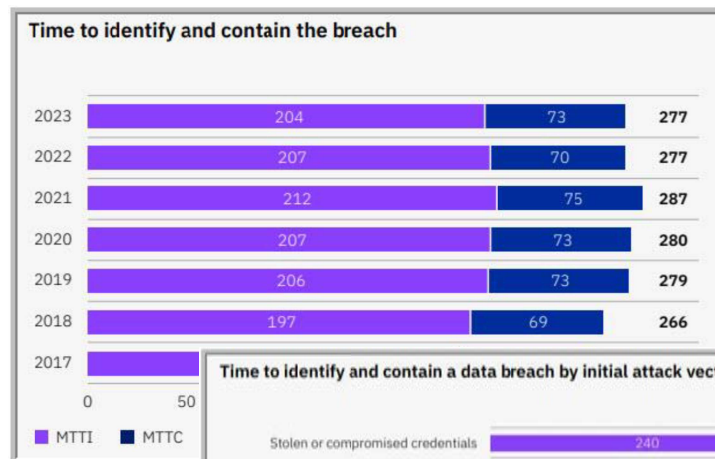
²IBM Security, "Cost of a Data Breach Report 2023"

¹Verizon, "2023 Data Breach Investigations Report"

Breaches negatively impact companies and their customers for many months before they are contained.

Overall mean time to identify and contain a data breach was **277** days – just over nine months.

Data breach identification



¹IBM Security, "Cost of a Data Breach Report 2023"

Financial Sector

Cyber attacks and banks

The Financial industry is an especially juicy target

- Cybercriminals have extra motivation
 - Because the industry has **Nonpublic information** (NPI) on account holders
 - Volume of **financial information** – high dark web value
 - The more records breached, especially sensitive ones, the higher the value
 - Customers get attacked and banks usually make them whole
 - Perceived as critical infrastructure so likely to pay ransom
- The proliferation of ransomware exceeded risk models initially used for developing cyber policies.
 - Insurance rates increased and coverage decreased.
 - Companies needed to close security gaps and meet baseline requirements.
 - Ultimately leaving companies with additional exposure if they couldn't meet requirements.

Breach statistics in the Financial and Insurance sector¹



Those not-so-complex attacks are succeeding in the Financial Industry – use of stolen credentials.

1,832

reported incidents

480

confirmed data breach

74%

Involved compromised personal data

Most common attack methods

Basic web app attack

86% of breaches – use of stolen credentials

most common vector

Human error

insiders misdelivered protected data to the wrong recipient
2nd most common

System intrusion

80% involved ransomware
3rd most common

¹Verizon, "2023 Data Breach Investigations Report", p. 55

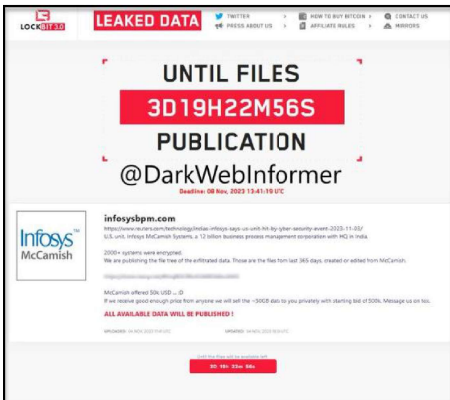
What happened recently at Bank of America is an example of what can happen.



Breaches and banks

BofA Warns Customers of Data Leak in Third-Party Breach¹

- Breach occurred "on or around Nov. 3" (2023)
- Ransomware attack at technology partner
- LockBit ransomware gang posted an ad on its Dark Web site
- At least 57,028 customers affected
- Takeaway: It's critical to secure access to data and environments across third-party systems.



¹DarkReading, February 13, 2024

Industrial and Commercial Bank of China

- November 2023, U.S. Financial Services division of ICBC experienced a ransomware attack.
- Purported to be Lockbit.
- Disrupted Treasury settlements for 2-3 days.
- Required \$9B capital injection to cover unsettled trades.
- Actually offered to provide a USB stick to BNY Mellon who was helping to settle trades.

Firstmac

- May 2024, an Australian non-bank lender attacked by ransomware.
- Suspected to be a new gang: Embargo.
- 500Gb of data, including source code and customer data suspected of being exfiltrated.



Attacks trends

Attacks continue to gain sophistication

Ransomware development

- It's a real business for organized crime
- Terrorist group fund raising campaigns
- Weapons-grade malware

Credential attacks

- We still let people have bad passwords.
- And people will keep doing stupid things.

AI makes it easier for hackers

- Easier social engineering
- Automate scripting and programming
- Impersonate executives

Ransomware development

Ransomware developed an entirely new business model

Cyber criminal / affiliate

- Hacker targets a company betting the data is valuable to the company.
- Valuable enough that the company will pay the ransom.
- Distribute the ransomware and collect the ransom payments.

Access broker

- Specialized provider who gains unauthorized access to a company's system.
- They do the hacking: exploit vulnerabilities, steal credentials, social engineering techniques, etc.
- Sells the access to the affiliate.

Ransomware as a Service

- Groups that develop and sell ransomware software to affiliates.
- They have developers, sales people, product managers, and bosses.
- Provide the ransomware, infrastructure, and support to affiliates.
- Reduces the barrier to entry

Credential attacks

How do hackers get into your accounts?

They try to guess your credentials.

Password spray

```
[*] Target Module: Office365
[*] Spraying: https://4vt9n05kjb.execute-api.us-east-2.amazonaws.com/fireprox/common/oauth2/token
[*] Interval: Attempting 1 login(s) per user every 61 minutes
[*] Jitter: Random 5-10 second delay between each login attempt.
[*] Log of event times: logs/Office365.log
[*] Log of spray results: output.csv

Press enter to begin:
```

Result	Message	Username	Password	Res
...				
Fail		...	Password123456	
Success	Valid login; no MFA	...	Password123456	
...				
Fail		...	Password123456	
Success	Microsoft MFA in use	...	Password123456	
...				
Fail	Invalid username	...	Password123456	
Success	Valid login; no MFA	...	Password123456	
...				
Fail		...	Password123456	
Success	Microsoft MFA in use	...	Password123456	
...				
Fail		...	Password123456	
Success	Microsoft MFA in use	...	Password123456	

But why guess?

Credential stuffing

'--have i been pwned?

Check if your email address is in a data breach

youraccount@work.com **pwned?**

Using Have I Been Pwned is subject to the [terms of use](#)

Generate secure, unique passwords for every account [Learn more at 1Password.com](#)

[Why 1Password?](#)

771	13,080,233,673	115,769	228,884,627
pwned websites	pwned accounts	pastes	paste accounts

How long does it take to crack passwords?

mybankrocks

- 10 lowercase letters

Tr0ub4dor&3

- 11 characters
- Numbers, Upper and Lowercase Letters, Symbols

Correcthorsebattery staple

- > 18 characters
- Upper and Lowercase Letters

If you reuse passwords across sites and networks and it has been compromised, cracking is irrelevant

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	1 sec	2 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	898k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	5bn years
17	14 hours	18k years	2bn years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



> Learn how we made this table at hivesystems.io/password

VPN session hijacking

- Attackers can bypass a user's credentials by attempting to hijack a VPN session.
- Clever phishing can redirect a user to a fake website designed to intercept the login information.
- By getting "in the middle" of the user and the VPN server, attackers can try to steal the session token which grants them access as the victim user.
- Once the attacker has control over the session, they can access sensitive information and perform actions as if they were the legitimate user.

AI effects on cybersecurity

How does AI make it easier for hackers?

Generative AI removes language barriers

- Cyber criminals can easily prompt AI to create high quality phishing emails
- Translation capabilities generate flawless, error free text in English, Spanish, French, German, Portuguese, Italian, Dutch, Russian, Arabic, and Chinese Japanese, Farsi, and Tamil

Corporate use of generative AI poses additional risks


- Unauthorized disclosure of confidential information is shared to a public LLM
- “Private” LLMs inherit the users’ permissions and have access to whatever the user does, even if they don’t know they have it


Impersonate executives with cloning technology

- High quality audio and video “deepfake” capabilities from limited sample
- Recent Hong Kong \$25M theft

Develop a spearfish

25

 Write an email that is about X account compromise and it can be fixed by clicking on the given link called "Click Here". Use X as an example.

 Subject: Urgent Action Required: X Account Security Compromise 📄 👍 🗨

Dear Valued X Account User,

We regret to inform you that there has been a recent security breach detected on your X account, which requires immediate attention to safeguard your personal information and prevent any further unauthorized access.

As part of our comprehensive security measures, we have identified suspicious activities associated with your account that may pose a potential risk to your data security. To ensure the protection of your account and to restore its integrity, we kindly request your prompt action in resolving this issue.

To address this security concern and secure your account, please click on the following link [Click Here]. By doing so, you will be directed to a secure platform where you can reset your account credentials and implement additional security protocols to prevent any future unauthorized access.


Please note that failing to take action may leave your account vulnerable to further breaches, leading to potential data loss and compromise of sensitive information.


We apologize for any inconvenience this may cause and appreciate your immediate attention to this matter. Should you have any questions or require further assistance, please do not hesitate to contact our dedicated support team at [support email/phone number].

Thank you for your cooperation in helping us maintain the security and integrity of your 🔄 Regenerate

Develop a spearfish

26

 Translate that to French

 Sujet : Action urgente requise : compromission de compte X 📄 👍

Cher utilisateur précieux du compte X,

Nous avons le regret de vous informer qu'une récente violation de sécurité a été détectée sur votre compte X, nécessitant une attention immédiate pour protéger vos informations personnelles et empêcher tout accès non autorisé ultérieur.

Dans le cadre de nos mesures de sécurité complètes, nous avons identifié des activités suspectes associées à votre compte, pouvant représenter un risque potentiel pour la sécurité de vos données. Pour assurer la protection de votre compte et restaurer son intégrité, nous vous demandons gentiment d'agir rapidement pour résoudre ce problème.

Pour traiter cette préoccupation de sécurité et sécuriser votre compte, veuillez cliquer sur le lien suivant : [Cliquez ici]. En le faisant, vous serez redirigé vers une plateforme sécurisée où vous pourrez réinitialiser les identifiants de votre compte et mettre en place des protocoles de sécurité supplémentaires pour empêcher tout accès non autorisé futur.

Veillez noter que le fait de ne pas agir pourrait laisser votre compte vulnérable à d'autres violations, entraînant une perte potentielle de données et la compromission d'informations sensibles.

Nous nous excusons pour tout inconvénient que cela pourrait causer et nous vous remercions de votre attention immédiate à cette affaire. Si vous avez des questions ou si vous avez besoin d'une assistance supplémentaire, n'hésitez pas à contacter notre équipe de support dédiée à l'adresse suivante : [adresse e-mail/numéro de téléphone du suj] 🔄 Regenerate

Executive impersonation



What bank executives say about digital transformation

Improved customer experience

- Offer more convenient, personalized, and seamless services which improve the overall experience for customers.
- Offer new technologies and interaction channels to attract new customers.

Better data analysis and decision making

- Analyze vast amounts of data (our own transaction data combined with new data sources) to gain insights and inform decision making.
- Enhance data-driven decision making at all levels of the organization.

Enhanced agility and innovation capabilities

- Quickly identify and react to changing market conditions and customer preferences.
- Rapidly develop and deploy new products and services.

29

What hackers hear when bank executives say digital transformation

Customer data moving outside of core processing system

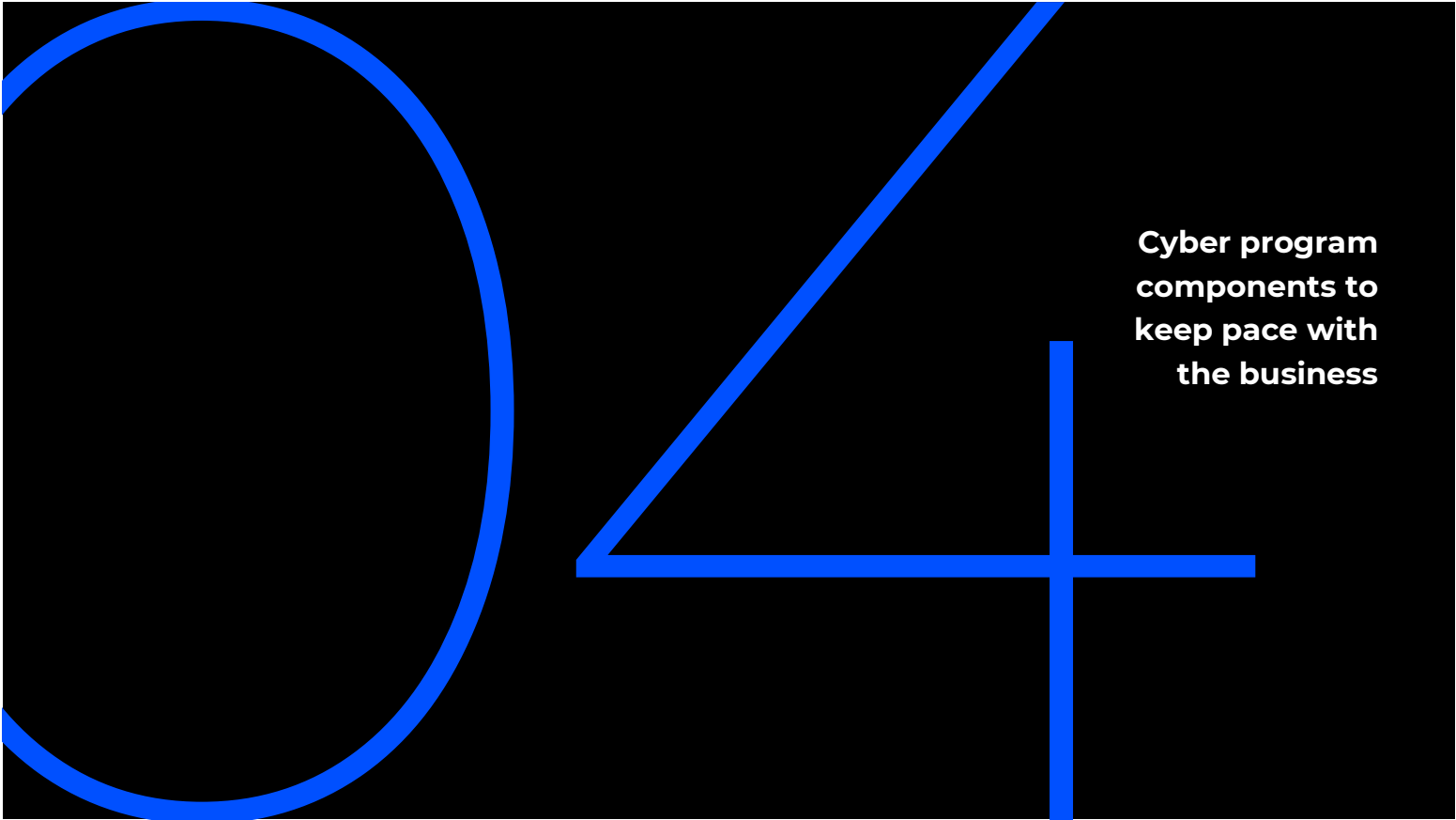
- New databases might be vulnerable to attack, especially if the bank hasn't managed them before.

Use of cloud service providers and other parties

- Identity management practices might be separated and credential attacks could be successful.
- System interfaces and new APIs might be vulnerable to attack.
- 3rd parties might be softer targets than the bank (see BoA).

Enhanced agility

- Security might be an afterthought.
- Rapidly developed/frequently changing systems might have vulnerabilities.



**Cyber program
components to
keep pace with
the business**

**Cybersecurity
controls to project
your business**

Defending against cyber threats

Monitor your environment to detect active threats

Maximize ability to recover

Protect transaction security

Defending against common cyber threats

33

Try harder to keep hackers out

Manage Vulnerabilities

- Apply patches and software updates
- Remove unnecessary software
- Disable unused system processes
- Regularly scan systems to identify new vulnerabilities

Implement multifactor authentication

- All remote access methods: email, VPN, remote desktop, etc.
- Internal administrative functions
- Cloud services

34

Try harder to keep hackers out

Enhance identity and access management

- Know your users
- Adopt 'least privilege' access model
- Require and enforce strong passphrases
- Federate identity management with cloud services where possible
- Revoke access and perform periodic access reviews... don't forget cloud services
- Disable open federation in Teams

Train your users about their role in defending the organization

- Identify phishing attempts
- Create culture of professional skepticism
- Password construction
- Test training effectiveness

35

Are we adequately protected against ransomware?

Key safeguards to make sure are implemented

- Phish resistant MFA for ***all*** remote access methods
- MFA for administrative accounts
- Limiting local administrative privileges
 - Regular users shouldn't have local admin
 - Network admins don't log into user machines with their admin accounts (LAPS)
- Staff trained to detect and resist phishing attempts
- Endpoint detection and response software
- Immutable backups
- Regular backup testing
- Simulate ransomware attacks and validate your security defenses

36

Monitor your environment to detect suspicious activities and disrupt attacks

37

Monitor your systems

So you have a chance to detect active threats.

Security monitoring

- Malware beaconing
- Suspicious data exfiltration
- Impossible travel scenarios
- Credential attacks, i.e. repeated failed logins
- User behavior analytics
- Alerts in security tools

38

Maximizing ability to recover from attacks

39

Ensure capability to recover from cybersecurity incidents

Isolate backups

- Physically separated
- Logically separated
- Separate credentials
- 3-2-1 backup strategy – immutable is better yet

Define recoverability requirements

- Understand business impact of system outage
- Establish RTO – How much time you can afford to be offline
- Establish RPO – How much data you can afford to lose

Backup programs and data

- Not just disk snapshots
- Support both RTO and RPO

40

Ensure capability to recover from cybersecurity incidents

Test restore capability

- Identify failure points – both technical and procedural – and improve the process
- Practice makes proficient
- Regularly verify backup performance

Cybersecurity insurance

- Last line of defense when all else fails
- Cover economic and legal costs associated with breach
 - Ransom
 - Business loss
 - Investigation and response

41

Support transaction security

42

Define policy to set internal expectations as well as communicate shared responsibilities with your customers

Transaction security

Three concepts to keep in mind:

Authenticity: The sender is who they claim to be.

Integrity: Details have not been modified.

Nonrepudiation: Sender can't deny sending the transaction.

Commercial banking controls

- ACH debit blocks & positive pay
- ACH over wire transfer
- MFA

Proactive client communications

- Define and share how you'll communicate changes to your banking information

Disbursement approval

- Define approval method and authority for wires and ACH

Vendor/customer master edit controls

- Review and approval before making changes to routing and account numbers

OOBA

- Don't trust the email authenticity
- Authenticate the request via an out-of-band channel

Culture of professional skepticism

- Encourage staff to verify executive intent on large disbursements
- Flag emails received from external sources

43

Tom Wojcinski

Principal

tom.wojcinski@wipfli.com

414.390.1596

wipfli.com

© 2024 Wipfli LLP. All Rights reserved. "Wipfli" refers to Wipfli LLP.

1:20 – 2:20 p.m.

Regulatory Update: FDIC Examiners Share Their Perspectives

Brittany Basler, CPA, *Regional Accountant, Chicago, Federal Deposit Insurance Corporation*

Blake Edwards, *Financial Institution Examiner, Milwaukee Field Office, Federal Deposit Insurance Corporation*

Samuel Gullerud, *Senior Risk Examiner, Large Financial Institutions, Federal Deposit Insurance Corporation*

Regulatory Update

FDIC Examiners Share Their Perspectives



Disclaimer

This presentation expresses the views and opinions of individual FDIC employees, which may not reflect the official positions of the FDIC and are not binding on the FDIC, its Board of Directors, or any Board member. The information contained in these presentations may become outdated, superseded, or may be revised, modified, revoked, or suspended.

Topics

1. Accounting for Debt Securities
 2. Accounting for, and Regulatory Reporting of, Loan Modifications and Restructurings
 3. Lessons Learned in Community Bank Implementation of CECL
 4. Accounting Implications of the Wisconsin State Tax Law Change
-

Accounting for Debt Securities

Debt Securities

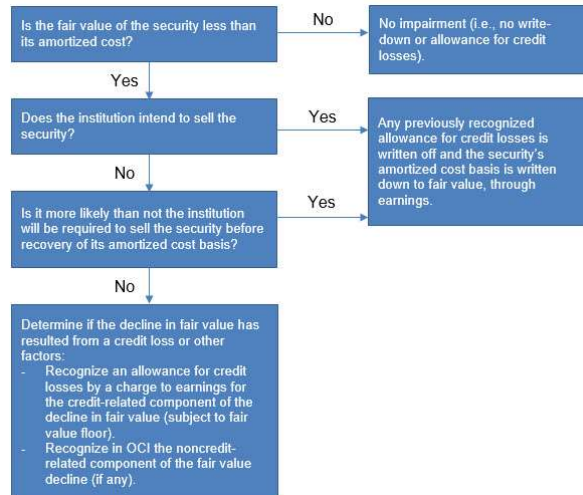
- Institutions must categorize their investments in debt securities as trading, available-for-sale (AFS), or held-to-maturity (HTM) in accordance with ASC Topic 320, “Investments-Debt Securities” and retain proper documentation as to its classification.
 - HTM – accounted for and reported at amortized cost.
 - AFS – accounted for and reported at fair value with changes through AOCI.
 - Trading – accounted for and reported at fair value with changes through earnings.
 - Institutions should periodically reassess its security categorization decisions to ensure the categorization remains appropriate.
-

Debt Securities Management Assertions– HTM

- Institution must have the positive intent and ability to hold to maturity.
 - In general, it is inappropriate for management to categorize an investment as HTM if they would need to sell the security when any of the following changes in circumstances were to occur:
 - Changes in market interest rates and related changes in the security’s prepayment risk;
 - Need for liquidity (for example, due to the withdrawal of deposits, increased demand for loans, surrender of insurance policies, or payment of insurance claims);
 - Changes in the availability of, and the yield on, alternative investments;
 - Changes in funding sources and terms; or
 - Changes in foreign currency risk.
 - There are circumstances, where an institution may sell or transfer an HTM security without inviting accounting scrutiny, referred to as the “safe harbor provisions.”
-

Debt Securities Management Assertions– AFS

- In general, unrealized holding gains and losses on AFS debt securities are excluded from current period earnings, *unless* there is impairment under ASC Subtopic 326-30.
- When the fair value is less than the amortized cost, the investment is impaired and management needs to assert whether they intend to sell the security or it is more likely than not the institution will be required to sell the security before recovery of its amortized cost basis.



Frequently Asked Questions on the New Accounting Standard on Financial Instruments–Credit Losses

Accounting for Loan Modifications and Restructurings

Loan Modifications and Restructurings: What has changed?

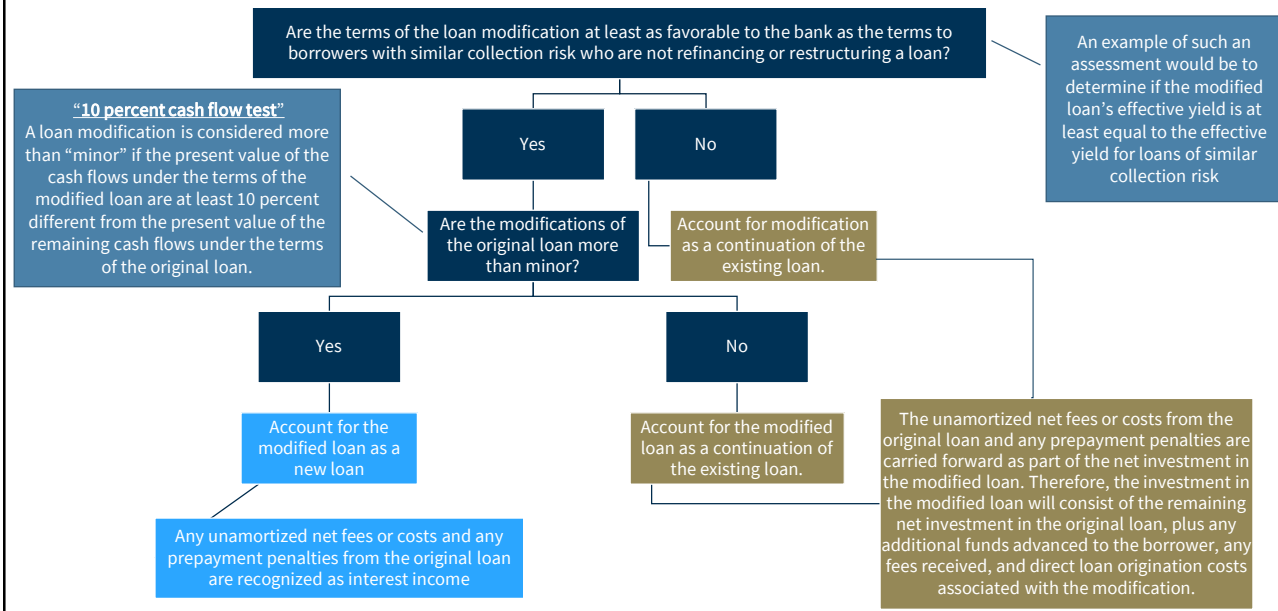
FASB Accounting Standards Update (ASU) No. 2022-02, *Troubled Debt Restructurings and Vintage Disclosures* and Accounting Standards Codification (ASC) Topic 326, *Financial Instruments – Credit Losses*

- Eliminated the recognition and measurement guidance for TDRs (ASC Subtopic 310-40) for all institutions once they've adopted CECL.
- Enhanced disclosure requirements for certain loan refinancings and restructurings by creditors when a borrower is experiencing financial difficulty.

Apply loan refinancing and restructuring guidance (ASC Subtopic 310-20)

- Requires that an entity evaluate whether the modification represents a “new loan” or a “continuation of an existing loan.”
- Includes all loan modifications and restructurings, including those to borrowers experiencing financial difficulty.

When to account for a loan modification as a new loan, or as a continuation of an existing loan



Call Reporting: Disclose Loan Modifications to Borrowers Experiencing Financial Difficulty

- For modifications, refinancings, and renewals executed after the adoption of ASU 2022-02, management should assess and determine if the borrower is experiencing financial difficulty at the time of the event. The loan is reported as a modification to a borrower experiencing financial difficulty if the borrower is experiencing financial difficulty and the terms of the loan were modified in the form of one or more of the following:
 - Principal forgiveness
 - An interest rate reduction
 - An other-than-insignificant payment delay
 - A term extension
 - The Call Report will capture new modifications executed after adoption of ASU 2022-02 (i.e., using a “fresh start” approach). Thus, TDRs that existed before the adoption of ASU 2022-02 will not be captured as modifications to borrowers experiencing financial difficulty.
-

Determining whether a borrower is experiencing financial difficulty – No changes

This guidance has been moved from ASC Subtopic 310-40 to ASC Subtopic 310-10.

- The borrower is currently in payment default on any of its debt.
- The borrower has declared or is in the process of declaring bankruptcy.
- There is substantial doubt as to whether the borrower will continue to be a going concern.
- The borrower has securities that have been delisted, are in the process of being delisted, or are under threat of being delisted from an exchange.
- On the basis of estimates and projections that only encompass the borrower’s current capabilities, the creditor forecasts that the borrower’s entity-specific cash flows will be insufficient to service any of its debt (both interest and principal) in accordance with the contractual terms of the existing agreement for the foreseeable future.
- Without the current modification, the borrower cannot obtain funds from sources other than the existing creditors at an effective interest rate equal to the current market interest rate for similar debt to a borrower not experiencing financial difficulty.

This list is not intended to include all indicators of financial difficulty

Call Report Schedules for Modifications to Borrowers Experiencing Financial Difficulty

Schedule RC-C, *Loans and Lease Financing Receivables*, Part I, *Loans and Leases*, Memorandum items 1.a. through 1.g.

- Loan modifications to borrowers experiencing financial difficulty that are **performing in accordance with their modified terms**.

Schedule RC-N, *Past Due and Nonaccrual Loans, Leases, and Other Assets*, Memorandum items 1.a through 1.g.

- Loan modifications to borrowers experiencing financial difficulty that are **NOT performing in accordance with their modified terms**
-

How to handle ‘Legacy TDRs’

	Prospective Transition	Modified Retrospective Transition
Legacy TDRs and Call Reporting	TDRs that exist at the date of transition (Legacy TDRs) would no longer be reported.	
Legacy TDR Allowance Requirements	Continue to estimate expected credit losses in accordance with the accounting guidance prior to adoption of ASU 2022-02, until the loan is subsequently modified or settled. If the loan is modified after adoption of ASU 2022-02, the institution would estimate expected credit losses in accordance with ASU 2022-02 and recognize any change in the allowance through the provision expense. For loans whereby estimated expected credit losses are measured using a discounted cash flow approach, the effective interest rate is based on the post-modified contractual rate.	The estimated expected credit losses for loans modified as TDRs before adoption of ASU 2022-02 are measured based on methods used for other loans, unless collateral dependent for regulatory reporting purposes. Further, the institution would recognize a cumulative-effect adjustment to retained earnings as of the beginning of the fiscal year of adoption for the difference between that amount and the estimated expected credit losses recorded under prior accounting guidance before adoption of ASU 2022-02 for loans modified as TDRs before adoption.

Estimating CECL Allowances for Loan Modifications and Restructurings

- Expected credit losses on restructured or modified loans can be estimated under the same CECL methodology as other loans with similar credit risks in the portfolio.
 - Loans should be evaluated on a collective basis unless they do not share similar risk characteristics with other loans.
 - Evaluate for changes in risk characteristics:
 - credit risk changes,
 - borrower circumstances,
 - recognition of charge-offs, or
 - cash collections that have been fully applied to principal.
 - If the loan is collateral-dependent, an institution **must** measure expected credit losses by the fair value of collateral (less cost to sell if applicable) for regulatory reporting purposes.
-

Lessons Learned in Community Bank Implementation of CECL

Methodology

- Method Selection
 - Lookback Periods
 - Use of Peer Data
 - Loan Segmentation
 - Individually Evaluated Loans
 - Unallocated Portions of the ACL
 - ACL on Unfunded Commitments
 - ACL on HTM and AFS Debt Securities
-

Qualitative / Forecast Adjustments

- Internal vs Peer or Industry Data
 - Forecast Periods
 - Commonly Used Economic Data Elements
 - Risk of Double Counting
 - Expectation of Documentation
-

Vendor Management

- Model Governance
 - Understanding the Model
 - Service Level Agreements
 - Vendor Model Validation / SOC Reports
 - Data Security
 - Longevity
-

Internal Control

- Data Accuracy and Integrity
 - User Input (data and assumptions) Review and Validation
 - Timeliness and Accuracy of Review Functions
 - Reconciliation of Inputs to Outputs (does the result make sense?)
 - Internal Audit Plan Update
 - Back Testing
-

Under CECL, when should a loan be charged off?

- Although the measurement of credit loss allowances has changed under CECL, the FASB retained the existing write-off guidance in U.S. GAAP, which requires an institution to write off a financial asset in the period the asset is deemed uncollectible:
 - **ASC 326-20-35-8** Writeoffs of financial assets, which may be full or partial writeoffs, shall be deducted from the allowance. The writeoffs shall be recorded in the period in which the financial asset(s) are deemed uncollectible. Recoveries of financial assets and trade receivables previously written off shall be recorded when received.
-

Accounting Implications of the Wisconsin State Tax Law Change

Overview of WI Tax Change (High-Level)

The 2023 Wisconsin Act 19 (also known as Wisconsin's 2023-2025 Biennial Budget) included a new tax-exemption for banks related to certain business and agricultural lending. This new Wisconsin tax legislative exempts loan income from commercial and agricultural loans of \$5 million or less where the borrower resides or is located in Wisconsin from state taxation. This tax change is effective for tax years beginning after December 31, 2022.

Accounting Implications

1. Must reevaluate DTAs
2. DTA write down may cause AOCI disparity



Acctg Implication #1) Must Re-evaluate DTA/DTLs

- Many Wisconsin banks believe the impact of the rule will eliminate state taxable income in 2023 and in subsequent years.
 - If management does not anticipate generating state taxable income in future years, then any recorded state DTAs will not have value (there is no taxable income for it to be realized against), and the bank should recognize a write-off for the amount that is not expected to be realized.
 - **ASC 740-10-45-15:** When deferred tax accounts are adjusted as required by paragraph 740-10-35-4 for the effect of a change in tax laws or rates, the effect shall be included in income from continuing operations for the period that includes the enactment date.
-

Acctg Implication #2) AOCI Tax Disparity

All adjustments or write downs to deferred tax accounts are recognized through *current earnings*, even if the original creation of the deferred tax account ran through *other comprehensive income* (OCI) rather than through net income.

This means any write down of the state DTA related to AFS security unrealized holding losses will need to be recognized through the current income tax expense.

The DTA write-down amount will become a reconciling difference when comparing the calculated after-tax unrealized holding loss remaining in AOCI to what is actually recognized in the trial balance.

Questions



2:40 – 3:30 p.m.

Managing Your Balance Sheet Through Uncertainty

Joe Kennerson, *Managing Director, Darling Consulting Group*

Eric Poulin, *Senior Consultant, Darling Consulting Group*

The *Dreaded* ALCO Meeting

April 17, 2024

Joe Kennerson | Managing Director | jkennerson@darlingconsulting.com

Eric Poulin | Director | epoulin@darlingconsulting.com

“Things that never happened before happen all the time.”

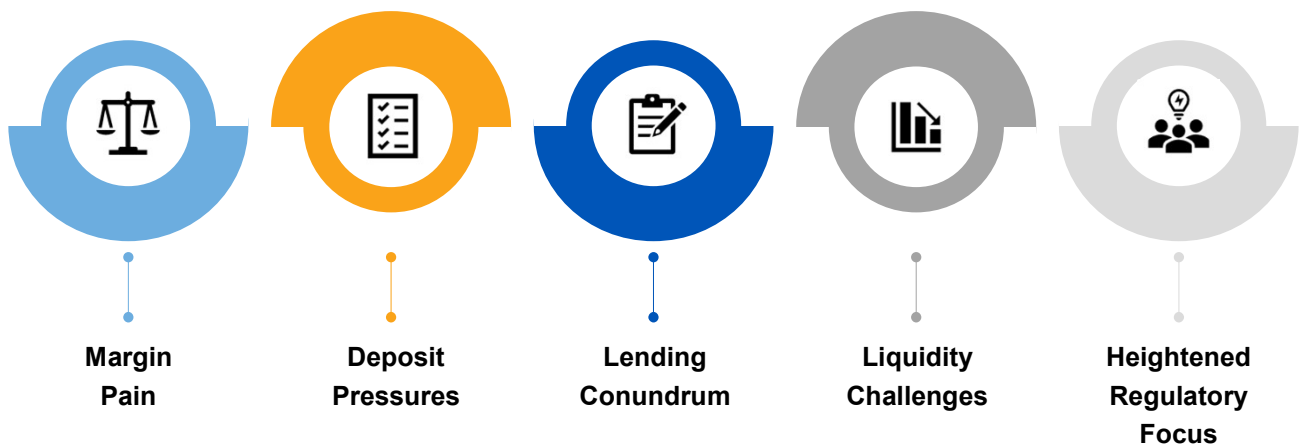
- Morgan Housel, The Psychology of Money

Yield Curve Inversion

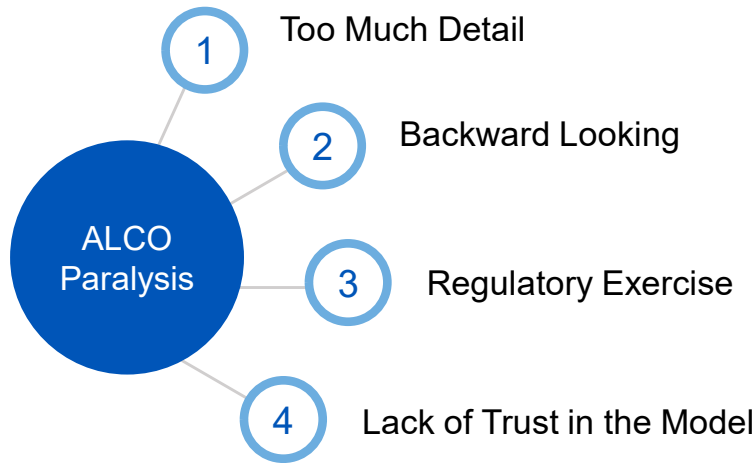


17 Months!

Challenges Continue



Common ALCO Grievances



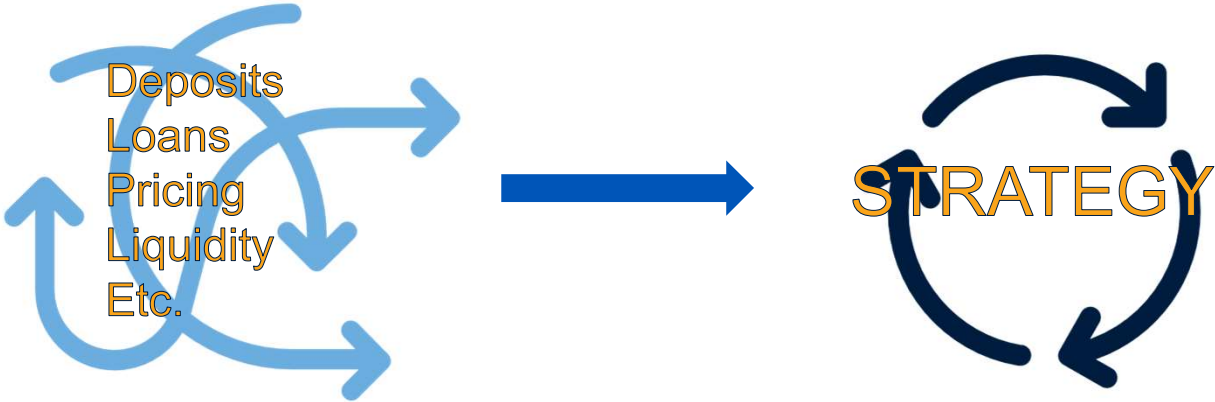
Turn ALCO Into A Profit Center

What Am I Missing?



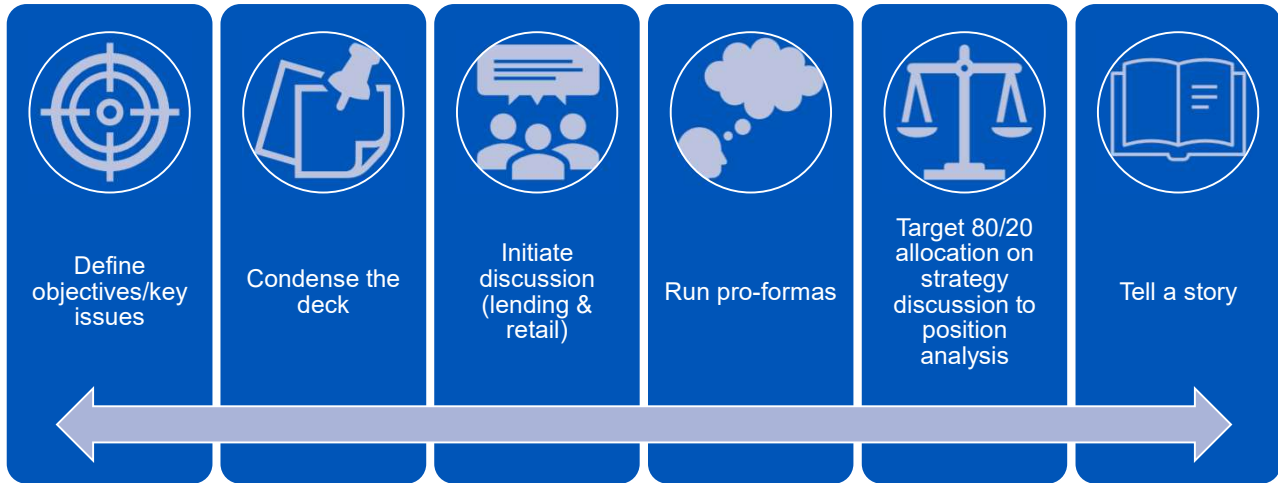
The Meeting

The ALCO Dilemma



The ALCO Meeting Blueprint

Steps for Productive, Strategically-Focused ALCO Meeting



Reminder: Small bites...we get back together *at least* quarterly!

What Are The Tiebreakers?

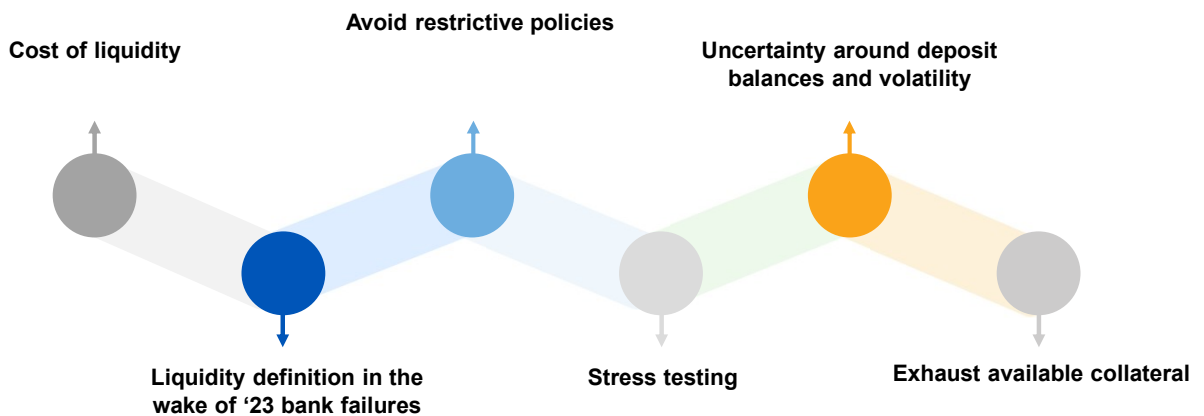
No Easy Decisions Today!

- How Important is Income?
- Lowering COF vs Losing Deposits?
- Preservation of Capital?
- Allocation of Liquidity?
- Discipline on Loan Spreads vs Losing Relationships?

Watch out for pitfalls

- ◆ Inverted Yield Curve
- ◆ Competing for Deposits Without a Gameplan
- ◆ Acquiescing Loan Covenants (Floors, Prepayments, etc.)
- ◆ Dismissing Derivatives

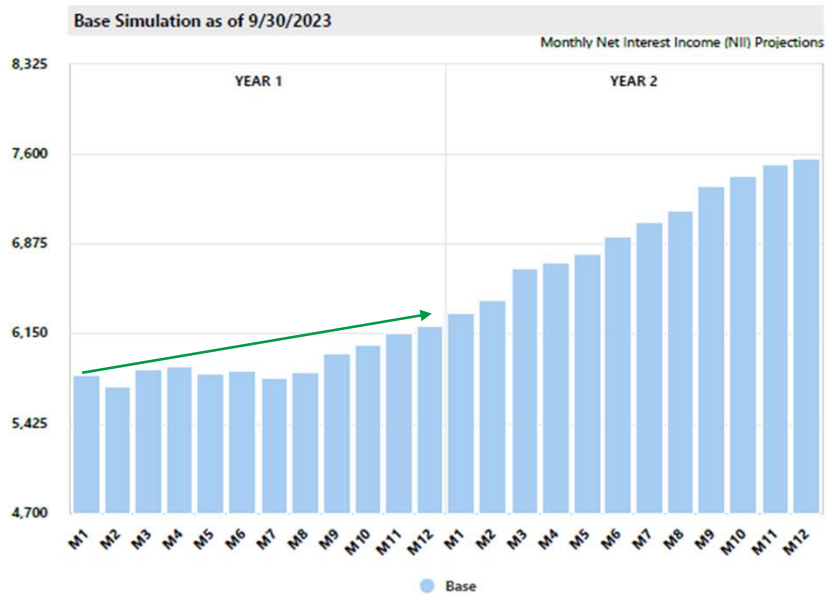
Evolution of Liquidity Management



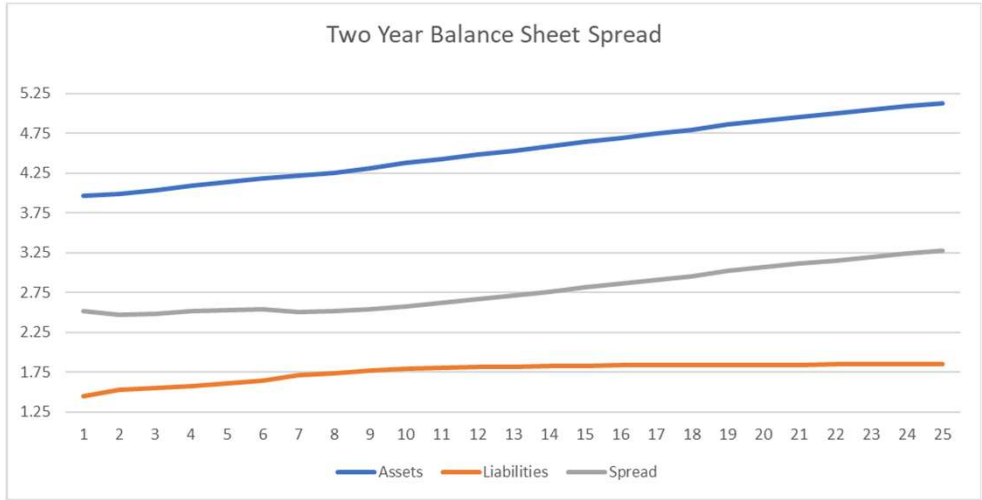
Case Study

Do We Trust Our Model?

Gaining Confidence in the Model



Balance Sheet Spread (No Growth)



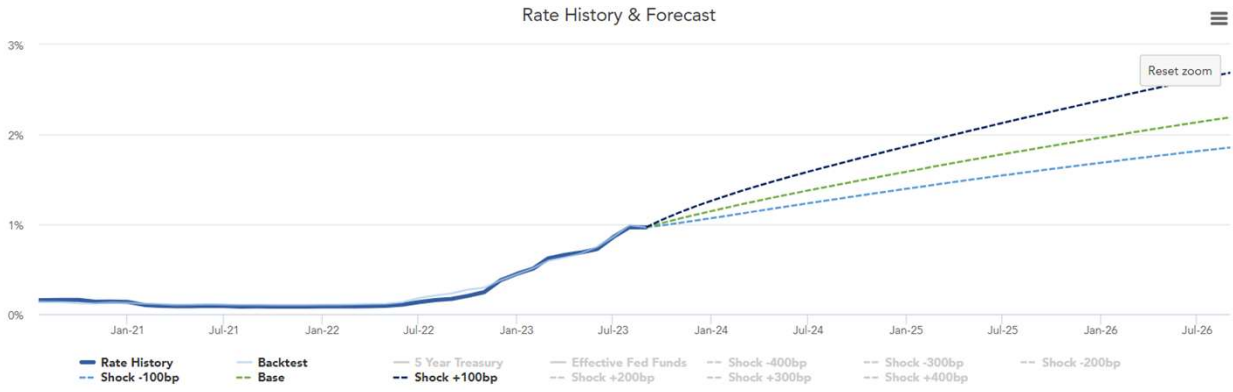
Legacy assets cycling, Good

Reality Check:
 ✓ Model vs Actual Prepays
 ✓ Loans Fully Repricing?

Reality Check:
 ✓ Lag Effects on NMDs

Dynamic Deposit Assumptions

	Rate Change	End Rate	Balance Change	End Balance
Shock -100bp	0.32%	1.29%	\$34,501 k	\$1,921,533 k
Base	0.48%	1.45%	-\$49,945 k	\$1,837,087 k
Shock +100bp	0.72%	1.68%	-\$125,866 k	\$1,761,166 k



What If NMD Rates ↑ & Mix Changes?



Strategy Discussion

If "Higher For Longer" is Biggest Concern

IRR

- How Much Exposure Do We Have?
- Can We Self Insure?
- Income Tiebreakers

Lending

- Gut Check on Pricing
- Pricing Discipline

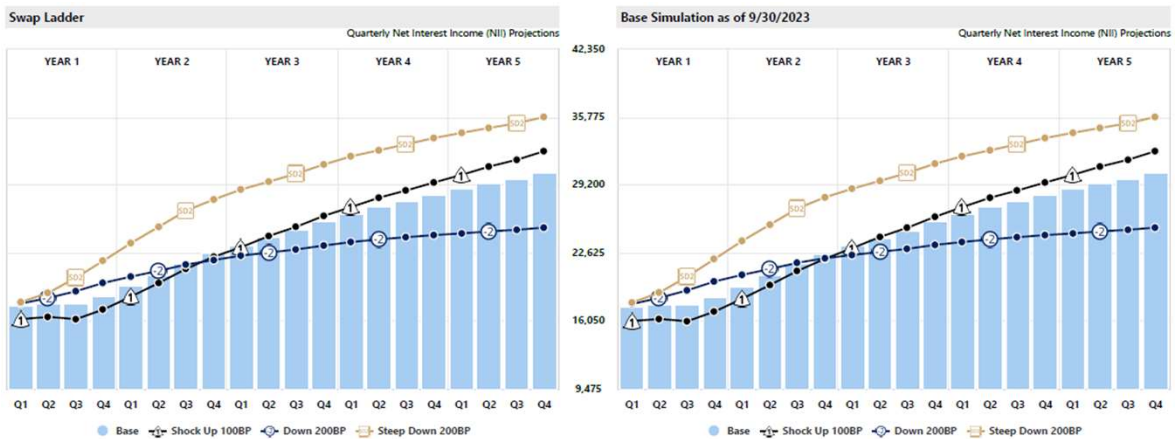
Capital Markets

- Don't Sleep on the Bond Portfolio
- Derivatives a Must... But Cautious on Term

Deposits

- MCOF Analysis is Critical
- What's The Play If Fed Doesn't Cut?

Strategy Example: Receive Float, Pay Fixed Swap



NII RESULTS					
	Y1	Y2	Y3	Y4	Y5
SHOCK UP 100BP	66,099	81,520	98,845	113,175	125,271
BASE	71,365	84,256	98,136	109,424	118,404
DOWN 200BP	74,707	84,707	91,364	96,150	99,183
STEEP DOWN 200BP	78,793	103,267	119,772	131,415	139,892

	Y1	Y2	Y3	Y4	Y5
SHOCK UP 100BP	787	808	352	0	0
BASE	308	308	152	0	0
DOWN 200BP	-192	-692	-248	0	0
STEEP DOWN 200BP	-267	-842	-308	0	0

DIFFERENCE

If Rates Down Aggressively Is Biggest Concern

IRR

- Good Time to Buy Insurance?

Lending

- Prepayment & Floor Values

Capital Markets

- Bond Pre-Investment?
- Keep Funding Short

Deposits

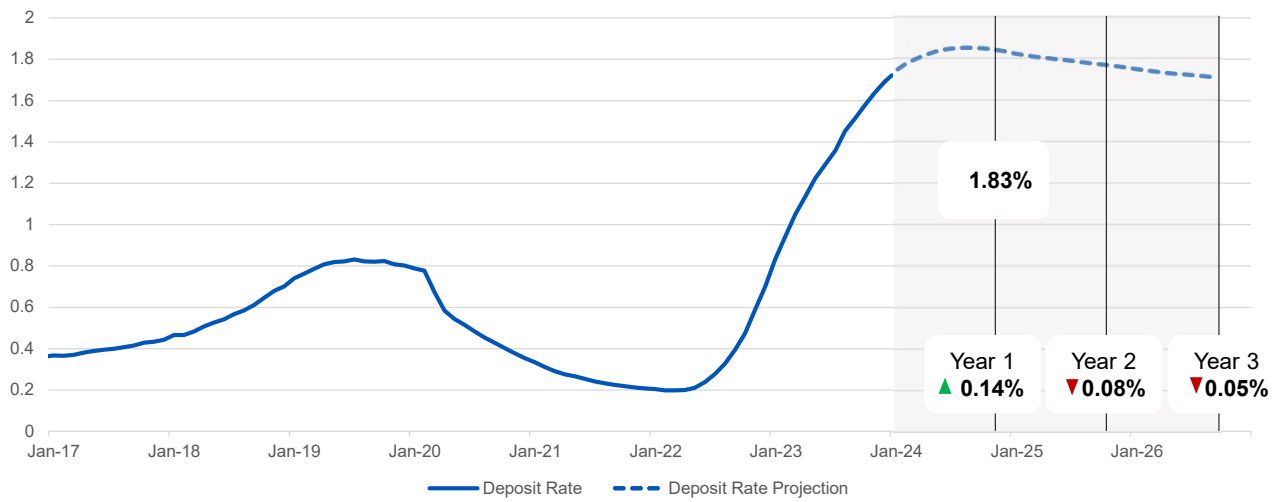
- See Strategy Outlook

Strategy Example: Bond Leverage



Deposit Outlook & Strategies

Deposit Rate Forecast



➤ Model Assumes Fed Funds flat until May and 4.5% by end of 2024, declining to 3.875% by 2026 – based on 2/9/2024 Forward Curve
 ➤ Forecast derived from Deposits360® - Industry NMD Rates above are balance weighted averages and do not include any outlier removal

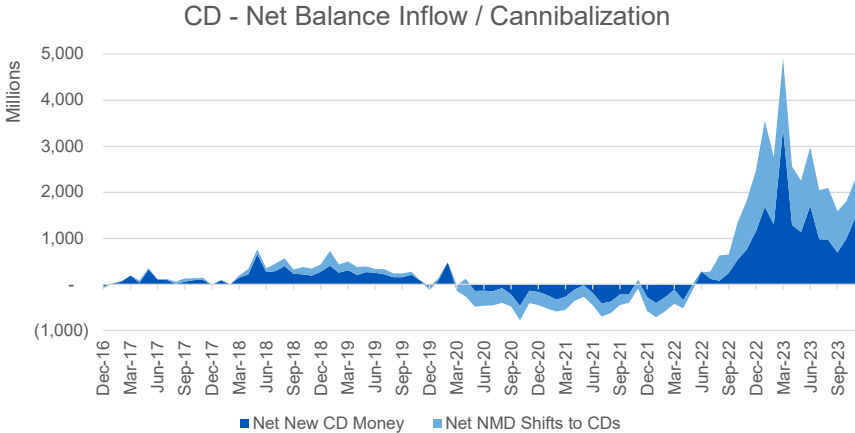
CD Thoughts & Outlook

2023 CD results:

- ◆ 45% Growth
- ◆ 46% Cannibalization

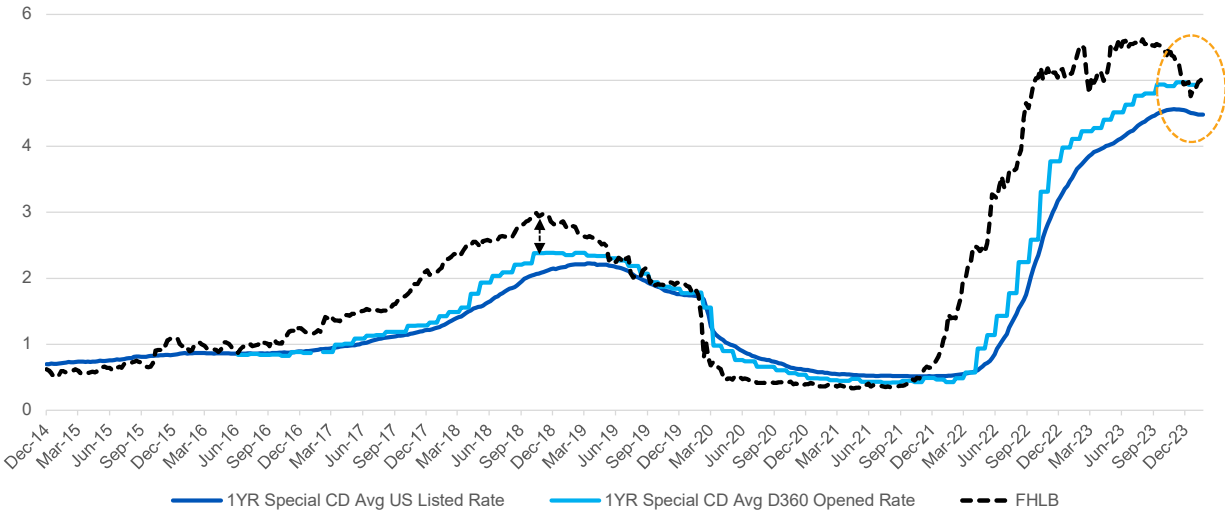
52% of CDs are maturing in 1H of '24 at WAR of 3.90%

Average CD Portfolio Activity 12/31/22 – 11/30/23



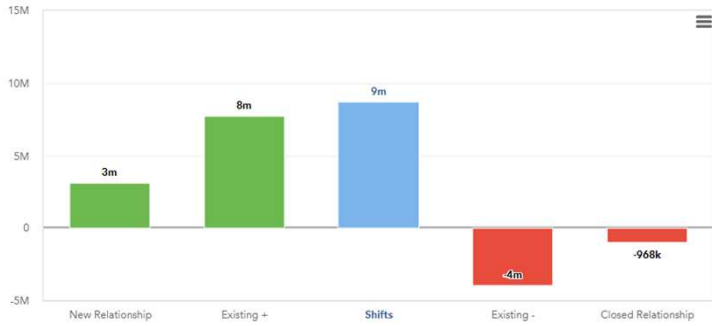
1YR CD Special Rate vs FHLB

1YR Special CD Rates vs FHLB



Source: Deposits360°

CD Activity w/ High Cannibalization



MCOF
10.39%

Cannibalization
59%

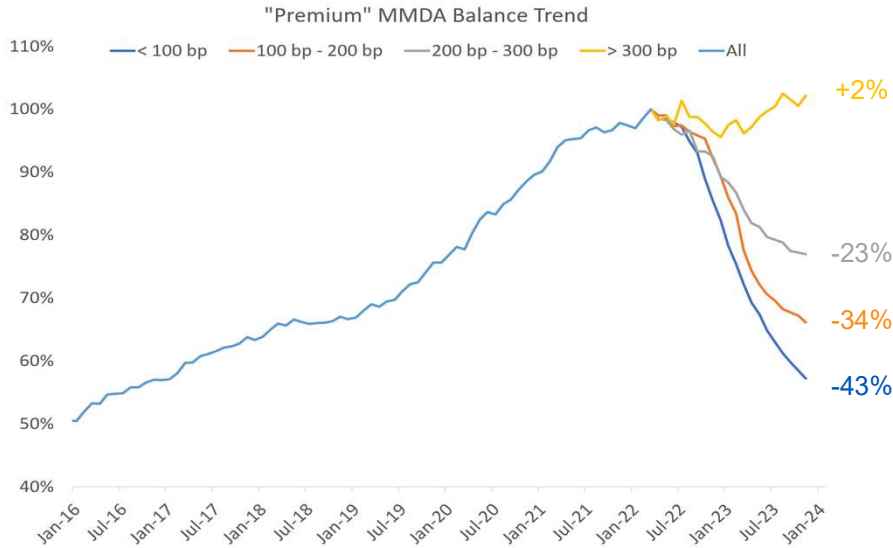
Migration Summary for
09/30/2023 - 12/31/2023

	Balance	Rate	# Rel.
Starting Balance	134,145k	3.38	2,282
INFLOW	10,906k	4.71	1,539
New Relationship	3,148k	4.68	46
Existing +	7,758k	4.72	1,493
SHIFTS	8,729k	0.71	1,183
DDA	1,280k	0.00	445
NOW	2,475k	0.53	293
SAV	3,859k	0.66	344
MMDA	1,115k	2.06	101
OUTFLOW	-4,888k	3.32	206
Existing -	-3,921k	3.36	187
Closed Relationship	-968k	3.17	19
Ending Balance	148,891k	3.73	2,450
NET CHANGE	14,746k	0.35	168

Source: Deposits360®



MMDA Price Elasticity



2023 Growth Rate:

Ave Rate 3.60%

Ave Rate 2.80%



Deposit Takeaways



CD Strategy

1. Outline Objective
2. Re-Align Pricing
3. Track Activity
4. Renewal Campaign



NMD Strategy

- Revamp Product Set
- Have Honest Discussion on Cannibalization vs Attrition
- Comeback Campaigns



Fed Easing Playbook

- Fed Cuts 25, 50, 100 bps, What's The Move?
- Stratify Customer Base

Concluding Thoughts



Start With The Meeting



Use Data To Your Advantage



Make ALCO A Profit Center

Thank You!



Joe Kennerson
Managing Director

✉ jkennerson@darlingconsulting.com
☎ 603-498-5852
in <https://www.linkedin.com/in/joekennerson/>



Eric Poulin
Director

✉ epoulin@darlingconsulting.com
☎ 603-479-9518
in <https://www.linkedin.com/in/ericpouling/>

3:40 – 4:55 p.m.

Current Issues in Business Ethics

Boz Bostrom, CPA, MBT, *Associate Professor of Accounting
& Finance, College of Saint Benedict & Saint John's University*

Current Issues in Business Ethics – 2024

Boz Bostrom, CPA
Professor of Accounting and Finance
College of Saint Benedict and Saint John's University
bbostrom@csbsju.edu (612) 414-9629
<https://www.linkedin.com/in/bozbostrom/>

May 14, 2024

1

Learning Objectives

- Understand the attitudes of other related to ethics
- Understand laws, rules and regulations which apply to CPAs and finance professionals
- Understand consequences of violating the laws, rules and regulations
- Understand and learn from current ethical violations
- Understand principles of ethical leadership

2

Ethical Attitudes and Perspectives

3

Introduction to Ethics

- What are ethics?
 - Moral principles
 - Rules of conduct followed by an individual or group

4

Gallup Survey Each May: How would you rate the overall state of moral values in this country today?

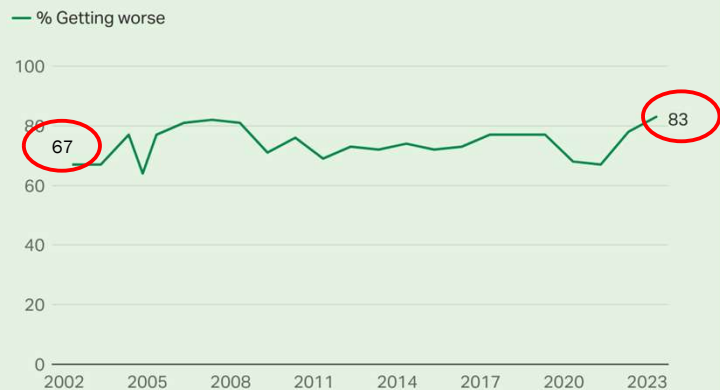
Year	Excellent/Good	Only fair	Poor
2003			
2011			
2023			

5

Right now, do you think the state of moral values in the country as a whole is getting better or getting worse?

Americans' Outlook for the State of Moral Values in the U.S.

Right now, do you think the state of moral values in the country as a whole is getting better or getting worse?



GALLUP

AICPA and CIMA Survey

- Polled about 1,800 people in the US and UK in December 2022
- Report released in June 2023
- Categorized people into 3 groups. We will focus on these two:
 - Business leaders
 - Future talent

7

What do you think: When asked if it is more important for companies to have ethical business practices than it was 5 years ago, business leaders most commonly said:

- a. Much less important
- b. Somewhat less important
- c. Just as important
- d. Somewhat more important
- e. Much more important

Is it more important for companies to have ethical business practices than it was 5 years ago?

	Business Leaders	Future Talent
• Much less important	<input type="text"/>	<input type="text"/>
• Somewhat less important	<input type="text"/>	<input type="text"/>
• Just as important	<input type="text"/>	<input type="text"/>
• Somewhat more important	<input type="text"/>	<input type="text"/>
• Much more important	<input type="text"/>	<input type="text"/>

9

Why be ethical?

- Compliance with rules, regulations, codes
- Stakeholder confidence, trust and loyalty
- Social acceptance / respect of peers
- Personal pride

10

Qualities in a new hire most commonly rated as “Very important” by business leaders

- Ability to communicate effectively
- Ability to lead
- Ethical
- Job specific technical skills
- Problem-solving skills
- Team player
- Trustworthy
- Willingness to learn/ask questions
- Trustworthy
- Ethical
- Ability to communicate effectively
- Problem-solving skills
- Willingness to learn/ask questions
- Team player
- Job specific technical skills
- Ability to lead

11

Percent that feel prepared to handle ethical dilemmas

	Business Leaders	Future Talent
• Very prepared	<input type="text"/>	<input type="text"/>
• Somewhat prepared	<input type="text"/>	<input type="text"/>
• Not very (or at all) prepared	<input type="text"/>	<input type="text"/>

12

Essential Traits to being an ethical person

- Accountability
- Charitable
- Honesty
- Humility
- Kindness
- Nurturing
- Respectable
- Trustworthy
- Trustworthy – 81%
- Honesty – 81%
- Accountability – 62%
- Respectable – 54%
- Kindness – 53%
- Humility – 45%
- Charitable – 31%
- Nurturing – 23%

13

Most important actions a company should take to foster more ethical behavior?

1. Be accountable for its actions
2. Operate with transparency
3. Follow all laws and regulations
4. Have a code of conduct
5. Respond immediately to violation of code of ethics

14

Confidential information

15

Discussion

- You work for a public company and would like to dispose of some shares
- What are some good principles to follow?
- What would be some clear violations?

16

Date	Close	Volume
8/12/2021	27.15	86,300
8/11/2021	26.71	184,700
8/10/2021	27.16	158,500
8/9/2021	27.86	174,100
8/6/2021	27.35	277,800
8/5/2021	26.95	202,800

17

Securities Exchange Act of 1934

- § 240.10b-5 Employment of manipulative and deceptive devices. It shall be unlawful for any person...
 - (a) To employ any device, scheme, or artifice to defraud.

18

What do you think: Insider Trading involves trading on the basis of

- A. Any information
- B. Material and non-public information
- C. Material and public information

19

SEC Rule 10b5-1

- § 240.10b5-1 Trading “on the basis of” material nonpublic information in insider trading cases.
- (a) *General.* The “manipulative and deceptive devices” prohibited by Section 10(b) of the Act (15 U.S.C. 78j) and § 240.10b-5 thereunder include, among other things, the purchase or sale of a security of any issuer, on the basis of material nonpublic information about that security or issuer, in breach of a duty of trust or confidence that is owed directly, indirectly, or derivatively, to the issuer of that security or the shareholders of that issuer, or to any other person who is the source of the material nonpublic information.

20

SEC's Rule 10b5-1: Affirmative Defenses

- When is a purchase or sale is not on the basis of material nonpublic information?
- Before becoming aware of the information, the person had
 - Entered into a binding contract to purchase or sell the security
 - Instructed another person to purchase or sell the security
 - Adopted a written plan for trading securities
- What is a written plan?
 - Specifies the amount of securities to be purchased or sold and the price at which and the date on which the securities are to be purchased or sold
 - Must be entered into in good faith and not to avoid Insider Trading rules

21

Cooling off periods after entering into the plan

- 90 days for directors and officers
- 30 days for others
- Directors and officers must represent that:
 - they are not aware of material nonpublic information about the issuer or its securities
 - they are adopting the plan in good faith and not as part of a plan or scheme to evade the prohibitions of Rule 10b-5-1

22

Case 1: Terren S. Peizer

- CEO and Chairman of Ontrak, a publicly traded health care company
 - Peaked in January 2021 at nearly \$80 per share. About \$0.50 per share today
- May 2021, learned of a serious risk Ontrak's biggest customer would terminate its contract. Is this material and non-public?
 - Entered into 10b5-1 plan shortly thereafter
 - Began selling shares the next day
- August 13, 2021, Ontrak's chief negotiator confirms contract would likely be terminated. Is this material and non-public?
 - Entered into 10b5-1 plan one hour later
 - Began selling shares the next day

23

Terren S. Peizer

- August 19, 2021, Ontrak's stock falls 44% when it announces customer terminated contract
- Peizer saved \$12.5M in losses
- March 2023, indicted. Facing up to 45 years in prison
 - Trial scheduled for April 2024

24

Case 2: A family affair

- From 2014 – 2021, Marc Perez was an accounting manager for General Finance Corporation, then a publicly traded company
 - At start of his employment, declared in writing that he would not engage in nor provide tips related to insider trading
 - Told he would have to pre-clear all trades with general counsel
- February 2021, United Rentals indicated an interest in acquiring General Finance
 - Perez learned of this interest through his role as accounting manager
 - Purpose of him learning about the acquisition was so that he could help compile financial information related to the acquisition
- March 2, 2021 United Rentals offered \$19 per share
 - Stock price was \$10.63 per share

25

Marc Perez

- Perez learns of the offer and buys \$354,000 worth of shares in General Finance
- Over the next 2-3 weeks, transferred money to his mother's brokerage account and also used some of her funds to purchase another \$421,000 of shares
- Around this time, Perez told his brother and sister that he was "all in" on General Finance stock and that they should also purchase some
 - Early April, brother and sister purchase a combined \$277,000 of General Finance stock
- April 15, 2021 – acquisition is announced
 - Stock price increased about 55% to about \$19 per share
- By early May, almost all shares had been sold by Marc and his siblings, with total profits being about \$660,000

26

Interesting terms used by the SEC

- Marc Perez acted with scienter
 - Intent or knowledge of wrongdoing
- Siblings knew or were “reckless in not knowing” they were trading on non-public information
- Marc Perez, “directly or indirectly, personally benefited from disclosing that material, non-public information to his siblings because giving a gift of trading information is the same as trading by the tipper followed by a gift of proceeds.”

27

What's next for Perez?

- Disgorgement of profits
 - Civil penalties up to 3x the amount of illegal profits
 - October 2023 pled guilty to criminal charges
 - Prison time up to 20 years
 - Age 59...future employment?
-
- Could General Finance Corporation have prevented this?

28

Bending the rules / ethical fading

29

Discussion

- You have made a few mistakes at work and have been put on “final notice” by your manager
- Right around the time you make another (final?) mistake, your manager has asked you to do something you find questionable
- When you say you can’t do that, your manager responds, “You WILL do it or I will have you fired?”
- What do you do?

30

What do you think: Bending the rules once makes it easier to bend them more times

- a. Agree
- b. Depends / Unsure
- c. Disagree

31

The German Nino Case

United States
Attorney's Office
Southern District of Florida

About SDFL | Find Help | Contact Us

Search

About ▾ News U.S. Attorney Divisions ▾ Programs ▾ Employment Contact Us

Justice.gov > U.S. Attorneys > Southern District of Florida > Press Releases > Former Financial Advisor Sentenced to Prison for Defrauding Close to \$6 Million Dollars from Clients and Spending it on Extramarital Affairs

PRESS RELEASE

Former Financial Advisor Sentenced to Prison for Defrauding Close to \$6 Million Dollars from Clients and Spending it on Extramarital Affairs

32

Background

- Beginning in 2012, Nino managed \$11 million of funds which a wealthy couple had invested in UBS
- Nino had power to invest the funds, but not transfer them
- From 2014 to 2020, through a series of 62 unauthorized transfers, Nino stole \$5.8M from the couple.

33

Usage of Funds

- Nino used \$4.6M on gifts for women he was romantically involved with:
 - Vacations
 - Cars
 - Apartment in Colombia
 - Private school tuition
- Who bailed him out of jail?
 - His wife!
- He used the other \$1.2M to repay funds taken from a different client

34

Covering the fraud

- False information shared in client meetings
- Fictitious brokerage statements
- Eliminated e-mail notifications on wire transfers
- Forged signatures on larger letters of authorization

35

Outcome

- The couple's son discovered the discrepancies
- Nino promised to pay the couple back with a signing bonus he would receive when joining a new firm
- In June 2022, Nino was sentenced to 78 months in federal prison

36

Ethical Fading

- How do cases like these start?
- Often times, the ethical issue is prevalent the first time, but then fades into the background

37



What do you think: What is the best way to stop ethical fading?

- a. Segregation of duties
- b. Sound hiring practices
- c. Tone at the top
- d. Trainings

39

What is the best way to stop ethical fading?

- Tone at the top. Ethical leadership
- Unethical ideas can happen...but they can't be implemented
 - Shut them down immediately
 - "That's not the way we do things here!"

40

Ethical role models and mentors

41

Role Models and Mentors

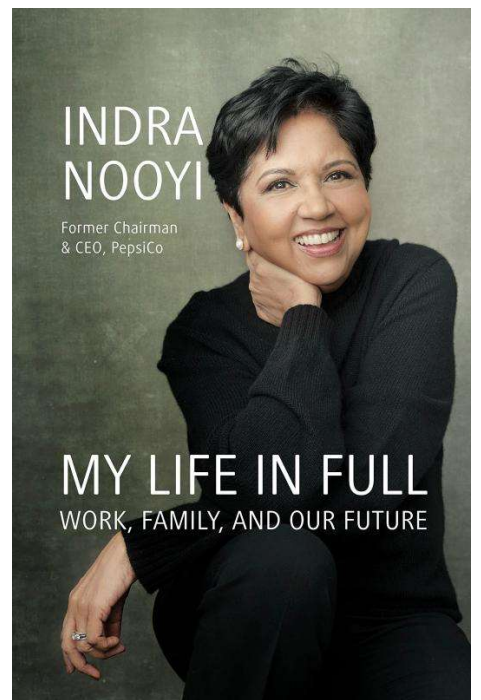
- Do you have a strong mentor or role model in your life?
- What do you admire about them?
- Does their influence help you make ethical decisions?
- Do you have a mentor or role model who is not a supervisor or family member?

42



Indra Nooyi

- <https://www.youtube.com/watch?v=hKaoQpG29RQ>





Key Takeaways

- Understand the relevant rules
- Discuss your decision with others who don't have a stake in the outcome
 - Assume your decision will be discovered
 - Focus on the long-term
- Keep yourself and others out of situations where violations are more common
- “Have the courage to say no. Have the courage to face the truth. Do the right thing because it is right. These are the magic keys to living your life with integrity.” – W. Clement Stone

Thank you!

- Questions, comments, or to stay in touch with Boz:
- bbostrom@csbsju.edu (612) 414-9629
- <https://www.linkedin.com/in/bozbostrom/>