

“TACTICS MEAN DOING WHAT YOU CAN
with what you have.”



ERM – Legal Perspectives for Now and The Future

By:
R. Todd Sherpy
Sherpy & Jones Law P.A.
Credit Union Resources &
Educational Services, LLC
Post Office Box 2599
Lexington, SC 29071
Atlanta Phone 770-631-3527
SC Phone 803 356-3327
rts@sherpy-jones-law.com



Copyright: © CURES, LLC, 1994-2018 - all rights reserved.

About Me ...

I'm not
Arguing.

I'm simply
Explaining
Why I'm
Right.



Introductory Notes: **Where to Start?**



**Let's Be Honest About
Our Regulation --**

Introductory Notes: **Where to Start?**



I wouldn't need
to manage
my anger
if idiots
would
manage
their stupidity!

Let's Be Honest About –

- 1. What we know**
 - 2. What we know we don't know.**
 - 3. What we don't know we don't know.**
-

Introductory Notes: **Where to Start?**



**Let's Be Honest About –
Attitude and Perspectives**

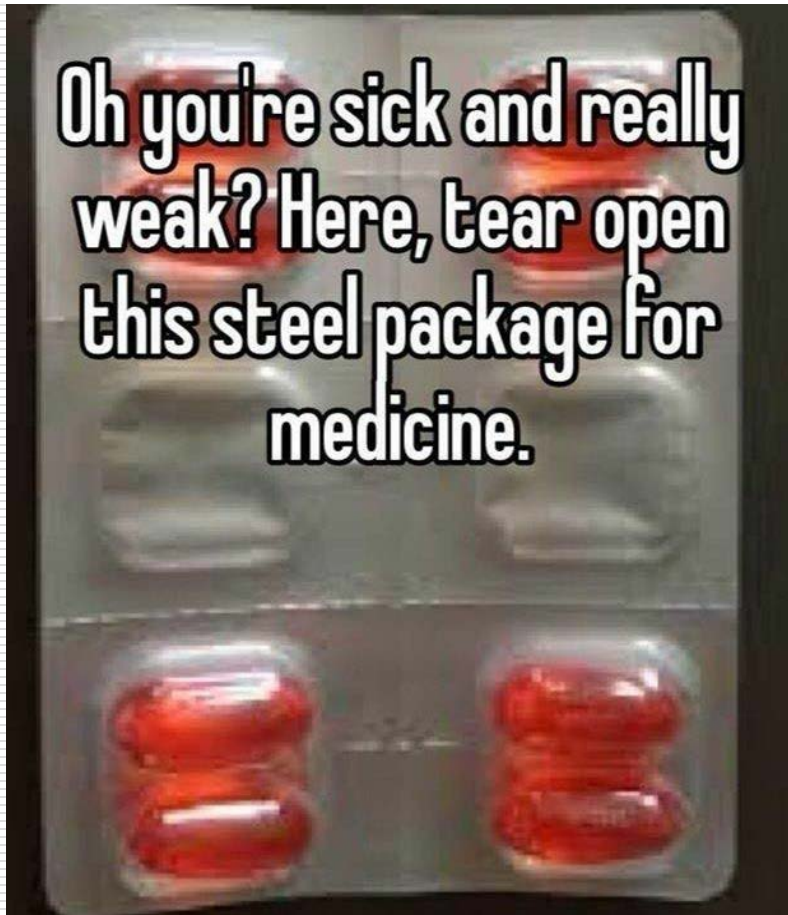
Introductory Notes: **Now – What's Wrong with Your Credit Union?**



What Laws, Rules or Regulations are your exposures.

"Jury selection didn't go as I'd hoped."

Introductory Notes: **Now – What's Wrong with Your Credit Union?**



What Laws, Rules or Regulations are your exposures that you did not mention?

What are you overlooking?

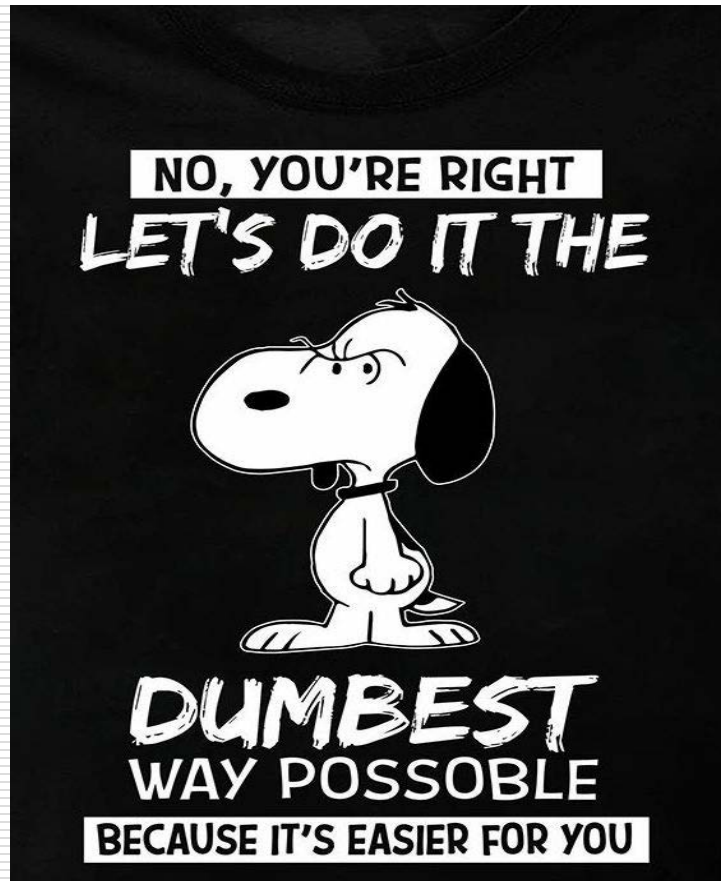
Introductory Notes: Now – What's Wrong with Your Credit Union?



What Laws, Rules or Regulations are your exposures that you did not mention?

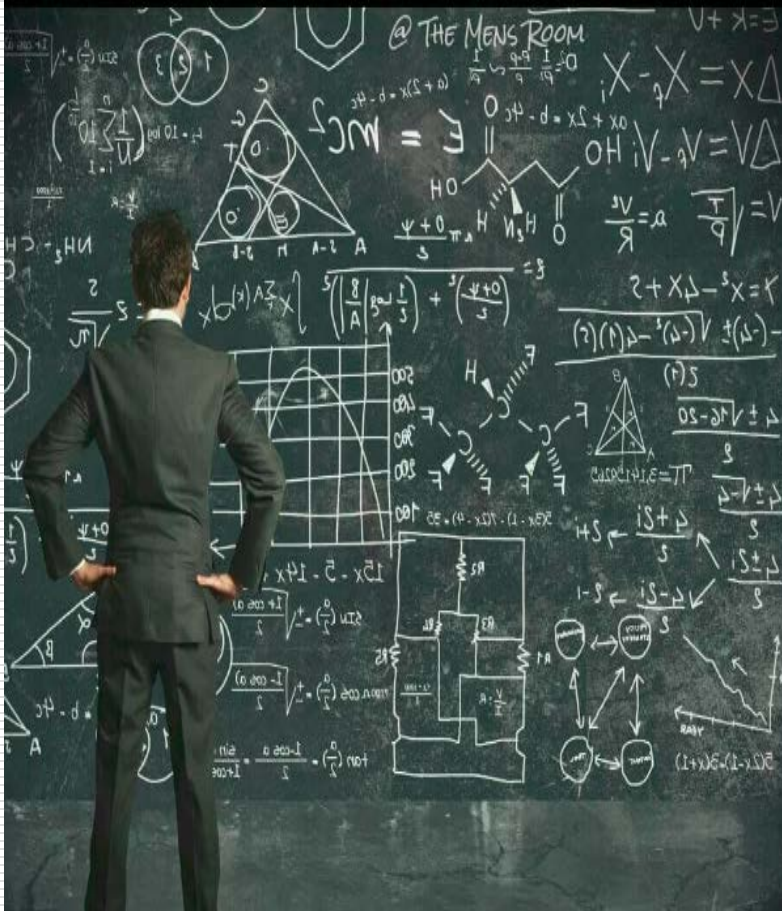
What are you overlooking?

Introductory Notes: **Now – What's Wrong with Your Credit Union?**



**Where else are you exposed –
or perhaps not protected as
well as one might wish?**

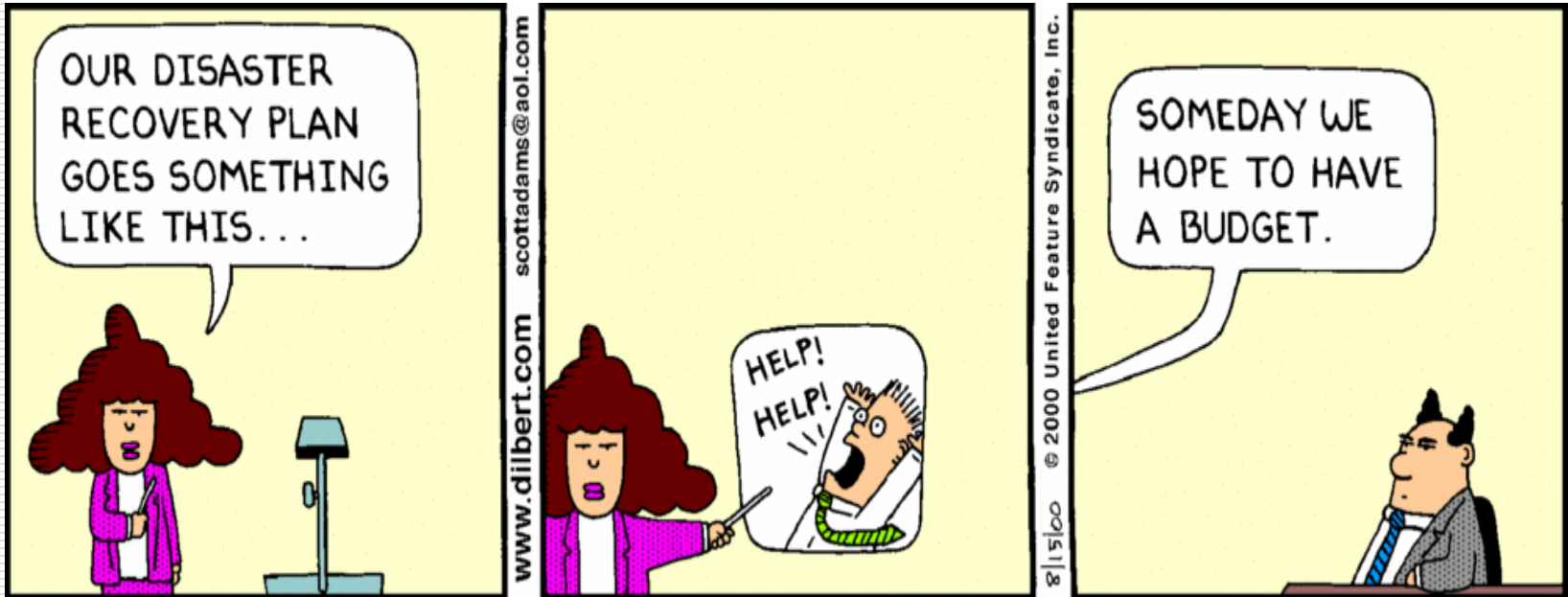
So How do you Figure it Out?



Where else are you exposed – or perhaps not protected as well as one might wish?

It is not just any one thing – there are many parts and you need to think TEAM Player.

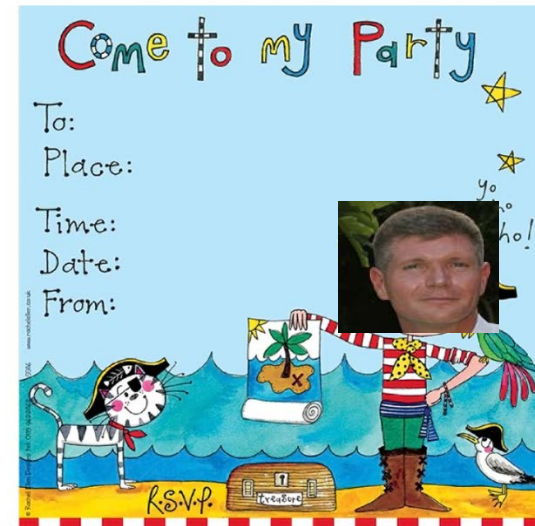
Any Plan Requires Risk Assessment and Management



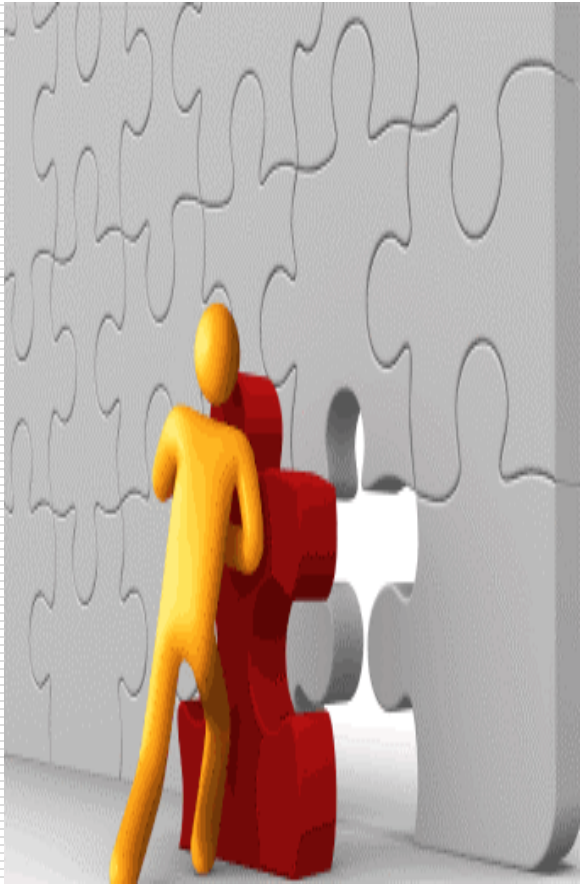
Now – Understand Legal and How Mucked up Things are: **Legal / Lawyers Are Stuck in a Mindset.**



Lawyers Need to Learn This:



What We Need to Accept



Legal is One of Many Parts

It IS NOT the only part.

When Legal becomes the only part – you will take no risks.

When you take no risks – you will kill your Credit Union.

Passing Judgment ???



- **May not agree, but do you know everything?**
- **Has the client been counseled on the risks?**
- **Judgmental People will not Thrive in an ERM Environment.**

So – How do We Change This Predicament?

Begin by Talking About it.

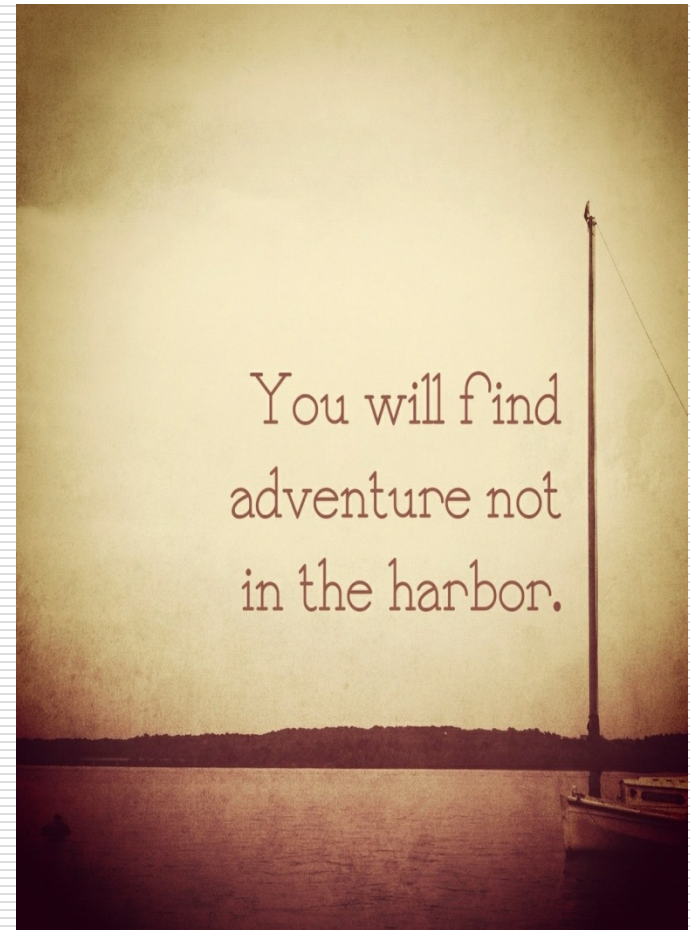
Make it Clear that the Credit Union is the Decision Maker; and the Lawyer is one Part of a Multi-faceted Process.



So – How do We Change This Predicament?

Discuss the fact that you'd like to know what the laws say, risks and options.

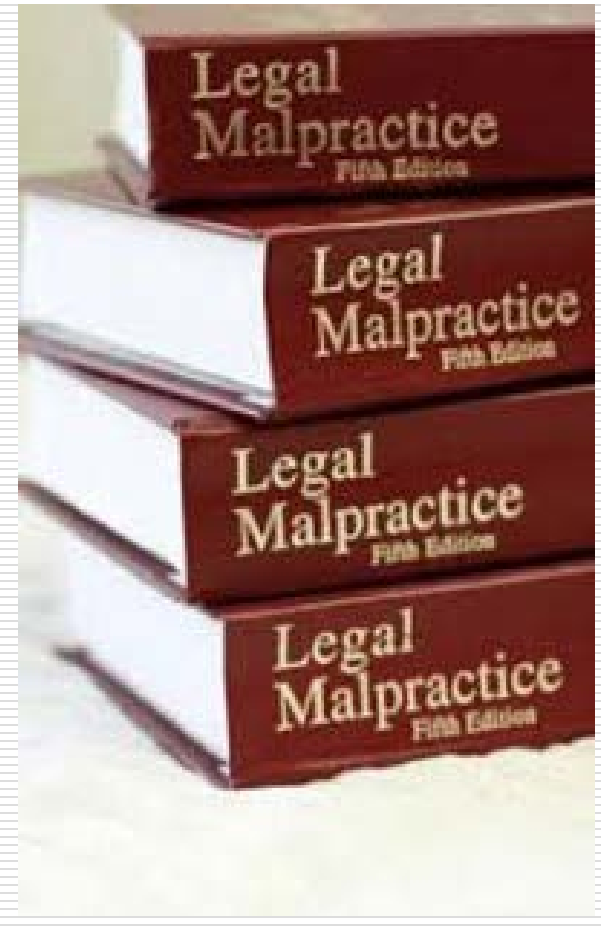
The lawyer will want to put you in a “Safe Harbour”; however being parked in a safe harbour may not always be the best “Business Decision” for the Credit Union.



The Lawyer's Conundrum

It's a real concern; and to engage in a true “risk management relationship” with counsel you need an understanding and TRUST.

Why is this an Issue? It's a New Era, A New Way, A Way where the Rules are Open to Discussion in so far as “Scope and Degree.”



Let's Start Small



Let's Start Small

**Your savings federally insured to at least \$250,000
and backed by the full faith and credit of the United States Government**

NCUA



National Credit Union Administration, a U.S. Government Agency

Let's Take it Up a Notch to Privacy Required Elements



[Privacy](#) | [Security](#) | [Web Policy](#) | [Accessibility](#) | [Browser Support](#) | [Site Map](#)

© 2018 Navy Federal Credit Union. All rights reserved

 Navy Federal Credit Union is federally insured by NCUA. |  Equal Housing Lender | Equal Opportunity Employer

Navy Federal conducts all member business in English. All origination, servicing, collections and marketing materials are provided in English only. As a service to members, we will attempt to assist members who have limited English proficiency, where possible. Military images used for representational purposes only; do not imply government endorsement. - Android™, Google Pay™ and Google Play™ are trademarks of Google LLC. The Android Robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License. Apple™, Apple Pay™, iPhone™, iSight™, Wallet™, Touch ID™ and iTunes™ are trademarks of Apple, Inc., registered in the U.S. and other countries. App StoreSM is a service mark of Apple, Inc. - Amazon, Kindle, Fire and all related logos are trademarks of Amazon.com, Inc. or its affiliates.

APY = Annual Percentage Yield | APR = Annual Percentage Rate

+Rates are based on an evaluation of credit history, so your rate may differ.

++Rates are variable and based on an evaluation of credit history, so your rate may differ.



*Message and data rates may apply. [Terms and Conditions](#) are available.

Let's Take it Up a Notch to Privacy Required Elements

The image shows a screenshot of the SRP Federal Credit Union website. The header is green with the SRP logo on the left and navigation links (About Us, Locations, Contact Us, FAQ, Privacy Notice) in the center. A search bar and a LOGIN button are on the right. Below the header is a green navigation bar with five categories: Insurance & Investments, Online Services, Membership & Benefits, Your Credit Union, and Business Services. A dropdown menu is open under Insurance & Investments, listing SRP Insurance Services, SRP Retirement & Investment Services, and TruStage Insurance. The main content area features a promotional banner with a child on the left and text on the right: "EARN UP TO \$300 When You Join SRP in May" and a "Learn More" button. On the right side of the banner is a login form with fields for Username and Password, and links for "Forgot Password" and "Enroll Now". A green LOGIN button is at the bottom of the form.

SRP
FEDERAL CREDIT UNION


About Us | Locations | Contact Us | FAQ | Privacy Notice


Search...   LOGIN

Insurance & Investments | Online Services | Membership & Benefits | Your Credit Union | Business Services

SRP Insurance Services
SRP Retirement & Investment Services
TruStage Insurance

EARN UP TO \$300
When You Join SRP in May

[Learn More](#) 



SRP ONLINE

Username

Password

[Forgot Password](#) | [Enroll Now](#)

LOGIN

It's Getting Hotter



Suspicious Activity Report

Name	Step 1. Filing Institution Contact Information	Step 2. Financial Institution Where Activity Occurred	Step 3. Subject Information	Step 4. Suspicious Activity Information	Step 5. Narrative
------	--	---	-----------------------------	---	-------------------

Part IV Filing Institution Contact Information

'82 Type of financial institution

'78 Primary federal regulator

'79 Filer name (Holding company, lead financial institution, or agency, if applicable)

'80 TIN '81 TIN type

83 Type of Securities and Futures institution or individual filing this report - check (boxes) for functions that apply to this report

<input type="checkbox"/> Clearing broker-securities	<input type="checkbox"/> Introducing broker-securities	<input type="checkbox"/> SRO Securities
<input type="checkbox"/> CPO/CTA	<input type="checkbox"/> Investment Adviser	<input type="checkbox"/> Subsidiary of financial/bank holding company
<input type="checkbox"/> Futures Commission Merchant	<input type="checkbox"/> Investment company	<input type="text"/> Other <input type="text"/>
<input type="checkbox"/> Holding company	<input type="checkbox"/> Retail foreign exchange dealer	
<input type="checkbox"/> Introducing broker-commodities	<input type="checkbox"/> SRO Futures	

84 Financial institution identification Type

Number

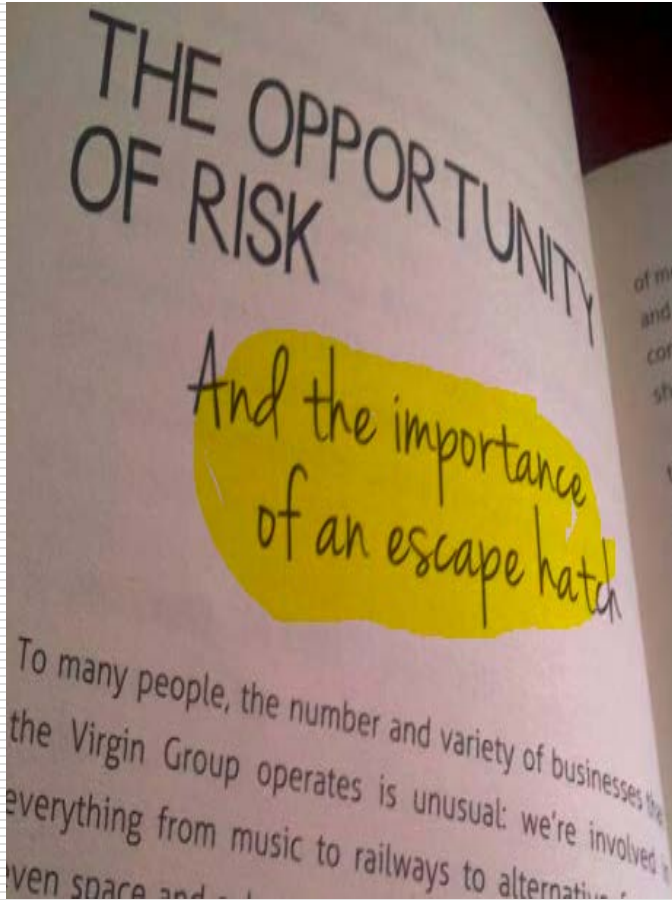
'85 Address

'86 City

'87 State '88 ZIP/Postal Code '89 Country

90 Alternate name, e.g., AKA - individual or trade name, DBA - entity

And then Sometimes it Gets Really Difficult



Discussion of One Client's ARM Problems

And then Sometimes it Gets Really Difficult II



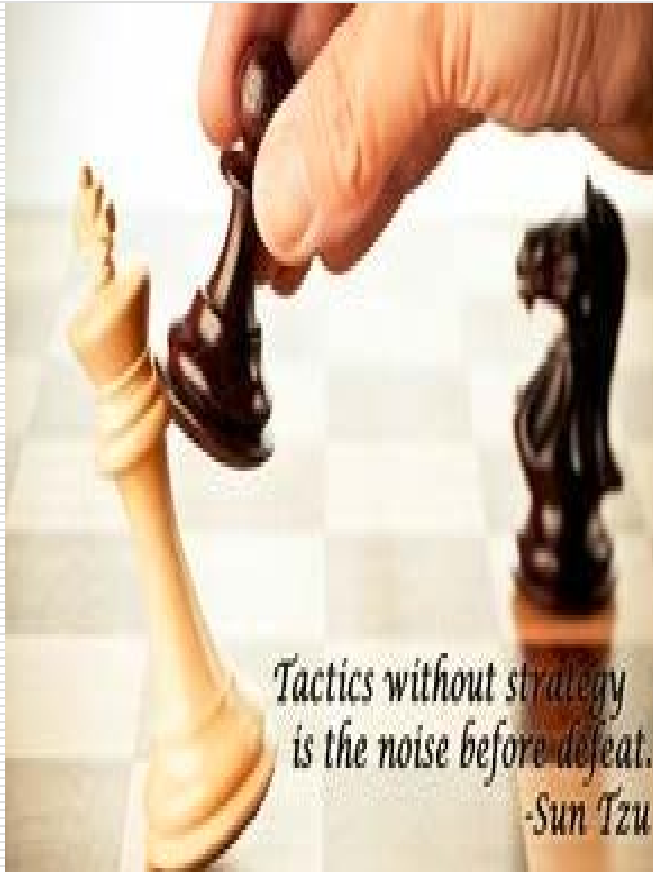
The Legal SAFE HARBOUR:

Notice and:

\$6,435,000.00

HOLY CRUD!

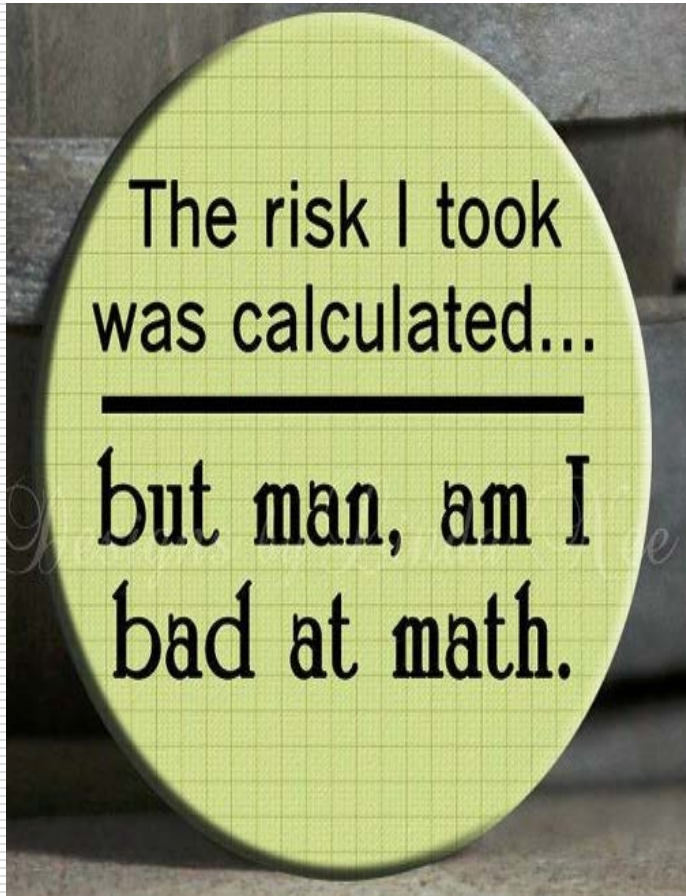
And then Sometimes it Gets Really Difficult III



**Now Let's Discuss Options
(Pros/Cons); Risks,
Rewards, Exposures,
Reputation, Etc.,**

*Tactics without strategy
is the noise before defeat.
-Sun Tzu*

And then Sometimes it Gets Really Difficult IV



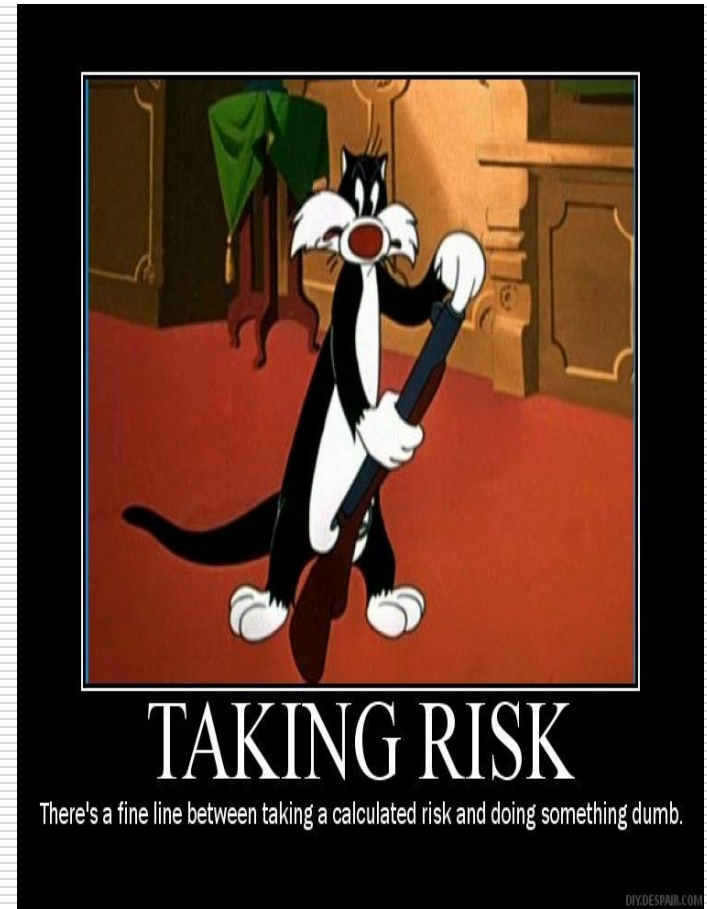
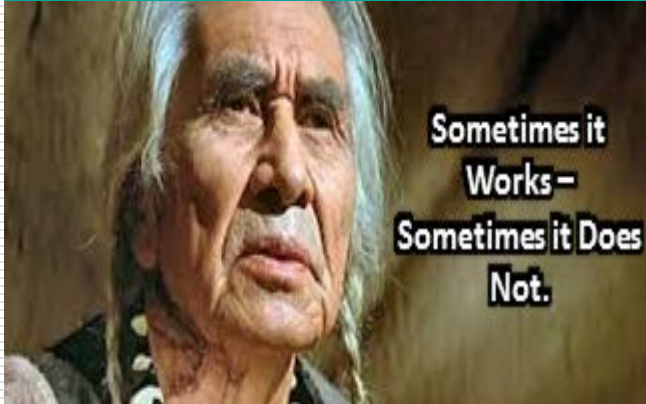
First – when leaving the safe harbour you must accept that there is risk.

The risks are dependent on a myriad of factors.

Sometimes risks may be speculative and difficult to measure.

And then Sometimes it Gets Really Difficult V

Option Two: Ostrich Defense



What the Mitigation or Back-up Plan?

If you take a risky course be sure to discuss what happens if it does not work.

Be ready to implement a mitigation plan.



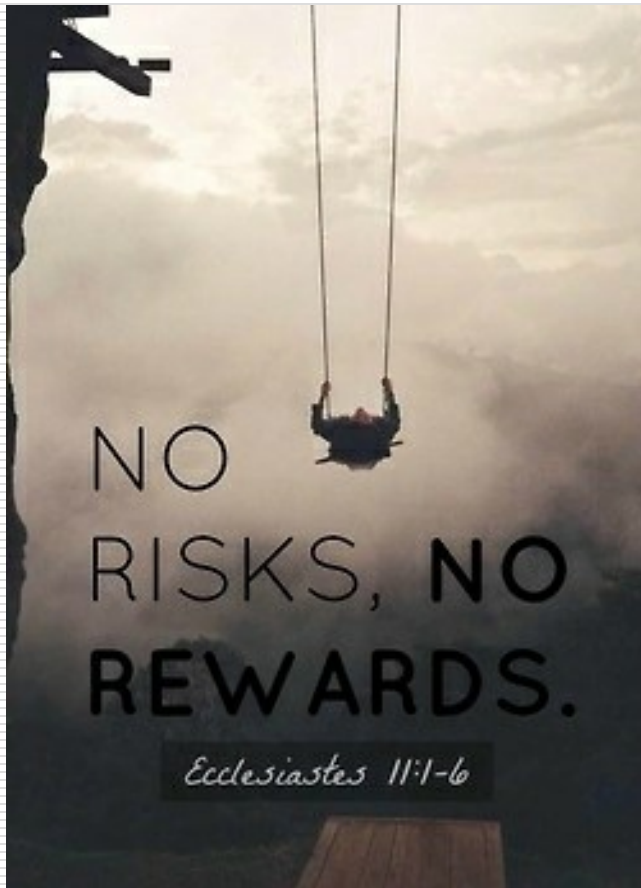
And then Sometimes it Gets Really Difficult VI



Thinking Outside the Box?
When there is no good answer – what do you do?



And then Sometimes it Gets Really Difficult VII



Sometimes an Option may not be 100% Legal Per Se.

- **Assess Options.**
 - **Consider “Workabilty.”**
 - **More of Less Exposure?**
 - **Ethics? What is Right?**
 - **What’s Your Duty?**
 - **Reputation Risk – Other Factors – will they impact your reputation adversely?**
 - **Beg for Mercy?**
 - **Middle Ground?**
 - **Are you making it worse?**
-

At the End of the Day – You are the Decision Maker



It's Not Always Easy – Not at All, but it's a Process All Need to Learn.



Risk Rating = Likelihood x Severity

S e v e r i t y	Catastrophic	5	5	10	15	20	25
	Significant	4	4	8	12	16	20
	Moderate	3	3	6	9	12	15
	Low	2	2	4	6	8	10
	Negligible	1	1	2	3	4	5
			1	2	3	4	5
			Improbable	Remote	Occasional	Probable	Frequent
			Likelihood				

Catastrophic	■	STOP
Unacceptable	■	URGENT ACTION
Undesirable	■	ACTION
Acceptable	■	MONITOR
Desirable	■	NO ACTION

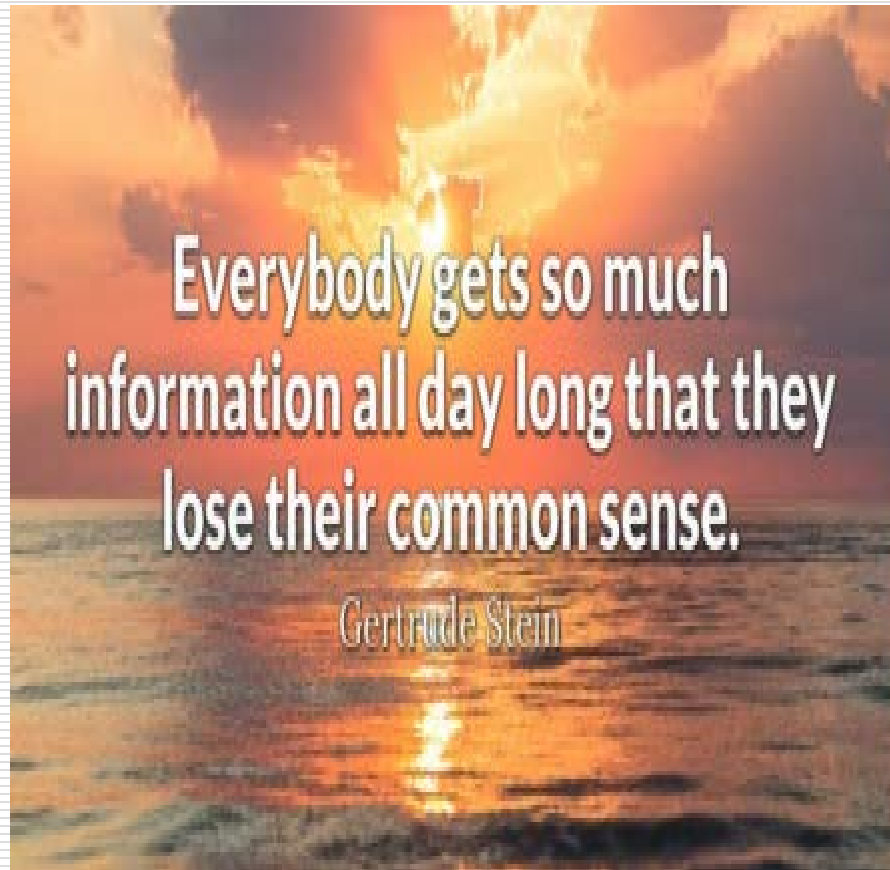
Audit as a Part of the Team?

Internal Audit Finds Problems ... that's it – game over – time to look for the next problem.

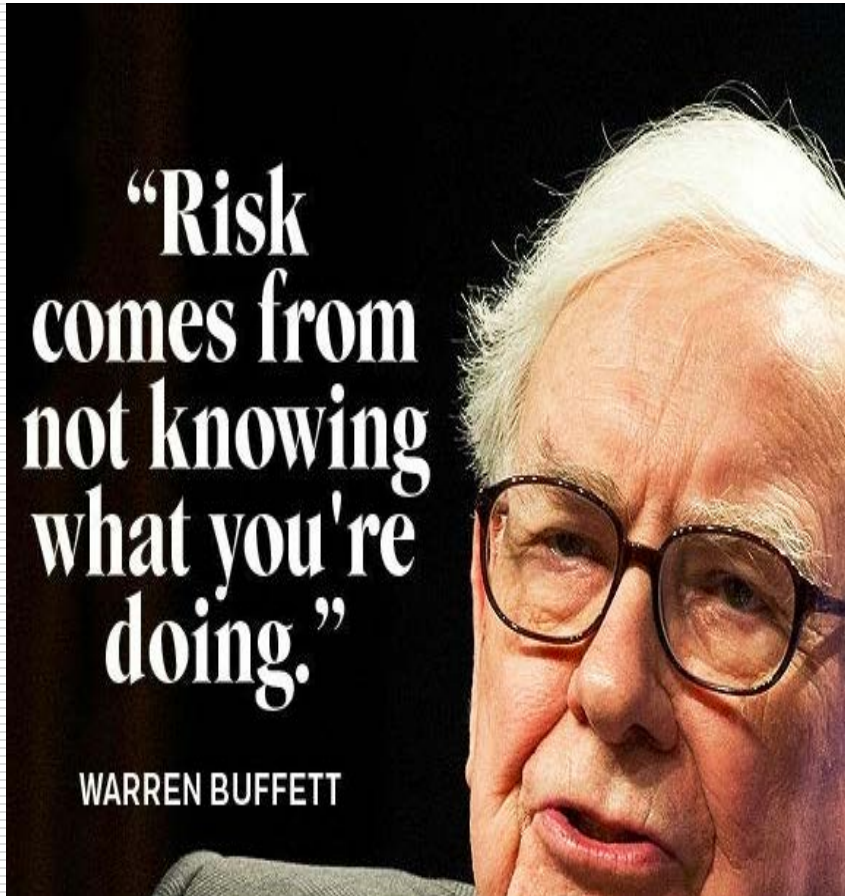
Risk Management Learns About the Problem – and then addresses it in a knowing manner that addresses it considering the interests of all relevant parties.



External Audit as a Part of the Team Too?



Overall Planning: Some Things are More Important than Others



The Goal is to Assess and Mitigate the Risks

Risk

Risk is measurable.

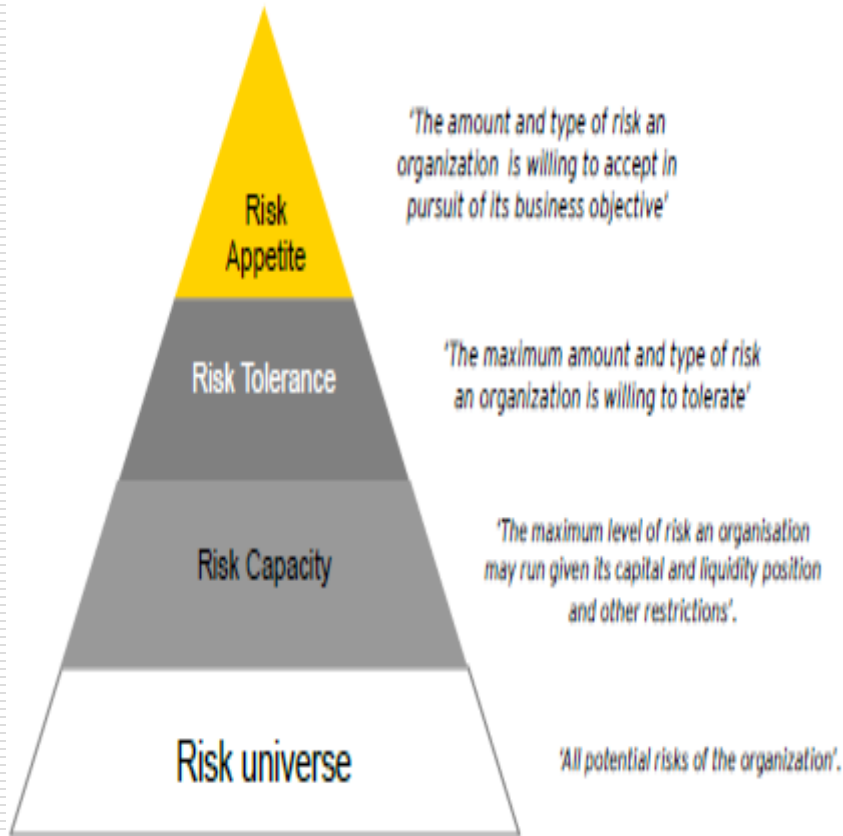
The odds of winning on any roll of a fair pair of dice are fixed and known before they hit the table.



- **Policies / Procedures**
- **Documents / Forms**
- **Everyday Matters**



Remember the Pyramid



But you have to Know them First -- Consider A Plan:

**"He who fails to plan
is planning to fail."**

Winston Churchill – WW2



CFPB before January 2016



CFPB after January 2016

Awww – and just who may need a whole pack of Therapy Dogs after last week's election?



Consumer Financial
Protection Bureau

Build this into everything



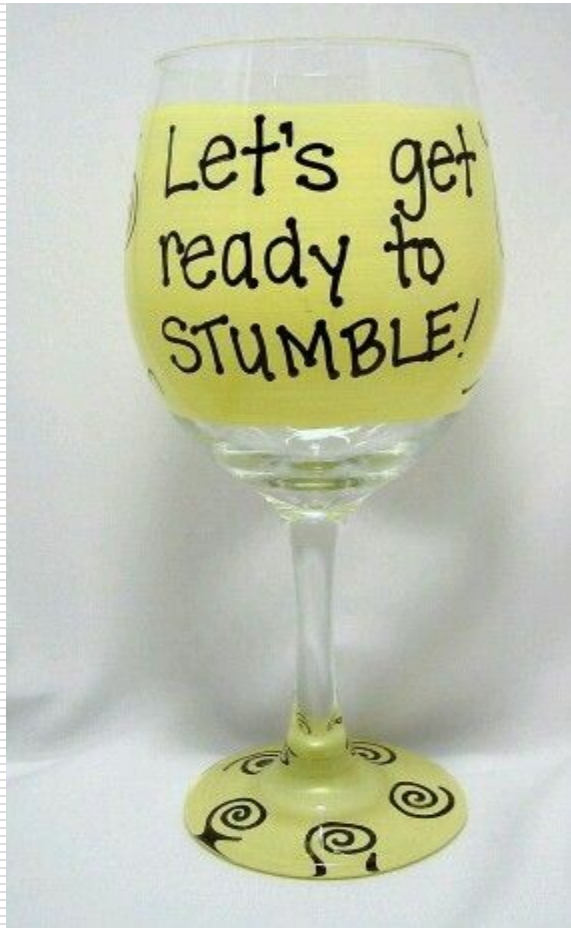
- Common Sense**
- Common Courtesy**
- Compassion**
- Promptness**

RIGHT THOUGHTS

RIGHT WORDS

RIGHT ACTION

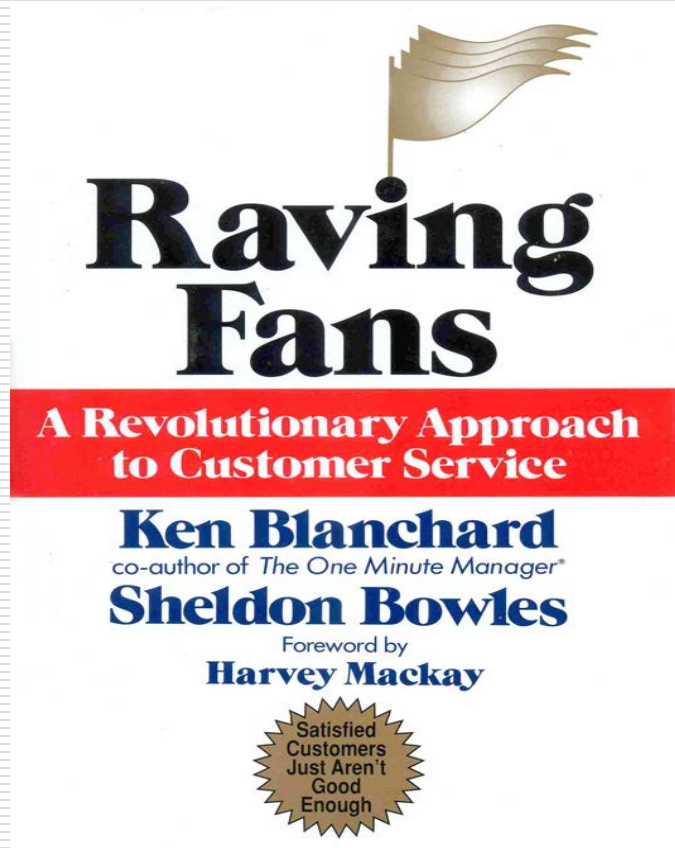
When In Doubt -- Ask



- Who? Depends**
- Teach This –**
- Open Doors ...**
- Don't**



Create the Team – Whatever it Takes



How's Your Team?



Staying Safe from Today's Risks --



Understanding and following some basic or primary rules can help your Credit Union stay in the safe zone. It is those items we seek to address via this program.

1st Legal Concept: “Loyalty”



RESPECT IS EARNED,
HONESTY IS APPRECIATED,
LOVE IS GAINED AND
LOYALTY IS RETURNED.

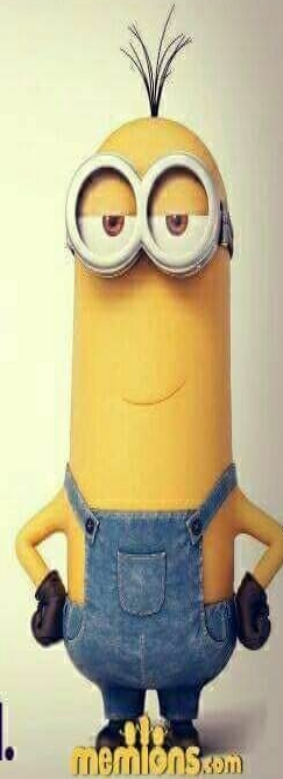
2nd Legal Concept: “Care”

What is Duty of Care?

Definition of Duty of Care

- Duty of Care is a requirement that a person act toward others and the public with watchfulness, attention, caution and prudence that a reasonable person in the circumstances would. If a person's actions do not meet this standard of care, then the acts are considered negligent, and any damages resulting may be claimed in a lawsuit for negligence.

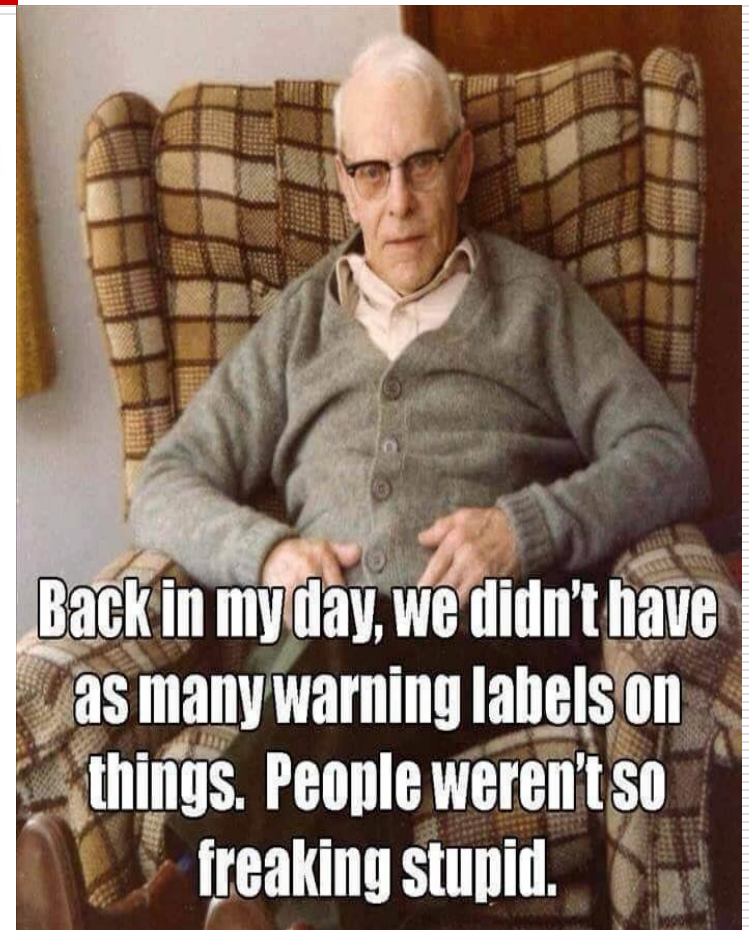
**WITH SO MANY THINGS
COMING BACK
IN STYLE...
I CAN'T WAIT
UNTIL MORALS
AND
INTELLIGENCE
BECOME
A TREND AGAIN.**



3rd Legal Concept: “Business Judgment Rule”

Business Judgment Rule

- ▶ Originated in USA – relates to effective decision making!
- ▶ Rule protects directors against being held accountable for business decisions however unwise they subsequently turn out to have been, if they were made on an informed basis, in good faith and without any conflict of interest, and if the decision was rational at the time in all the circumstances
- ▶ Not a “general shield” for directors from personal liability
- ▶ Complimented by directors’ “duty of care”
- ▶ Duty of care always necessary... for example.... if a director failed to verify a set of financial accounts (glaring errors), there could be liability under the duty of care.... in these circumstances the “business judgment” rule would not have application!

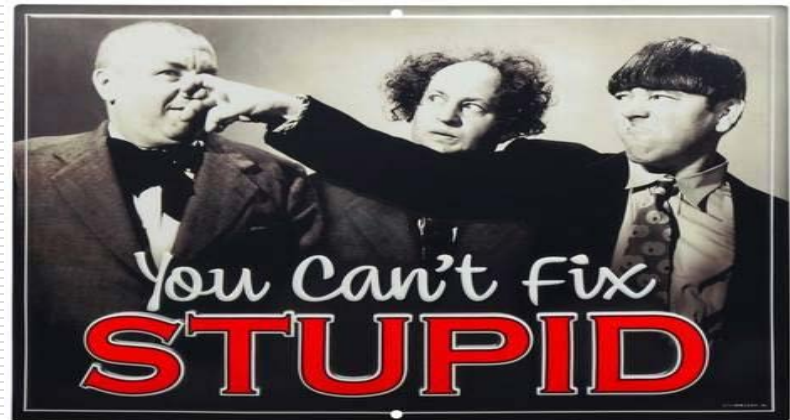


Everyday Expectations?



What do your members' want? Expect?

Think About many of our laws --



Privacy / Confidentiality/ Red Flags

SHOULDN'T HAVE SAID THAT

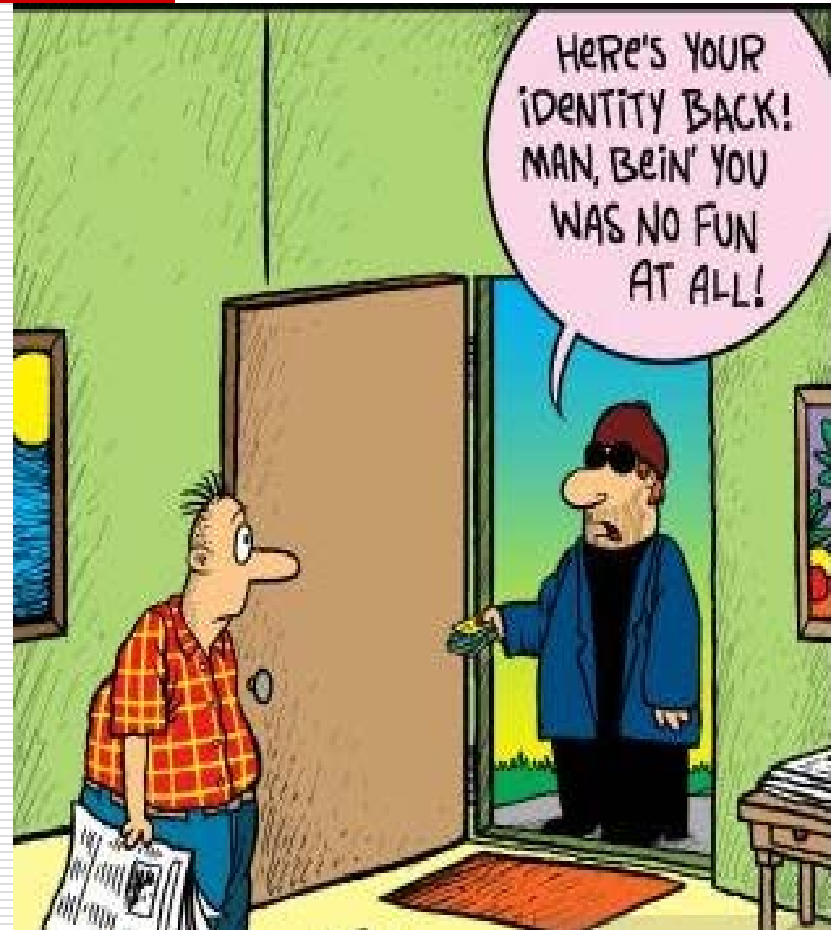
I SHOULD NOT HAVE SAID THAT

Start with
Common
Sense



What are Red Flag?

Fraud committed or attempted using, without authority, the identifying information of another person (Name, SSN, TIN, etc. Very broad) ...



Examples:

Suspicious Documents

5. Documents provided for identification appear to have been altered or forged.
 6. The photograph or physical description on the identification is not consistent with the appearance of the applicant or customer presenting the identification.
 7. Other information on the identification is not consistent with information provided by the person opening a new covered account or customer presenting the identification.
 8. Other information on the identification is not consistent with readily accessible information that is on file with the financial institution or creditor, such as a signature card or a recent check.
 9. An application appears to have been altered or forged, or gives the appearance of having been destroyed and reassembled.
-

Examples:

Suspicious Personal Identifying Information

10. Personal identifying information provided is inconsistent when compared against external information sources used by the financial institution or creditor. For example:
 - a. The address does not match any address in the consumer report; or
 - b. The Social Security Number (SSN) has not been issued, or is listed on the Social Security Administration's Death Master File.
 11. Personal identifying information provided by the customer is not consistent with other personal identifying information provided by the customer. For example, there is a lack of correlation between the SSN range and date of birth.
-

ID Theft Trends

FinCEN Report on ID Theft Trends, Patterns and Typologies.

<https://www.fincen.gov/sites/default/files/shared/ID%20Theft.pdf>



ID Theft Trends

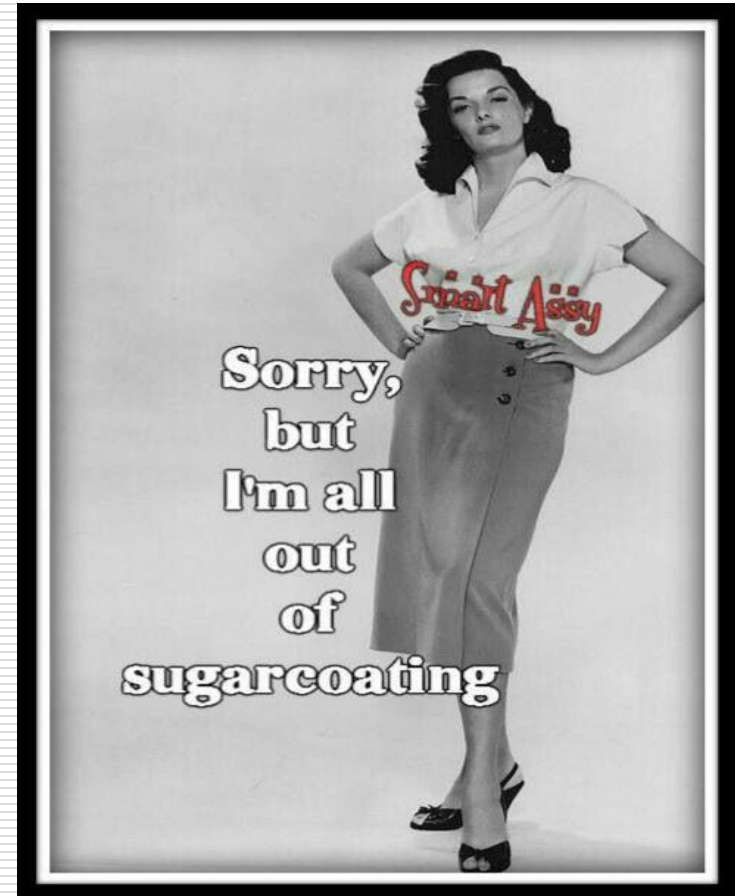
Credit Card ID Theft

- Physical theft
- Virtual theft

30% of the time the thief added his/her name as an authorized user

Deposit Account Fraud

- ID thief opens a new joint account with member's name.
- Thief then poses as victim and directs transfer from existing member's account into joint account



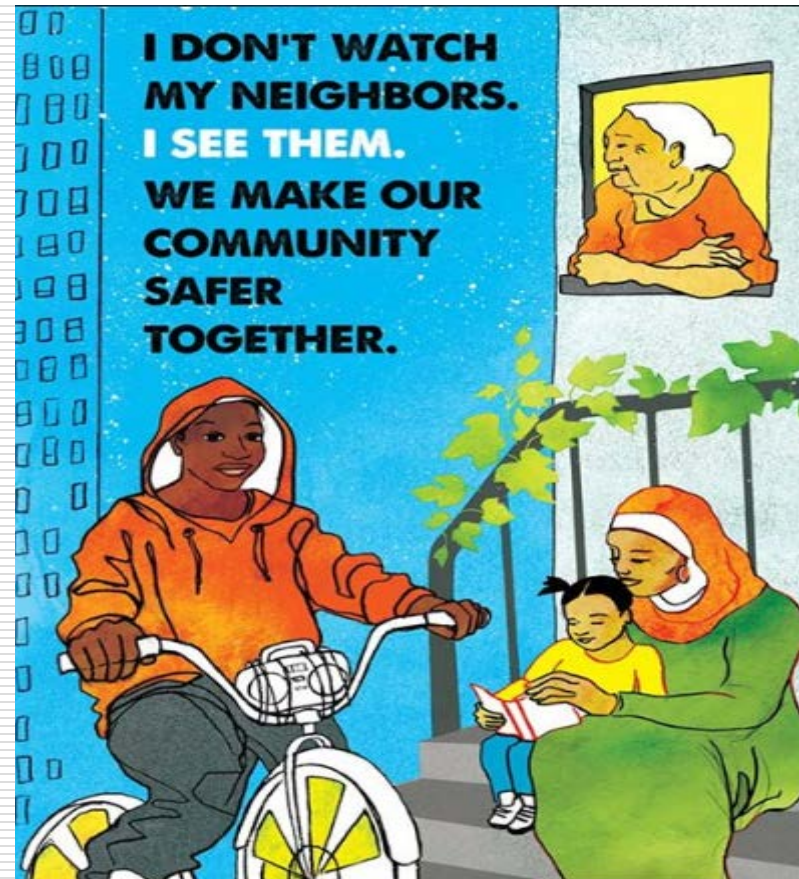
Resources



<https://www.occ.treas.gov/topics/bank-operations/financial-crime/identity-theft/index-identity-theft.html>

<https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a003>

Common Sense in Security



Internal Controls – Covers More than You May Think --

Internal controls include the policies and procedures that financial institutions establish to reduce risks and ensure they meet operating, reporting, and compliance objectives. The board of directors is responsible for ensuring internal control programs operate effectively. Their oversight responsibilities cannot be delegated to others within the institution or to outside parties. The board may delegate operational activities to others; however, the board must ensure effective internal control programs are established and periodically modified in response to changes in laws, regulations, asset size, organizational complexity, etc.



Internal Controls and Fraud Prevention



What NCUA says: Credit union safety and soundness includes establishing a strong system of internal controls and a comprehensive approach to managing fraud risk. Examiners will continue to evaluate the adequacy of credit union internal controls, as well as overall efforts to prevent and detect fraud.

Internal Controls – Audit, Compliance and Duty

Regulatory Focus -- Exposures



(Photo: Michigan Attorney General's office)

- CONNECT
- TWEET
- LINKEDIN
- COMMENT
- EMAIL
- MORE

A former CEO of Saginaw-based Valley State Credit Union — a credit union that ran afoul of state regulators earlier this year — faces 13 felony charges connected with the alleged embezzling of more than \$710,000.

Stanley Hayes, who headed the credit union from 2005 until he was terminated in 2016, allegedly used money from the credit union's funds to pay his car insurance, property taxes, travel and other personal expenses, according to Michigan Attorney General Bill Schuette's office.

Benton County Justice Center in Keweenaw File - Tri-City Herald

Richland HAPO teller charged with embezzling \$18,420 from 3 customer accounts

BY KRISTEN K. KRUEGER
kkru@tricityherald.com

A teller with HAPO Community Credit Union is accused of taking \$18,420 total from the accounts of three customers without their permission.

Two of the alleged transactions by Gabriela M. Perez were just one minute apart on the same day last December.

In the third transaction, the customer noticed the missing money that night, immediately transferred his remaining funds to another account, and then went into the credit union to report the problem the following morning after Perez called claiming she'd made an error.

Perez, 21, of Richland, pleaded innocent Thursday in Benton County Superior Court to one count of first-degree theft. Her trial is set Oct. 23.

She was working at the Richland branch



CREDIT UNION EMPLOYEE ARRESTED FOR EMBEZZLING FUNDS

The Basics of Internal Controls

Basic Principles

- Critical Business Processes
- Transaction Authorisation Controls
- Segregation of duties
- Internal Controls
 - Governance Controls
 - Application Controls
 - IT General Controls
- Monitoring & Internal Audit Controls



The Basics of Internal Controls – Coloring within the lines

LEGISLATIVE



- ★ Makes laws
- ★ Approves presidential appointments
- ★ Two senators from each state
- ★ The number of congressmen is based on population

EXECUTIVE



- ★ Signs laws
- ★ Vetoes laws
- ★ Pardons people
- ★ Appoints federal judges
- ★ Elected every four years

JUDICIAL



- ★ Decides if laws are constitutional
- ★ Are appointed by the president
- ★ There are 9 justices
- ★ Can overturn rulings by other judges

The Board
Sets Policy

Management Team
Executes Policy

Supervisory and Regulators
Ensure Rules Followed

The Basics of Internal Controls – Coloring within the lines – **Broad Applications**



Internal Controls – Broader Application and Personal Effects?

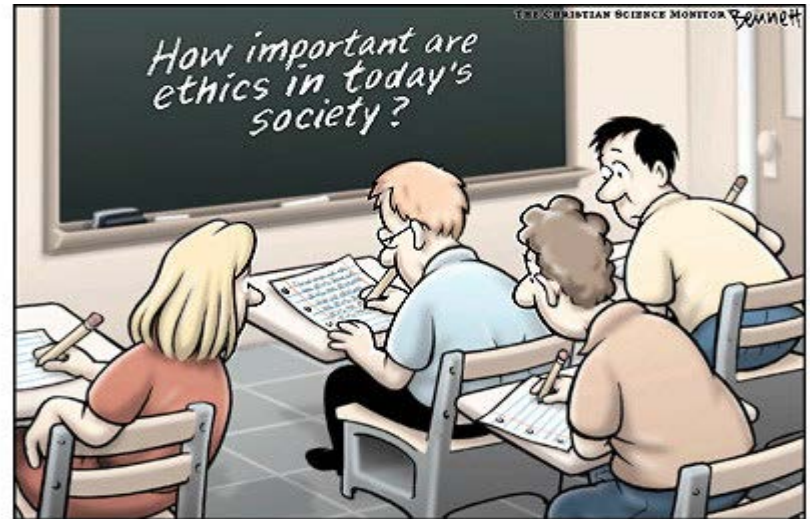


Know and Follow the Rules!



“Ethics”

Ethics (also moral philosophy) is the branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong conduct.

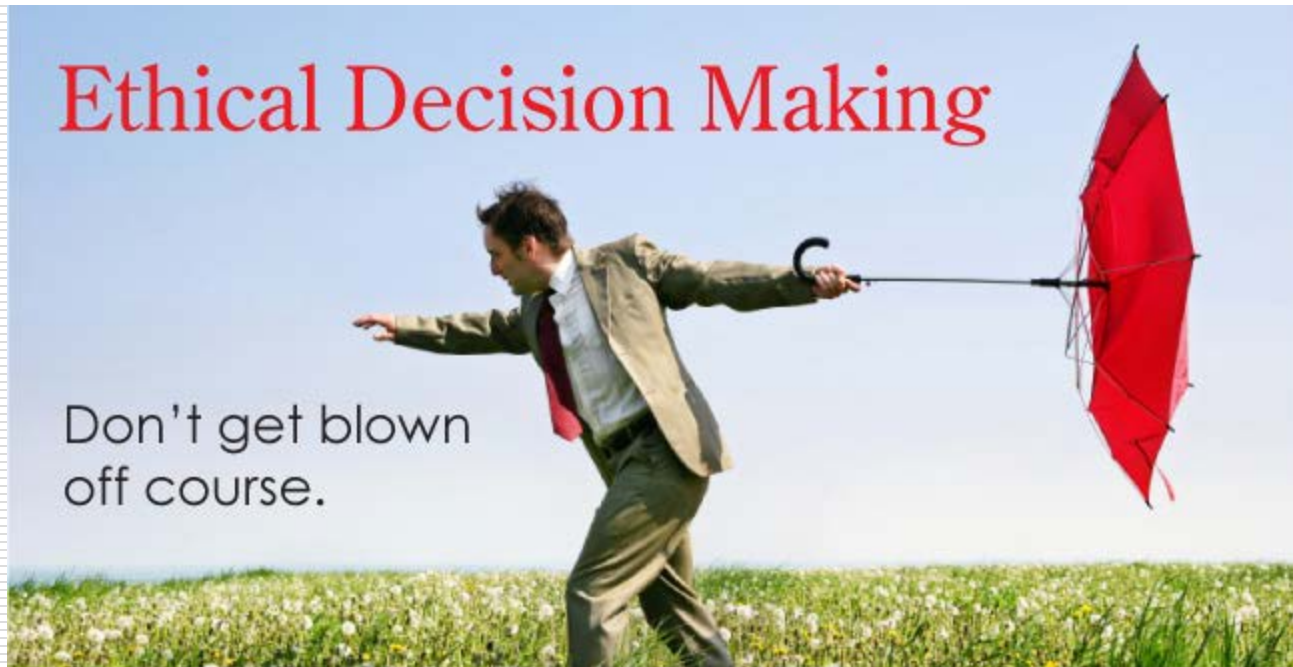


Right & Wrong -- Expectations

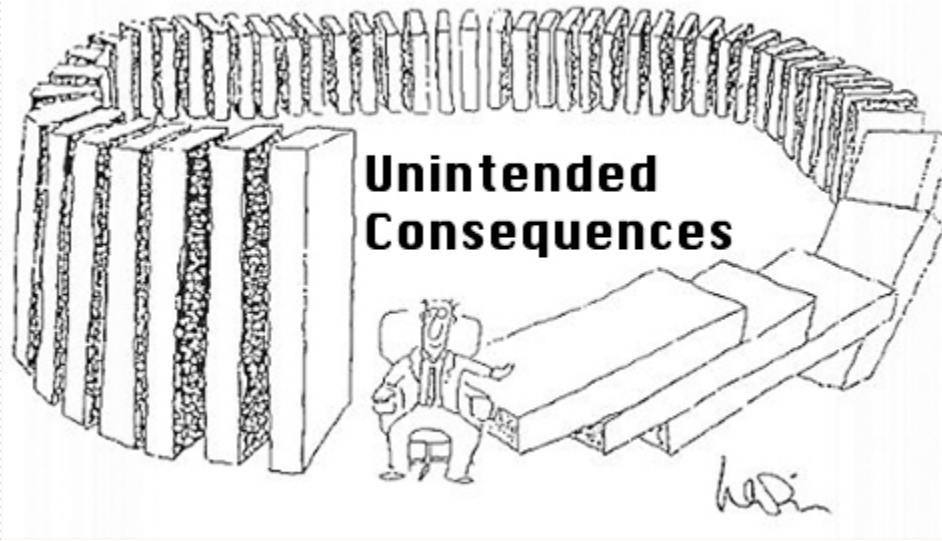
Business ethics are often guided by law, while other times provide a basic framework that businesses may choose to follow in order to gain public acceptance. The concept often hinges on public expectations as well as legal requirements.



Example – Credit Union Counsel



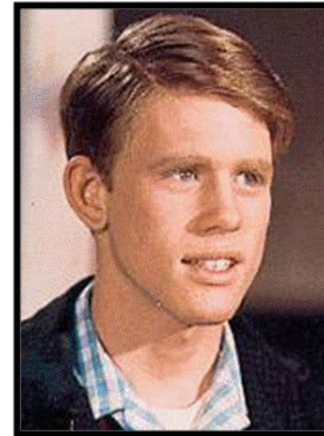
Human Nature - Incenting Bad Behavior



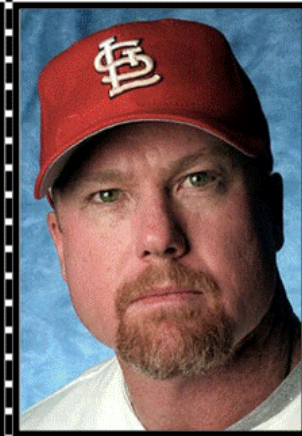
Human Nature - Motivated Blindness



Mark McGwire

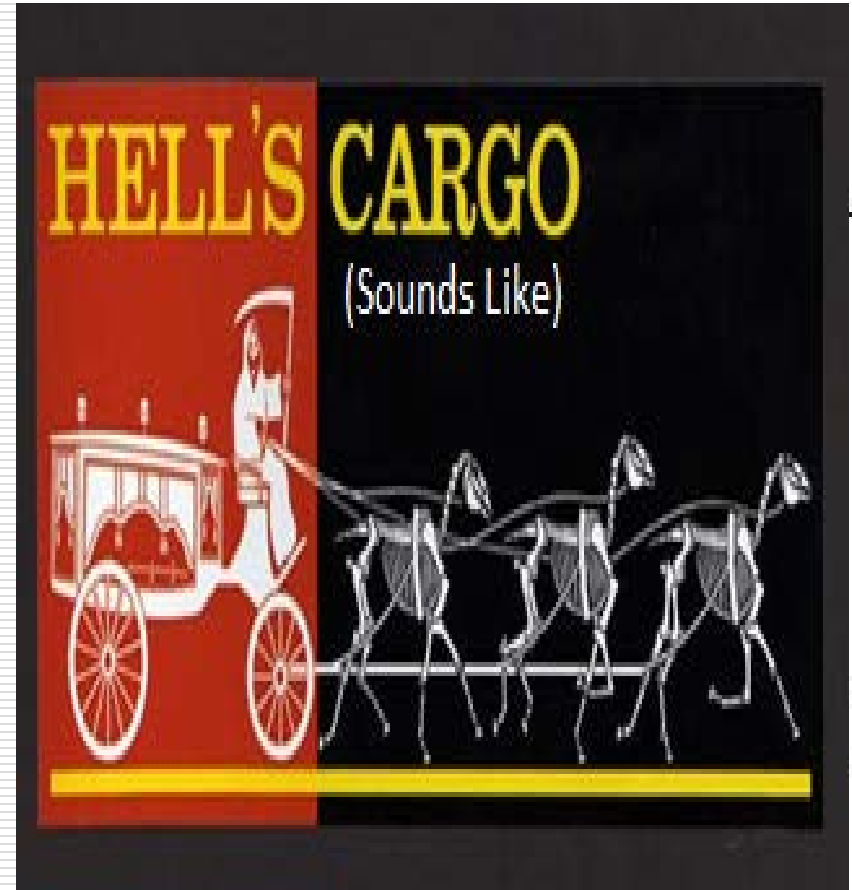


Just BEFORE
using steroids



1 year AFTER
starting steroids

Consequences of a Lack of Ethical Conduct & Lack of Controls



Understand the Dynamics – Be Aware – Establish Principles - Expectations

The Navy Federal Code of Ethics

In accordance with Board Policy, every Director, Committee Member, Officer, Agent, Attorney and Employee of Navy Federal Credit Union shall be guided by the Code of Ethics set forth below and should:

<https://www.navyfederal.org/about/code-of-ethics.php>



Turning to the Policy and Where it Comes From 03-FCU-07 and Other Stuff



Bribery – it's a common sense thing.



Whistleblowers?



Whistleblower (also written as whistle-blower or whistle blower) is a person who exposes any kind of information or activity that is deemed illegal, unethical, or not correct within an organization that is either private or public. The information of alleged wrongdoing can be classified in many ways: violation of company policy/rules, law, regulation, or threat to public interest/national security, as well as fraud, and corruption. Those who become whistleblowers can choose to bring information or allegations to surface either internally or externally. Internally, a whistleblower can bring his/her accusations to the attention of other people within the accused organization such as an immediate supervisor. Externally, a whistleblower can bring allegations to light by contacting a third party outside of an accused organization such as the media, government, law enforcement, or those who are concerned. Whistleblowers, however, take the risk of facing stiff reprisal and retaliation from those who are accused or alleged of wrongdoing.

NCUA Rules?

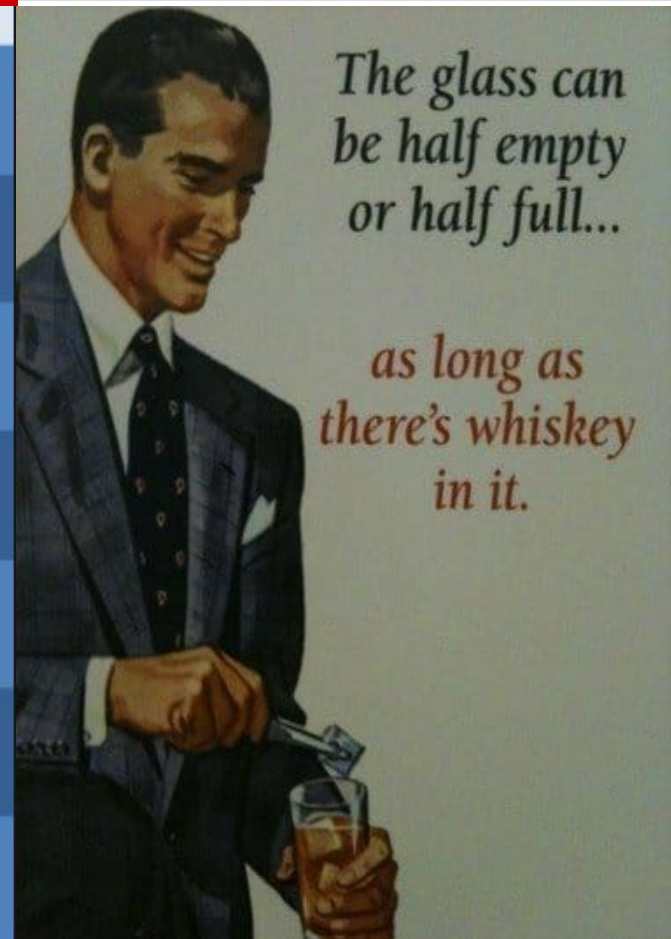


What You Want / What You Need / What Mgmt. Provides



ERM Integration

“Know Yourself... Know your Enemies”	Enterprise Risk Management
“Build the Walls”	Contracts
“Dig the Moat”	Policies/Processes/ Governance & Controls
“Guard the Walls”	Whistleblower/Audits/Ethics & Compliance Management/Ongoing Assessments
“Protect the Frontier”	Legislative & Regulatory Affairs
“Sound the Alarm”	Effective Reporting/Timely Decision Making
“Go to War”	Litigation, Lobbying & Investigations



Sweeping things under the rug

Unless you are her
➤➤➤➤➤➤➤➤ you likely
will not get away with it;
and it's a real bad idea
anyways.

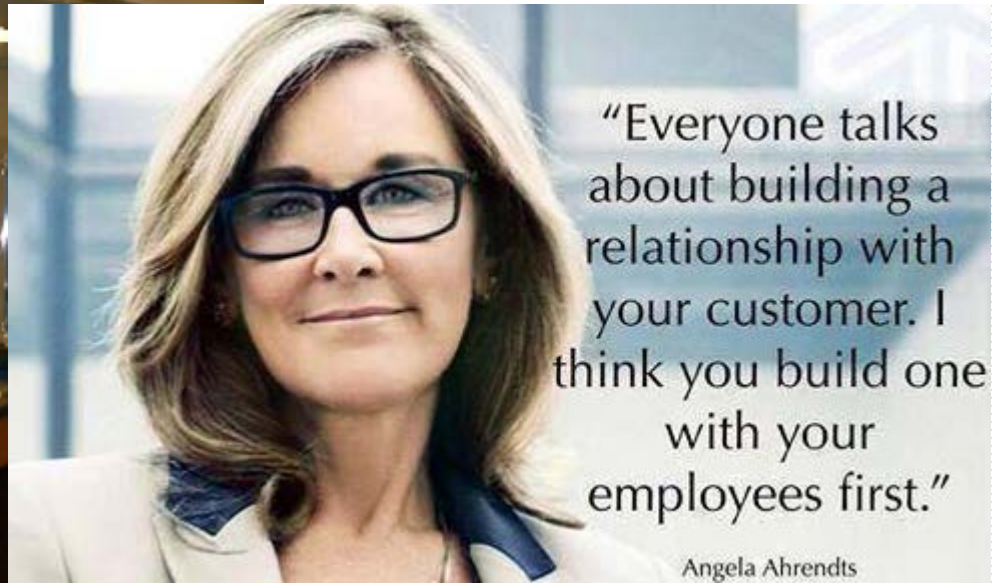
Remind me of this slide
when we do harassment later
in the year.



Day to Day Issues: One

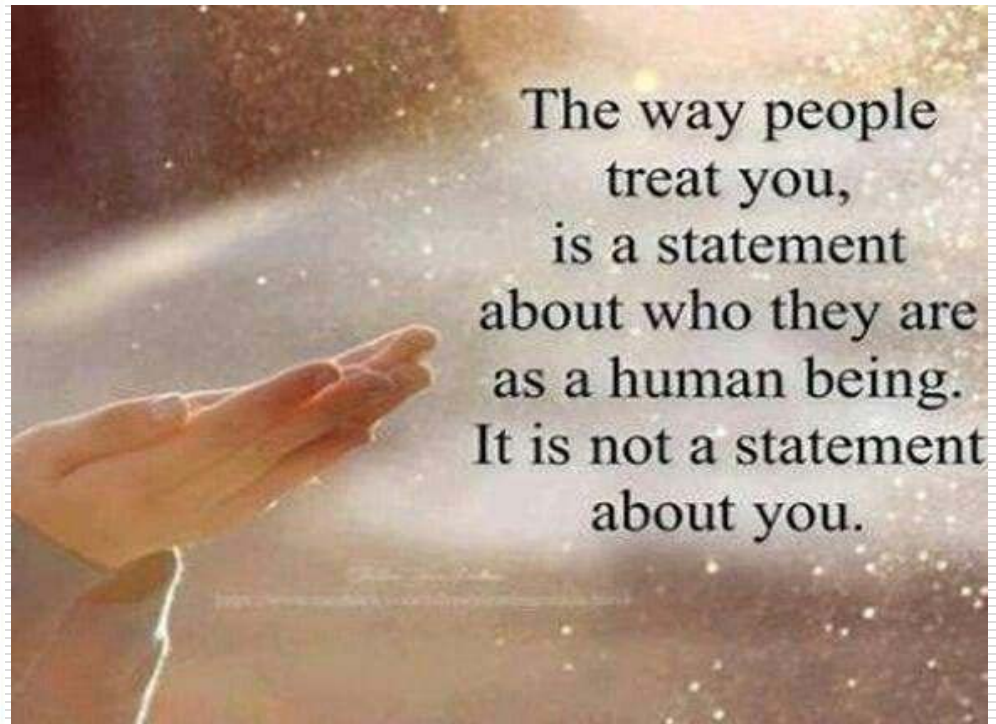


Day to Day Issues: Two



Day to Day Issues: Three

**BE NICE
OR
LEAVE
-THANK YOU**



The way people
treat you,
is a statement
about who they are
as a human being.
It is not a statement
about you.

Day to Day Issues: Four



- Assess your Safety Protocols**
 - Are they being followed?**
 - Are personnel trained?**
 - Are they accurately addressed in procedures?**
 - Are they enforced?**
-

Day to Day Issues: Five



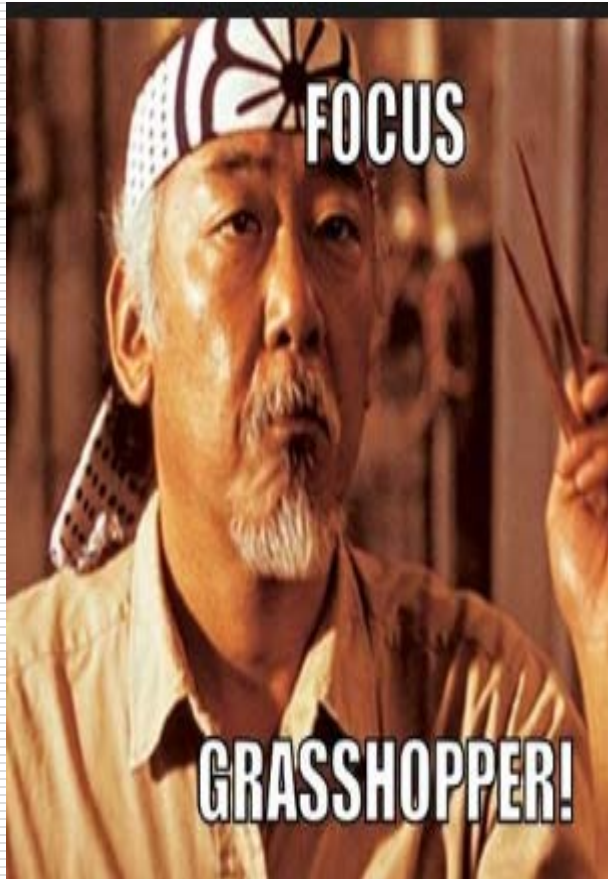
- Where are you most often hurt?**
 - Internally?
Externally?**
 - What can you do to prevent / mitigate?**
-

Day to Day Issues: Six



**Screw Ups Happen –
Internal Controls
Procedures; Training
and Documentation
Help.**

Now – lets consider a few items in detail:





Do You Really Understand E-Sign? I am Thinking No. Here is Why --

By:
R. Todd Sherpy
Sherpy & Jones Law P.A.
Credit Union Resources &
Educational Services, LLC
Post Office Box 2599
Lexington, SC 29071
Atlanta Phone 770-631-3527
SC Phone 803 356-3327
rts@sherpy-jones-law.com



Copyright: © CURES, LLC, 1994-2018 - all rights reserved.

Introductory Notes: **The Message is not Registering**



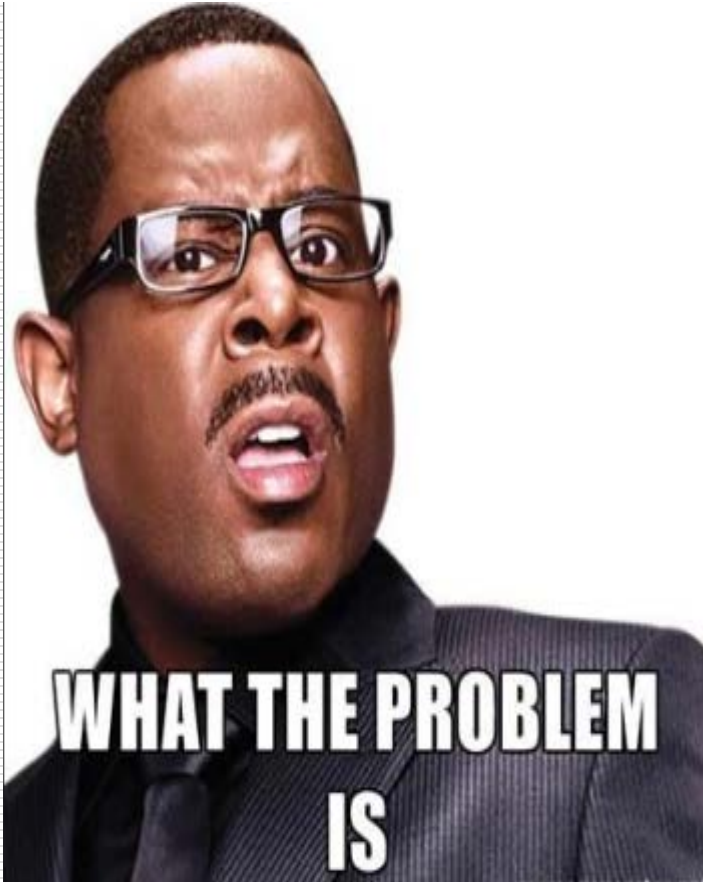
Introductory Notes: **If you want the Historical Notes**



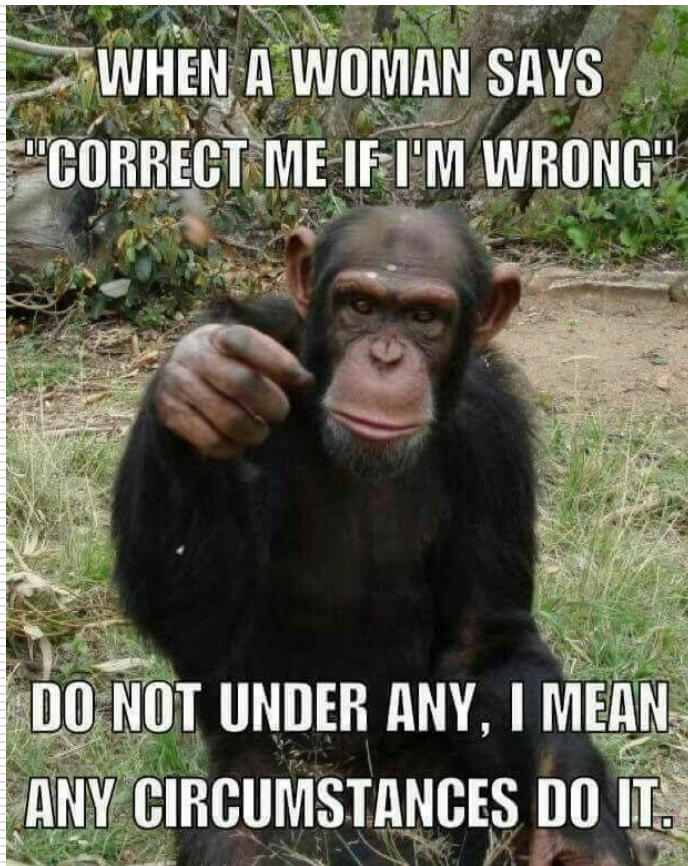
Electronic Disclosures; E-Sign; UETA and Electronic Records

2015

Introductory Notes: **The Problem is ...**



To Assess You Need to Understand the Steps:



Step One: Availability of Paper Delivery or Paper Copies



Before seeking a consumer's consent to use electronic records, institutions *must inform the consumer in a clear and conspicuous statement of any right or option to have the record provided in non-electronic form, the right to withdraw that consent, the consequences of withdrawing consent (including terminating the relationship), and any fees imposed in the event of withdrawal.* Institutions must also inform consumers of their right to request a paper copy of an electronic record and whether any fees apply.

Step Two: Consent Choices



Before seeking a consumer's consent to the use of electronic records, a financial institution must inform the consumer in a clear and conspicuous statement *whether consent relates to a particular transaction only or whether consent relates to broader categories of information.*

Step Three: Consumer Actions



Before seeking consent, financial institutions must disclose to consumers the procedures to withdraw consent at a later date and to update the consumer's contact information, such as notifying the financial institution when the consumer's e-mail address changes.

Step Four: Hardware & Software Requirements



Before seeking consent, financial institutions must provide consumers with a statement detailing the hardware and software requirements to access and retain electronic records.

Step Five: “Affirmatively Consent”



To ensure a consumer can communicate electronically with the financial institution to which consent has been provided, the E-Sign Act requires that the consumer provide consent electronically "in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent."

Step Six: Disclose



Give Disclosure.

TRUTH-IN-LENDING DISCLOSURE STATEMENT
(THIS IS NOT A CONTRACT FOR A COMMITMENT TO LEND.)

Applicant: _____ Proposed By: _____
 Property Address: _____ Date Proposed: _____
 Application No: _____

ANNUAL PERCENTAGE RATE	FINANCE CHARGE	AMOUNT FINANCED	TOTAL OF PAYMENTS
The rate of your credit as a yearly rate.	The dollar amount the credit will cost you.	The amount of credit provided to you or on your behalf.	The amount you will have paid after making all payments as scheduled.
%	\$	\$	\$

DEQUIRED DEPOSIT: The annual percentage rate does not take into account your required deposit.
PAYMENTS: Your payment schedule will be:

Number of Payments	Amount of Payment	Number of Payments	Amount of Payment	When Payment Is Due	Number of Payments	Amount of Payment	When Payment Is Due

DEMAND FEATURE: This obligation has a demand feature.
 VARIABLE RATE FEATURE: This loan contains a variable rate feature. A variable rate disclosure has been provided earlier.

CREDIT LIFE/ACCIDENT/DEATHLITY: Credit life insurance and credit disability insurance are not required to obtain credit, and will not be provided unless you sign and agree, on page 3b, to obtain credit.

<input type="checkbox"/> Credit life insurance <input type="checkbox"/> Credit life <input type="checkbox"/> Credit disability <input type="checkbox"/> Credit life and disability	<input type="checkbox"/> No credit disability insurance <input type="checkbox"/> I want credit life insurance <input type="checkbox"/> I want credit disability insurance <input type="checkbox"/> I want credit life and disability insurance	<input type="checkbox"/> Property insurance <input type="checkbox"/> Flood insurance <input type="checkbox"/> Signature <input type="checkbox"/> Signature <input type="checkbox"/> Signature
---	---	---

INSURANCE: The following insurance is required to obtain credit:
 Credit life insurance No credit disability Property insurance Flood insurance
 This may obtain the insurance from anyone you want that is acceptable to credit.
 If you purchase _____ property Flood insurance from another you will pay it for a one year term.
SECURITY: You are giving a security interest in:
 This goods or property being purchased Real property you already own.
PREPAID FEES: &
LATE CHARGE: If a payment is more than _____ days late, you will be charged \$ _____.
PREPAYMENT: If you pay off early, you:
 may will not have to pay a penalty.
 may will not be credited as a credit of part of the finance charge.
ASSIGNMENT: Insurance, including your property.
 may may not assign the remainder of your loan on the original terms.
 See your insurance documents for any additional information about assignment. Assign, any required assignment in full before the scheduled date and payment schedule and penalties.
 I require an estimate All other oral or written disclosures except the late payment disclosure are estimates.
 ***NOTE: The Department of Consumer Affairs requires copies for Mortgage Lenders or Applicants, to include Property, Personal Insurance.

THE UNDERSIGNED ACKNOWLEDGES RECEIVING A COMPLETED COPY OF THIS DISCLOSURE.

 (Applicant) (Date)

 (Applicant) (Date)

 (Lender) (Date)

549a Form - 10/01/00

Step Seven: “Re-Consent”



To ensure continued electronic access, financial institutions must provide consumers with a statement detailing any revised hardware and software requirements for access to and retention of electronic records, and the right to withdraw consent without the imposition of any fees for such withdrawal and without the imposition of any condition or consequence that was not disclosed. After providing this statement, institutions must again obtain consumers' affirmative consent as in Step 5. *The procedures in Step 7 must be followed when the changes in hardware and software requirements create a material risk that consumers will not be able to access or retain electronic records.*

The Real Bugger is Step Five

The most difficult part of the E-Sign Act's rules involves the correct method for consumers to "demonstrate" that they can access the required information electronically (Step 5). To ensure compliance with this requirement, financial institutions are encouraged to develop procedures to ensure they maintain records of the consumer's consent process. A financial institution's failure to obtain consumer consent properly can significantly affect its compliance with consumer laws and regulations such as Regulation E's error resolution procedure.

EXAMPLE: Under Regulation E, the customer generally has 60 days from receiving a periodic statement to claim an error. If the statements are sent only electronically and the e-sign consent requirement was not obtained properly, the error period could be extended until a paper statement that includes the error is provided.

What Congress Intended

Mr. MCCAIN. Is it the Senator's understanding that pursuant to subsection 101(c)(1)(C)(ii) of the conference report a consumer's affirmative consent to the receipt of electronic records needs to "reasonably demonstrate" that the consumer will be able to access the various forms of electronic records to which the consent applies?

Mr. ABRAHAM. Yes. The conference report requires a "reasonable demonstration" that the consumer will be able to access the electronic records to which the consent applies. By means of this provision, the conferees sought to provide consumers with a simple and efficient mechanism to substantiate their ability to access the electronic information that will be provided to them.

Mr. MCCAIN. I agree. The conferees did not intend that the "reasonable demonstration" requirement would burden either consumers or the person providing the electronic record. In fact, the conferees expect that a "reasonable demonstration" could be satisfied in many ways. Does the Senator agree with me that the conferees intend that the reasonable demonstration requirement is satisfied if the consumer confirmed in an e-mail response to the provider of the electronic records that he or she can access information in the specified formats?

Mr. ABRAHAM. Yes. **An e-mail response from a consumer that confirmed that the consumer can access electronic records in the specified formats would satisfy the "reasonable demonstration" requirement.**

What Congress Intended II

Mr. MCCAIN. Does the Senator also agree with me that the **"reasonable demonstration" requirement would be satisfied, for instance, if the consumer responds affirmatively to an electronic query asking if he or she can access the electronic information or if the affirmative consent language includes the consumer's acknowledgement that he or she can access the electronic information in the designated format?**

Mr. ABRAHAM. Yes. A consumer's acknowledgment or affirmative response to such a query would satisfy the "reasonable demonstration" requirement.

Mr. MCCAIN. **Would the "reasonable demonstration requirement" be satisfied if it is shown that the consumer actually accesses records in the relevant electronic format?**

Mr. ABRAHAM. Yes. The requirement is satisfied if it is shown that the consumer actually accesses electronic records in the relevant format.

Mr. MCCAIN. Mr. President, I appreciate my colleague's willingness to participate in this colloquy to clarify the clear intent of the conference with respect to this provision.



Example of Demonstrable Consent: Email and Response

We have been offering electronic statements for a couple years and our current process is to have the consumer open a sample PDF document which contains a specific "code". Before E-Statements may be accessed or "consented" to, the consumer must provide us with the specific code to "demonstrate" they can access and view the statements.

Very Cumbersome? Yes ...



Woman Kills Boyfriend Who Fake Proposed As An April Fools Prank -

A New York woman is facing murder charges after she allegedly shot her boyfriend for playing an April Fools prank

Example of Demonstrable Consent II: Email Still

Simple E-Statement Scenario: The customer must log into online banking and then open a pdf document. We will be sending the customer a notification via email that their current statement is available, but the email is in no way necessary in order for the customer to view the statement. In order to enroll the consumer must log into online banking, agree to the terms and conditions by checking an accept box, and provide a confirmation code they will obtain by opening a pdf located on the terms and conditions page. The following verbiage is contained in the agreement - You understand that if you do not receive an email notification, it does not release you from the responsibility to review your electronic statement promptly and notify the bank of any errors within 30 days of the statement date.

Demonstrable Consent and Your Credit Union

It is going to depend on how it is all tied together contractually. If you have a compliant E-Sign system, delivery happens when you push the button regardless of whether the recipient ever looks at it. Getting the system to meet Step 5 is the key.

**RISK-BASED
DECISION MAKING**



Establishing Demonstrable Consent:

Electronic Delivery Consent For U.S. Bank Easy Checking

You must review and agree to the **E-SIGN Consent Agreement** before submitting your application. Please print or save a copy for your records.

- I, **Jon Doe**, consent to the terms of the **E-SIGN Consent Agreement** and have been advised to print or save a copy of the E-SIGN Consent Agreement for my records. I also confirm that I agree to receive required disclosures and communications electronically from U.S. Bank.

Required Disclosures For U.S. Bank Easy Checking

Please read the following required disclosures for your Deposit Account and either **Print** or **Save** them for your records.



[Deposit Account Agreement.pdf](#)



[Consumer Pricing Information Brochure.pdf](#)

- I, **Jon Doe**, agree I can and did access the required disclosures listed above. I further confirm that I have read and printed or saved the disclosures.

Acceptance For U.S. Bank Easy Checking

All applicant(s) consent and agree to the following:

- All information on this application is true and accurate.
- The computer being used meets the **system requirements** necessary to receive and view this and other electronic communication.
- All disclosures and agreements provided have been received, reviewed, and retained, including, but not limited to the E-SIGN Consent Agreement and the Required Disclosures listed above.
- All terms and conditions provided in disclosure and agreements.
- To grant U.S. Bank permission to verify customer identity and prevention of fraud through the use of third party verification tools and public databases.

Demonstrable Consent (Making it fit???)

Agreement

After reviewing the following documents please print a copy of each for your records and check the box below:

- I Agree:** By clicking the 'I agree' box, I confirm that: (1) I can access and read this [Electronic Signature Agreement](#); and (2) I can print on paper the disclosure and signature card or save or send the disclosure and signature card to a place where I can print it, for future reference and access; and (3) Until or unless I notify the Credit Union as described above, I consent to receive, through electronic means, all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to me by the Credit Union during the course of my relationship with you.

 - I Agree:** By clicking the 'I agree' box, I confirm that I have read, understand and agree to the Founders Federal Credit Union [Membership Agreement](#), [Negative Information Disclosure](#), [Privacy Policy Agreement](#), [Electronic Funds Transfer Agreement and Disclosure](#), [Fee Schedule](#).
-

Consumer Disclosures & Risks of Not Meeting Steps Discussed.

Most of the regulations that govern day-to-day banking operations (Regs E, DD, and CC for example) require disclosures, and in most cases these disclosures must be "written", "in writing", "in a form the consumer may keep", or otherwise capable of retention for the consumer's later reference.

If you fail to provide these "written" disclosures in proper form, you may be exposed to civil liability--it's just like you didn't give the disclosures at all! In cases of with systemic violations this can quickly multiply into a staggering aggregate civil liability by way of a class action lawsuit.



Smart Devices; Zip Drives and Other Options???

<http://www.bankersonline.com/forum/ubbthreads.php?ubb=showflat&Number=1658205>

http://www.bankersonline.com/technology/guru2010/gurus_tech101810c.html

<https://www.bankersonline.com/forum/ubbthreads.php/topics/1190682/re-demonstrate-able-consent-for-esign-and-disclosure>

Smart Devices; Zip Drives and Other Options???

II

Multiple Access Devices

Your acceptance of this agreement on one Access Device constitutes your acceptance on all Access Devices you use. For example, if you view and accept this agreement on a mobile device, the terms of this Agreement will apply to electronic documents accessed on a traditional computer (or vice versa).

Additionally, by viewing and accepting this agreement on any Access Device, you are reasonably demonstrating your ability to access and view electronic documents in the format that the services are provided on that Access Device and all subsequent Access Devices. If you change Access Devices (or use multiple Access Devices), it is your responsibility to ensure that the new Access Device meets the applicable system requirements and that you are still able to access and view electronic documents on the subsequent Access Device. Continuing your application on other Access Devices is your reaffirmation of this Agreement.

Please contact us at 1-800-USBANKS (1-800-872-2657) if you have difficulties accessing or viewing electronic documents on your selected Access Device.

Acceptance

You will be asked to acknowledge your acceptance of these terms by checking the box before you are able to continue with your application. In doing so, you are confirming that you meet the system requirements described above, that you have demonstrated your ability to receive, retain, and view electronic documents on your Access Device, and that you have an active and valid email address.

Record Retention

UETA & Evidence Laws provide that legal effect, enforceability or validity requires that electronic records be:

1. Capable of being retained; and
2. Capable of being accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or other record.

This applies to electronic signatures stored in a computer or server, so that any printout or output readable by sight, shown to reflect the data accurately, is considered an original. In the case of an electronic signature, then, it is important to demonstrate to the satisfaction of the courts that: (1) the appropriate level and amount of information surrounding the signing process was accurately retained, and (2) the system used to retain the information is itself reliable.

Perfect System?





**Why do Some Fail at
ADA Compliance?**

ADA/Websites How Did We Get Here and Where Do Things Stand Now?

**By:
R. Todd Sherpy
Sherpy & Jones Law P.A.
Credit Union Resources &
Educational Services, LLC
Post Office Box 2599
Lexington, SC 29071
Atlanta Phone 770-631-3527
SC Phone 803 356-3327
rts@sherpy-jones-law.com**



Copyright: © CURES, LLC, 1994-2018 - all rights reserved.

It's Not a New Thing ...



- **Our First Community Notice on this was October 2010**
 - **CUNA/CMG's First "Risk Alert" was September 2014.**
 - **We have issued 18-Notices on this Topic; and ADA Web Accessibility Primer and Suggested Website Notices / Disclosures on ADA Accessibility.**
 - **So – Why the Shock?**
-

The Shock Comes from Complacency – Dilly Dilly.



**Thoughts on Credit
Union Websites
Generally:**

34



From the Beginning.



History

ADA Overview

- Americans With Disabilities Act of 1990
- 42 U.S.C. § 12101 et seq.
- Rulemaking & Enforcement Authority: US-DOJ

Application of ADA to Business

No discrimination on basis of disability in enjoyment of goods/services “of any place of public accommodation by a person who owns, leases . . . or operates a place of public accommodation” **Public accommodation includes financial institutions.**

From the Beginning.

A recent study
found that women
who carry a
little extra
weight live
longer than the
men who mention it!



History II

Application of ADA to Business -- *Is website a “place of public accommodation”?*

Courts Are Split:

- Website without connection to physical place might not be public accommodation. *Cullen v. Netflix*, 600 Fed. Appx. 508 (9th Cir. 2015).
- But see *Nat'l Federation of the Blind v. Scribd*, 97 F.Supp. 3d 535 (D. Vt. 2015), quoting *Carparts Distrib. Ctr., Inc. v. Auto Wholesaler's Ass'n of New England*, 37 F.3d 12, 19 (1st Cir. 1994).

Recent Case to Note:

In another website accessibility case, [Andres Gomez v. Bang & Olufsen America, Inc.](#), the sole issue before a Florida district court was whether the retailer defendant's website was a place of public accommodation under the ADA. In granting the retailer's motion to dismiss, the court relied on cases concluding that a website that is wholly unconnected to a physical location is generally not subject to ADA. The court noted that the plaintiff had alleged that he could not purchase products online, but did not claim that the website's inaccessibility impeded his ability to go to a store, despite the fact that the website allowed users to make private appointments with sales representatives at a physical location.



Does it Or Does it Not?

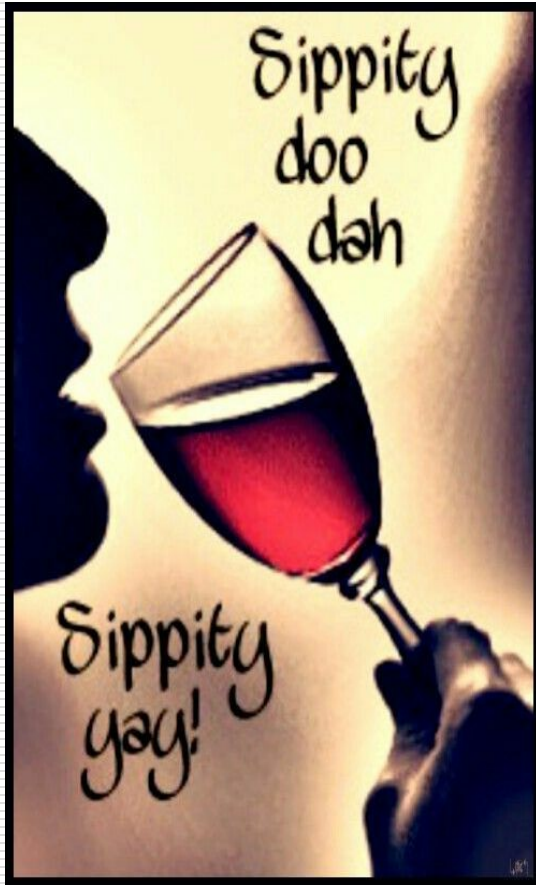


History III

DOJ Rules History 2010 thru 2018 ...



Likely it Applies

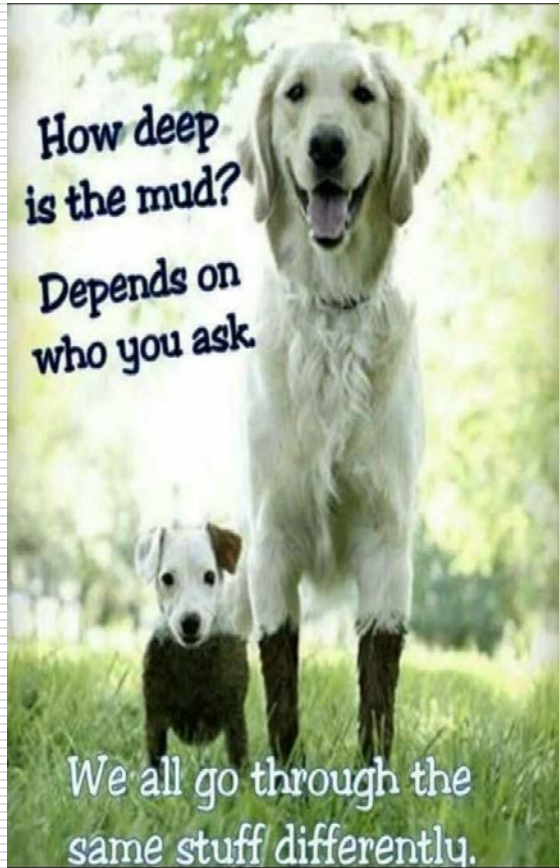


History IV

Despite not finalizing formal rules that require businesses that are public accommodations, like CUs, to adopt website accessibility standards, DOJ intervened in some private lawsuits and entered into consent orders with some entities. Examples include:

- 2009-2010 – Airline Cases
- 2011: Wells Fargo (bank had existing policies to improve accessibility, and pledged to continue efforts in a settlement agreement)
- 2013: H&R Block (DOJ intervened in a private suit, in a consent decree H&R Block agreed to adopt “recognized international industry standards for web accessibility, known as the Web Content Accessibility Guidelines (WCAG) 2.0”) *2014 CMG Issued Risk Alert*

The Rest of the Story:



History V

Non-Specific Website Accessibility Rules –

DOJ Regulations: 28 C.F.R. Part 36

36.303(a): Must ensure that no one with a disability is denied services, segregated or treated differently because of the absence of auxiliary aids and services.
Exceptions:

- Providing aids/services would fundamentally alter the nature of the goods, services, offered; OR
- Providing aids/services would result in an **undue burden**, i.e., significant difficulty or expense.

The Rest of the Story:



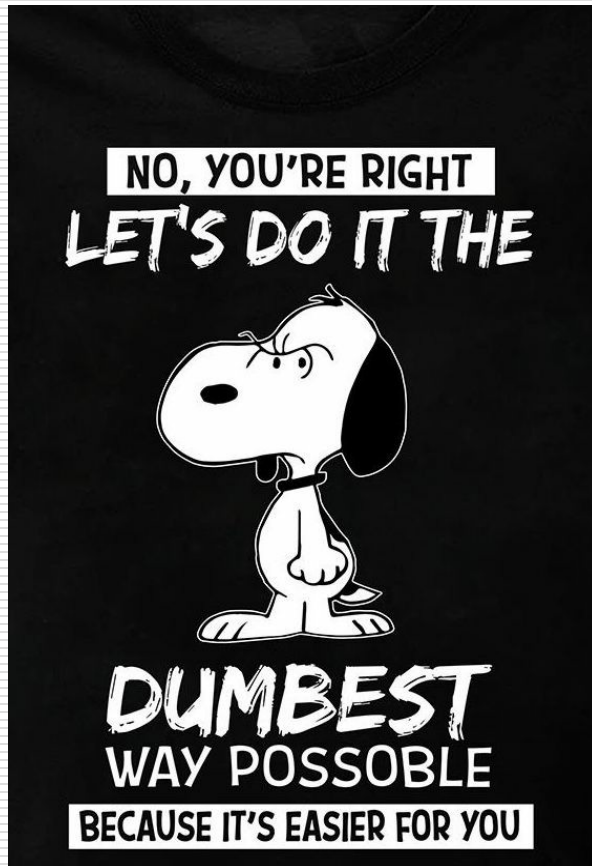
History VI

Non-Specific Website Accessibility Rules –

DOJ Regulations: 28 C.F.R. Part 36

- 36.303(c): *shall furnish auxiliary aids and services necessary to ensure effective communication with individuals with disabilities.*
 - 36.303(b): provides examples of auxiliary aids and services including “qualified readers” and “other effective methods of making visually delivered materials available to individuals who are blind or have low vision,” and acquiring or modifying equipment or devices.
-

The Rest of the Story:



History VII

Specific Website Accessibility Rules –

- 36.203: must provide goods/services in the most integrated setting appropriate to needs of the individual
- Regulations include specific standards for ATMs, but nothing for websites
- Section 508 regulations (revised effective 3/20/17, compliance required 1/18/18) adopt WCAG 2.0 A and AA – Applies Only to Federal Agencies -- Not applicable to private entities! **BUT...**

Statutory
Interpretation



The Rest of the Story:



History VIII

- De Facto standard: WCAG 2.0 AA
- Web Content Accessibility Guidelines 2.0 AA --
Developed by World Wide Web Consortium
(W3C) Web Accessibility Initiative

Includes guidelines to make sites functional with aids and usable for persons with disabilities, e.g.:

- Text alternatives for non-text content
 - Color, contrast, and font size guidance
 - Functions available from keyboard (not require mouse)
 - Avoid content that causes seizures (flashing, etc.)
-

So – What Happened?



WHAT EXACTLY IS AN
**AMBULANCE
CHASER?**



What is Motivating these Actions?



Not Justice, Making the World a Better
Place, Curing Legal Deficiencies --- Just
Pure Unadulterated Greed.

Is there Exposure?

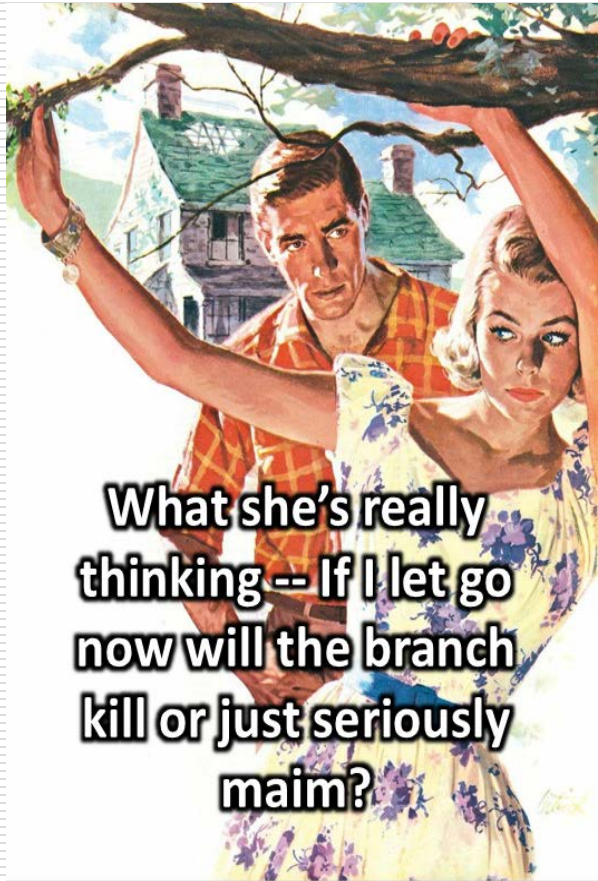


There is a broad range of exposures – ranging from moderate to extreme.

On average cases are settled for between \$10,000 and \$25,000 (90% of which goes to the lawyers).



Facing Reality and Recent Credit Union Wins

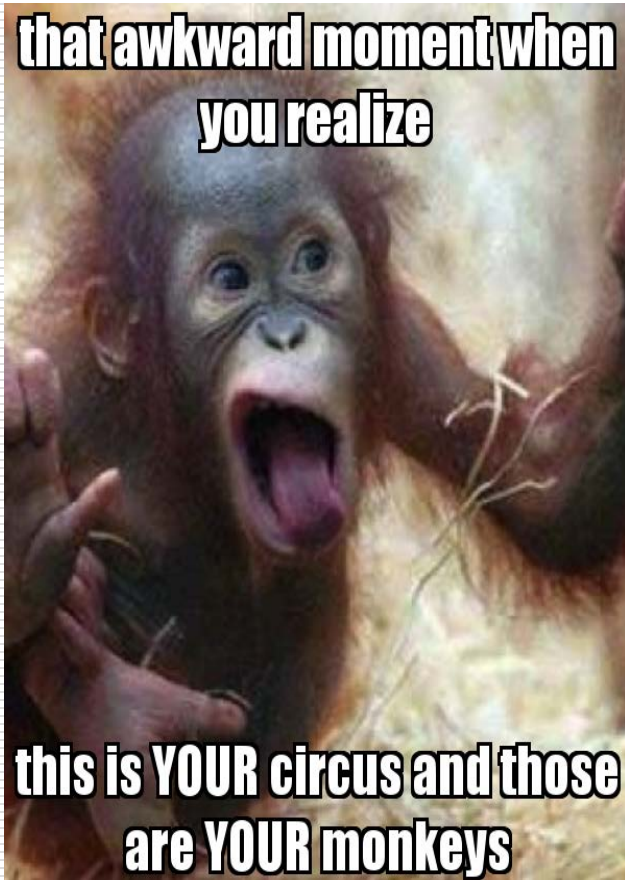


The Recent wins are nice, but ...

Winning on Technicalities versus Substantive Wins.



What Should The Credit Union Be Doing?

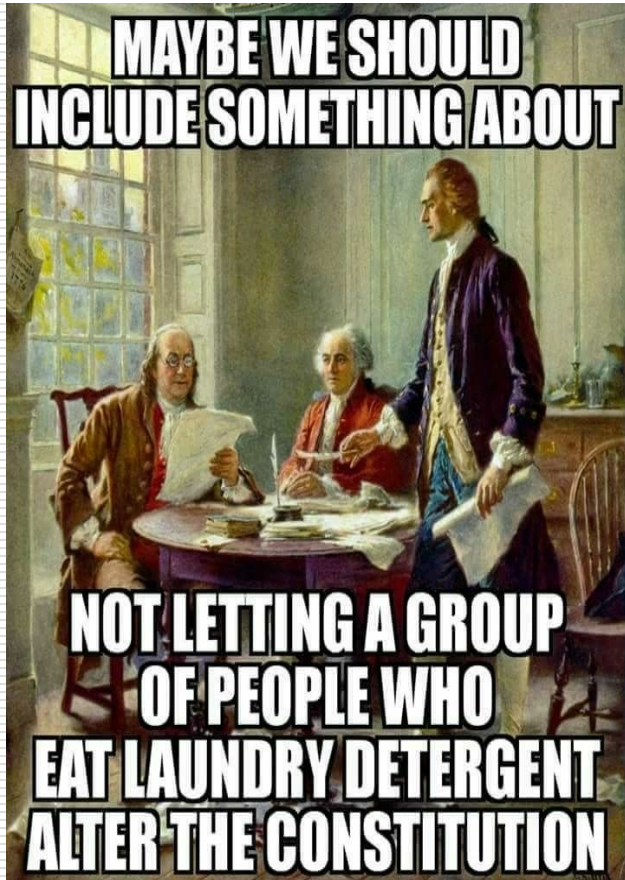


Recognize ADA compliance obligation
Website and mobile infrastructure

- **Budget**
- **Marketing impact**
- **Develop a plan**
- **Emerging legal standards**
- **Hire competent consultants**

**Achieve substantial compliance in
reasonable time frame**

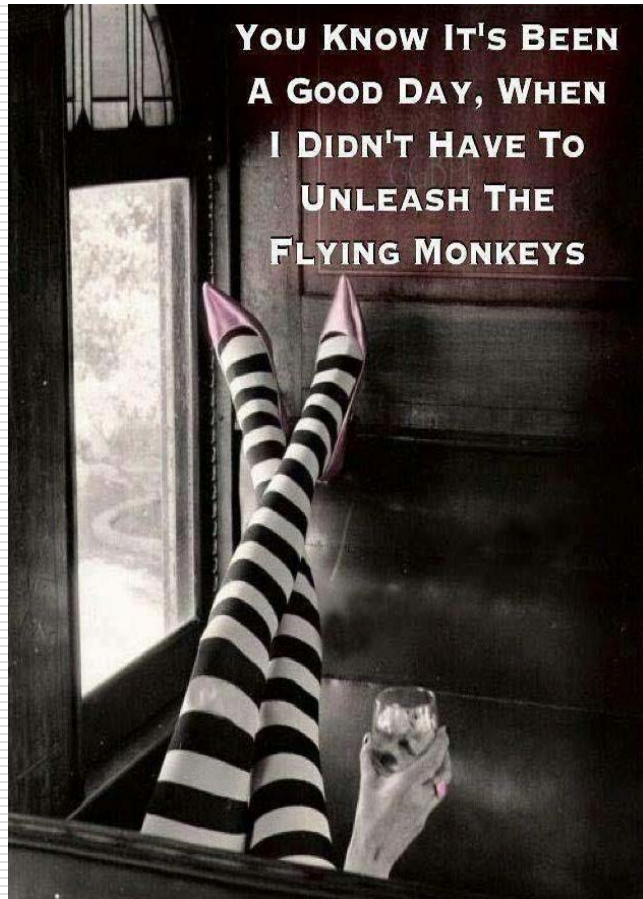
What Should The Credit Union Be Doing II?



Maintain compliance

- Future changes to website/mobile
 - New technologies
 - Complaints
 - Periodic audits
-

If you Receive a Claim or Demand?



1. Notify your bond/insurance carrier.
 2. Consider a Website ADA Assessment and Remediation per your risk-assessment.
 3. Consider discussing the matter with your legal counsel. Some of these demands do not list a represented party (plaintiff) by name. For instance, some here in Georgia list the client as “a blind Georgian.” We have written several letters to “educate” the sender of these letters; and I must admit to also convey my opinion of the senders. Without a named person we cannot even assess whether there is a potential claim (based on FOM issues).
 4. Consider whether there is a need to formally document an “undue burden defense” to such claims based on our prior writings.
-

Other Steps to Consider:



Every Credit Union's Situation is Unique

Go Back and Read

1. Primer on ADA Accessibility

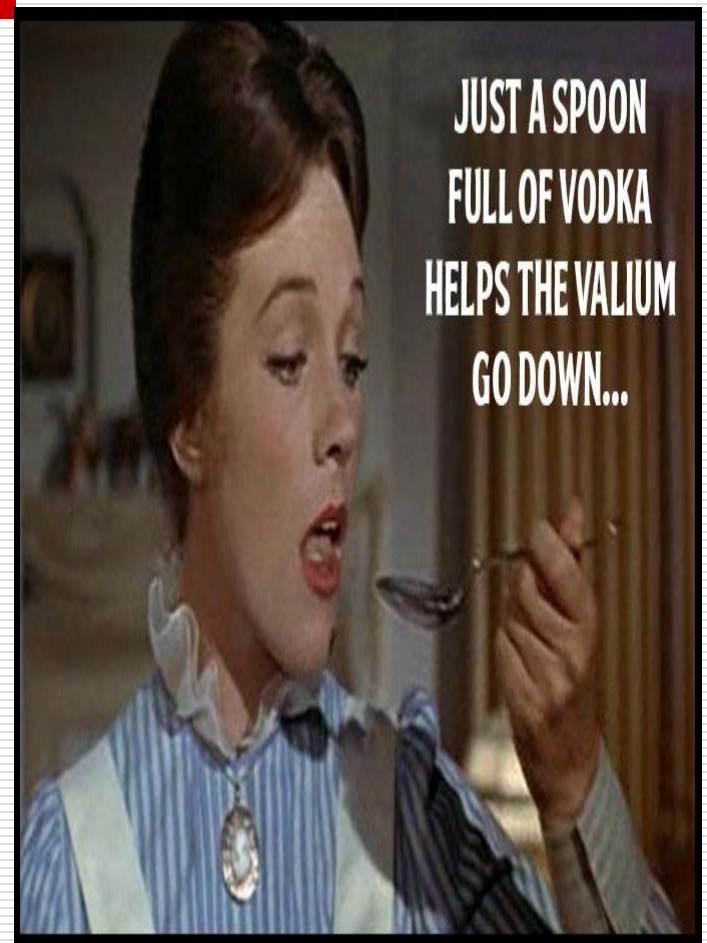
2. Community Notices:

- N88-2017 – More on ADA Website Issues
 - N90-2017- ADA “Letters - Demands” and Action Steps (Whether we Like them or not)
 - N100-2017 – Final Thoughts on ADA Demand Letters From the “Wrong” Coast Law firm in California.
 - 16-2018 – ADA and Your Website – Some Basics to Consider and Liability Protection
-

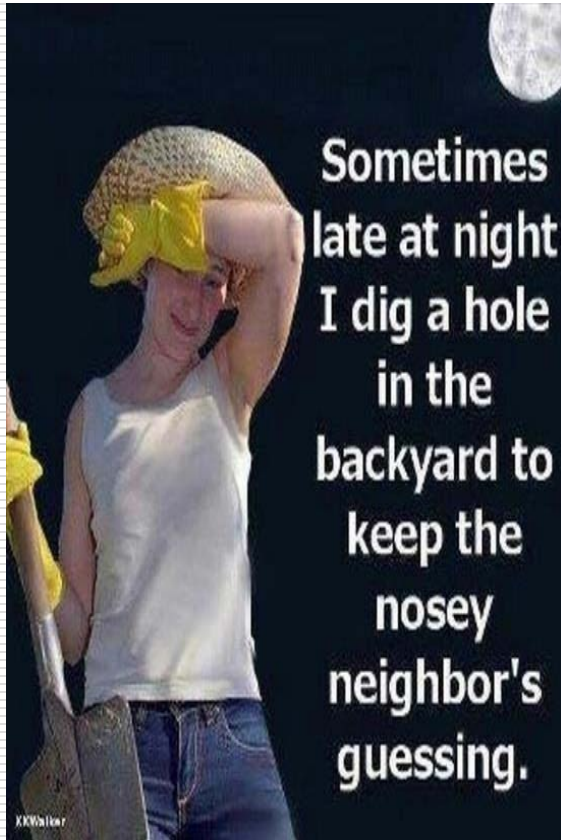
Assess Undue Hardship as Applicable WITH QUALIFIED LEGAL COUNSEL

The Credit Union is not required to accommodate individuals with disabilities if doing so creates an undue hardship on the Credit Union. An accommodation may be an undue hardship when it requires “significant difficulty or expense” to implement.

The concept of undue hardship includes any action that is **unduly costly, extensive, substantial, or disruptive, or that would fundamentally alter the nature or operation of the business.**



Assessing Undue Hardship



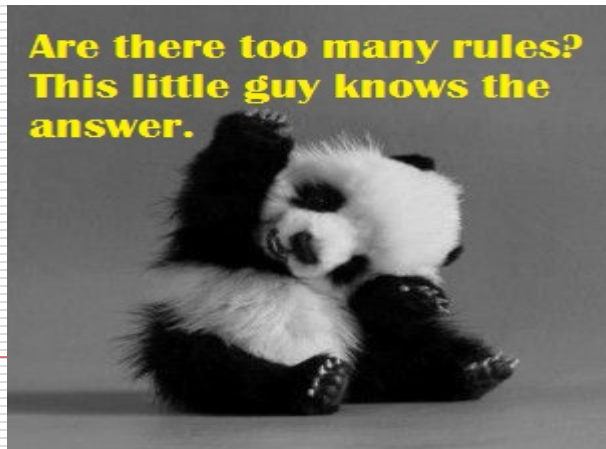
The Credit Union must consider the following factors when determining whether an accommodation is an undue hardship.

- The nature and net cost of the accommodation needed, considering tax incentives
 - The number of persons employed/served by the Credit Union and the overall size of the organization
 - The financial resources of the Credit Union
 - The structure of the Credit Union's operations
 - The impact of the accommodation on the operation of the facility
-

More on Accommodation

If a particular accommodation would be an undue hardship, the Credit Union should try to identify another accommodation that would not pose such a hardship. If cost is the cause of the undue hardship, the Credit Union should also consider whether funding for an accommodation is available from an outside source, such as local service organizations, the Department of Rehabilitation, and the Public Utilities Commission. Alternatively, the Credit Union should also give a job applicant /employee / affected person with a disability an opportunity to provide the accommodation or pay for the portion of the accommodation that constitutes an undue hardship.

**Are there too many rules?
This little guy knows the
answer.**



Adopt ADA Accessibility Policy and Statement




"You misspelled 'constant criticism'."

Why?

Risk Management and Mitigation

CUPP & Other Resources

	Americans with Disabilities Act
1	Americans with Disabilities Act Policy and Procedures
2	Americans with Disabilities Act Audit
3	DOJ ADA Checklist for Existing Facilities
4	DOJ Guidance_2010ADASTandards_prt
5	DOJ Common Errors in New Construction

Web Accessibility Initiative (WCAG 2.0) – [Http://www.w3.org/WAI/](http://www.w3.org/WAI/)

“ADA Toolkit” which is the first place I’d state. They label this as “Best Practices.”

<https://www.ada.gov/pccatoolkit/chap5toolkit.htm>





Georgia Bankers Resource:

[http://resources.gabankers.com/e-Bulletin/images/2016/Oct%2014/GBAversion Checklist re ADA Compliance-v1.pdf](http://resources.gabankers.com/e-Bulletin/images/2016/Oct%2014/GBAversion%20Checklist%20re%20ADA%20Compliance-v1.pdf)

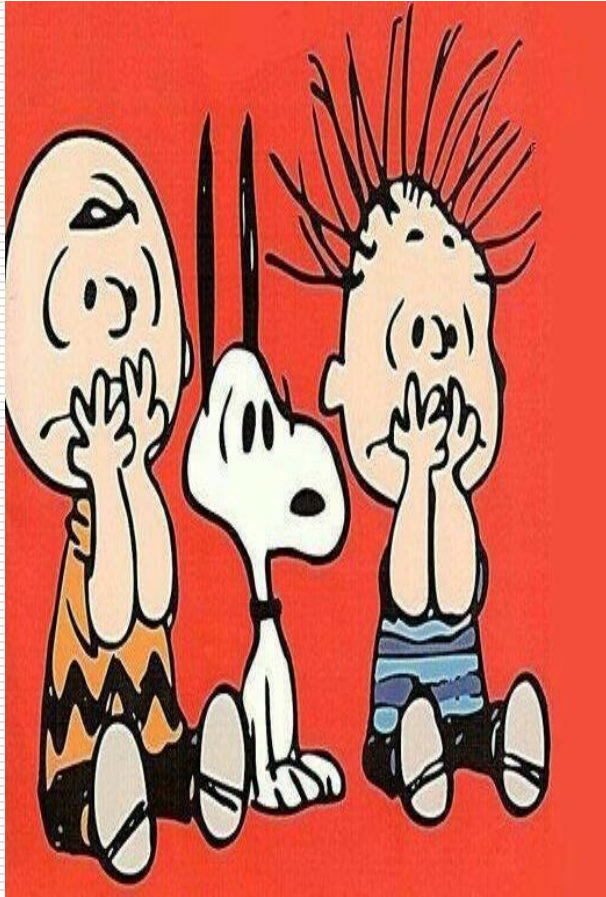
CUPP & Other Resources

K- Electronic Banking

Web Accessibility Assessment Resources

 1- Primer on ADA Web Accessibility and ...	3/1/2017 9:59 AM	Microsoft Word D...	74 KB
 2- Website Accessibility Under Title II of t...	3/1/2017 10:00 AM	Microsoft Word D...	74 KB
 3- Website Accessibility Under Title II of t...	3/1/2017 10:01 AM	Microsoft Word D...	69 KB
<hr/>			
 O- Basic ADA Accessibility Statement	1/22/2018 6:19 PM	Microsoft Word D...	14 KB

Other Notes:



Court Dismisses Website Accessibility Case as Violating Due Process, Since DOJ Still Has Not Issued Regulations:

California district court recently granted Dominos Pizza's motion to dismiss under the primary jurisdiction doctrine, which allows courts to stay or dismiss lawsuits pending the resolution of an issue by a government agency. In *Robles v. Dominos Pizza LLC*, U.S. Dist. Ct. North Dist. Cal. Case No. CV 16-06599 SJO, the court held it would violate Domino's due process rights to hold that its website violates the ADA, because the Department of Justice still has not promulgated regulations defining website accessibility – despite issuing a notice of proposed rulemaking back in 2010.

Other Notes II:

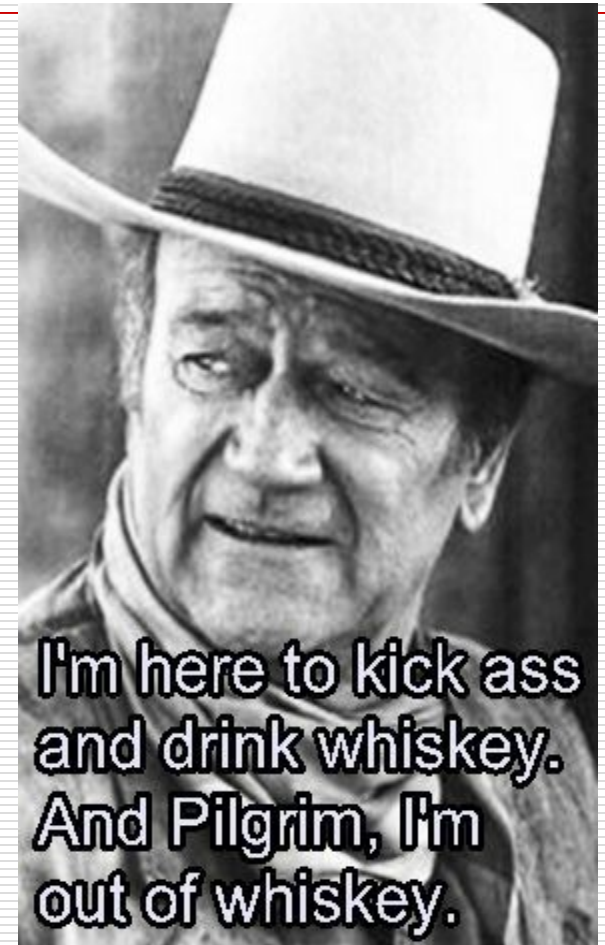
The court stated that the DOJ's application of an industry standard, the Website Content Accessibility Guidelines 2.0 (WCAG 2.0), in statements of interest and consent decrees in other cases does not impose a legally binding standard on all public accommodations. It also noted that those consent decrees indicated flexibility to choose an appropriate auxiliary aid to communicate with disabled customers, and suggested that Domino's provision of a telephone number for disabled customers may satisfy this obligation. Retailers that do not have an accessible website should therefore provide a toll-free number serviced by live customer service agents who can provide all the information and services available on the website.

NOTE: The court rejected Dominos' argument that the ADA simply does not apply to websites. It found distinguishable those cases holding that the ADA does not apply to retailers and service providers that operate solely on the internet, without a nexus to a brick and mortar location. It noted that Dominos "does not challenge the existence of a 'nexus' between its websites and its pizza franchises."



Final Notes:

1. **Future Concerns – Services Provided via Third Parties**
2. **Fighting Fire With Fire?**



**LOOK OUT, EVERYBODY! I'M
GONNA BE CRABBY FOR
THE REST OF THE DAY!!**



Vendor Contract Management – Where you are Failing in the Game of Vendor Management and Considerations on Fixing the Problems

By:

R. Todd Sherpy

Sherpy & Jones Law P.A.

**Credit Union Resources &
Educational Services, LLC**

Post Office Box 2599

Lexington, SC 29071

Atlanta Phone 770-631-3527

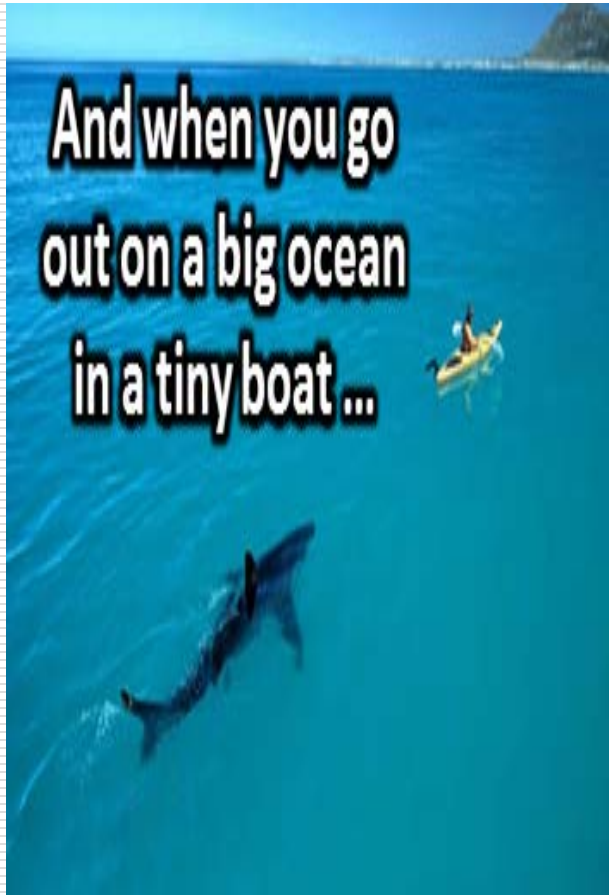
SC Phone 803 356-3327

rts@sherpy-jones-law.com



Copyright: © CURES, LLC, 1994-2018 - all rights reserved.

When Vendor Management became a Mere Checklist ...



OCC Warns Banks Against Complacency

- **Growing risk and regulatory concerns with inadequate resources.**
 - **Interconnected third party risks that are not visible.**
 - **Silos of third party oversight.** Allowing different departments to go about third party management without coordination, collaboration, consistent processes, information, and approach leads to inefficiency, ineffectiveness, and lack of agility. This is exacerbated when organizations fail to define responsibilities for third party oversight and the organization breeds an anarchy approach to third party management leading to the unfortunate situation of the organization having no end-to-end visibility and governance of third party relationships.
-

When Vendor Management became a Mere Checklist ...



OCC Warns Banks Against Complacency II

- **Document, spreadsheet, and email centric approaches.** When organizations govern third party relationships in a maze of documents, spreadsheets, and emails it is easy for things to get overlooked and buried in mountains of data that is difficult to maintain, aggregate, and report on. There is no single source-of-truth on the relationship and it becomes difficult, if not impossible, to get a comprehensive, accurate, and current-state analysis of a third party. To accomplish this requires a tremendous amount of staff time and resources to consolidate information, analyze, and report on third party information. When things go wrong, audit trails are non-existent or are easily covered up and manipulated as they lack a robust audit trail of who did what, when, how, and why.

When Vendor Management became a Mere Checklist ...



OCC Warns Banks Against Complacency III

- **Inadequate processes to monitor changing relationships.** Organizations are in a constant state of flux. Governing third party relationships is cumbersome in the context of constantly changing regulations, risks, processes, relationships, employees, processes, suppliers, strategy, and more. The organization has to monitor the span of regulatory, geo-political, commodity, economic, and operational risks across the globe in context of its third party relationships. Just as much as the organization itself is changing, each of the organization's third parties is changing introducing further risk exposure.

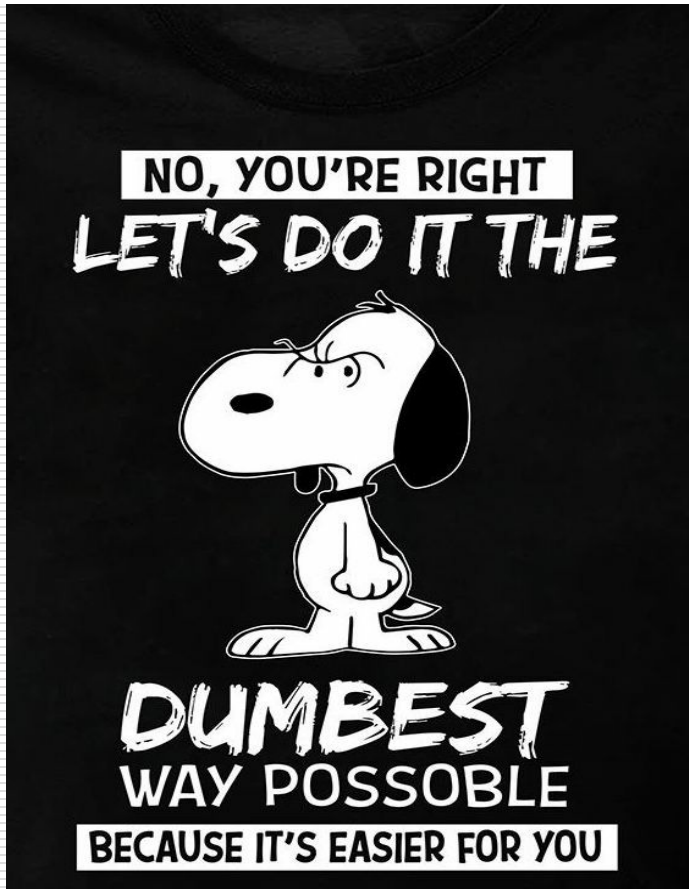
When Vendor Management became a Mere Checklist ...



OCC Warns Banks Against Complacency IV

- **Third party performance evaluations that neglect risk and compliance.** Metrics and measurements of third parties often fail to properly encompass risk and compliance indicators. Too often metrics from service level agreements (SLAs) focus on delivery of products and services by the third party but do not include monitoring of risks, particularly compliance and ethical considerations.
- **Worse.** Not considering your own people and experience.

Very Real and High Risks Associated with Non-Compliance or Just Poor Compliance



- 1. You Can Be Sued.**
 - 2. You're a target.**
 - 3. You might face some severe consequences.**
 - 4. Regulatory Penalties:** The CFPB, OCC and other regulators have been extremely active in bringing enforcement actions resulting in Consent Orders or settlements related to failures to properly manage third-party risk. In these cases, the penalties have been severe and do not begin to account for the ancillary expenses involved in responding to the action itself. Nor do they account for the costs associated with compliance or vendor programs that could have been avoided had there been effective processes throughout the vendor relationship.
-

Challenge and Fragmented Reality – Accept it, then do something about it.

I made it through
the day without
beating
anyone with
a chair.
I'd say my
people skills
are improving!

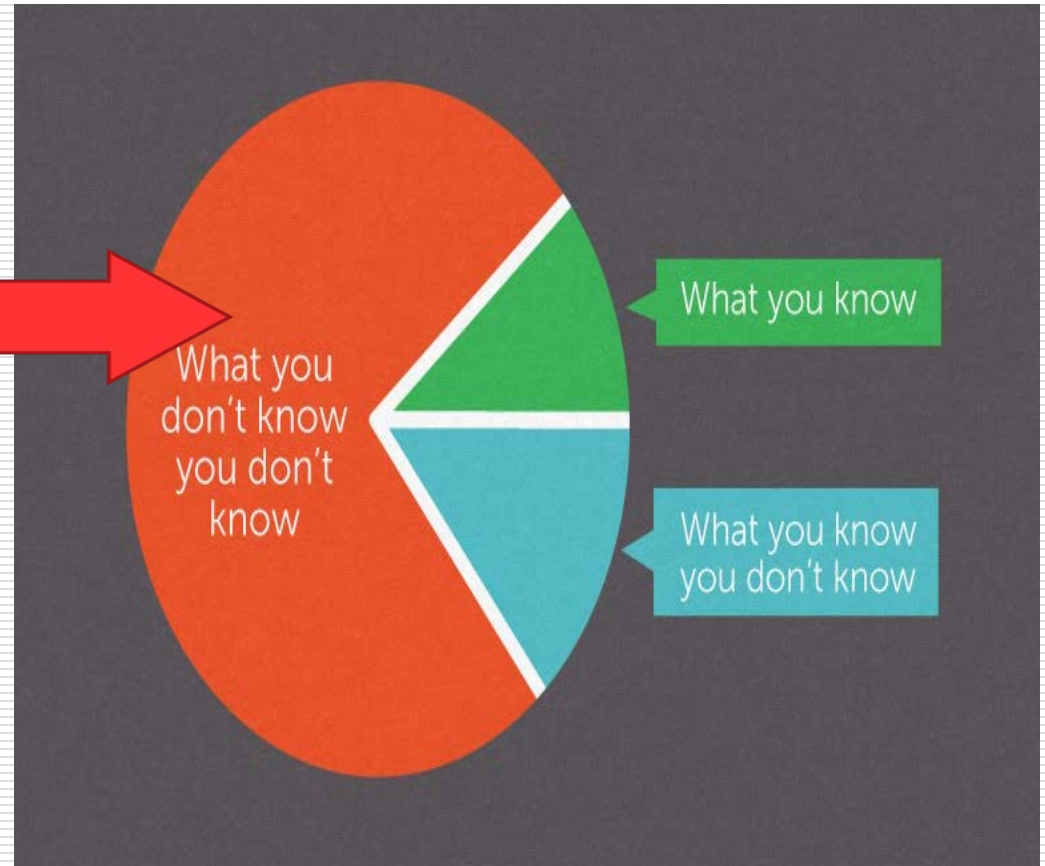


The challenge: Can you attest to the governance, risk management, and compliance or third parties across your organization's business relationships?

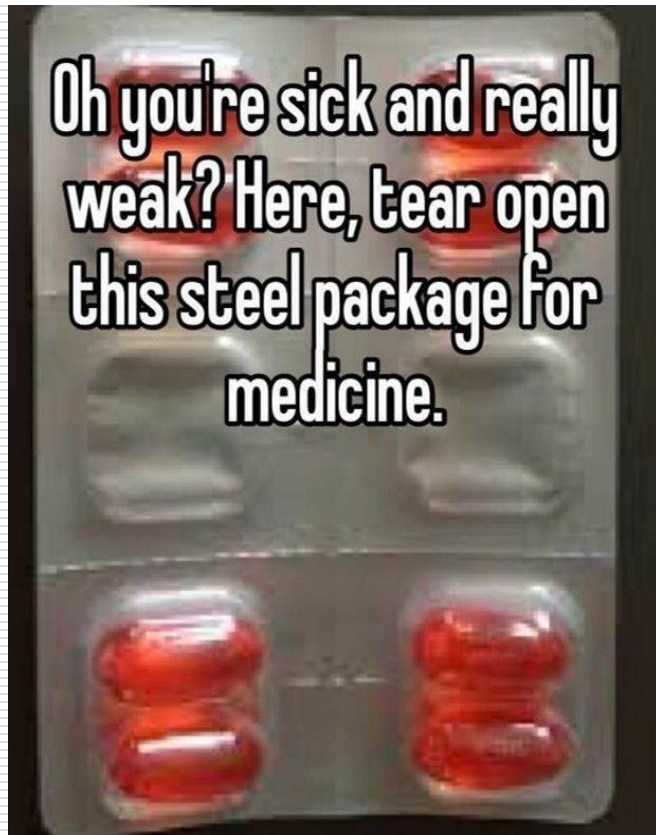
Reality: Organizations manage third parties differently across different departments and functions with manual approaches involving thousands of documents, spreadsheets, and emails. Worse, they focus their efforts at the formation of a third party relationship during the on-boarding process and fail to govern risk and compliance throughout the lifecycle of the relationship.

This fragmented approach to third party governance brings the organization to inevitable failure. Reactive, document-centric, and manual processes cost too much and fail to actively govern, manage risk, and assure compliance throughout the lifecycle of third party relationships. Silos leave the organization blind to the intricate exposure of risk and compliance that do not get aggregated and evaluated in context of the organization's goals, objectives, and performance expectations in the relationship.

Even Worse – Outsourcing, Ignorance and Bliss?

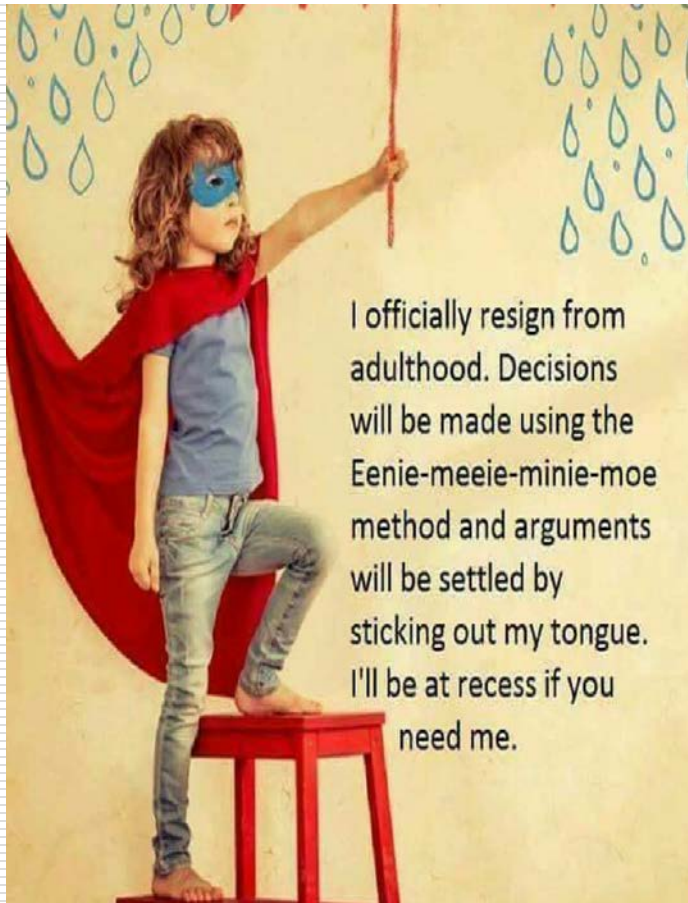


Let's Go Back to the Beginning:



NCUA and FFIEC Guidelines or Requirements (See NCUA Letter Nos.: 00-FCU-11;07-FCU-13; 01-CU-20; and 08-FCU-09 as applicable. We also assess per the recent issuance on governance of third party relationships and industry standards per OCC 2013-29 (Issued October 30, 2013)

What NCUA Really Wants --



The NCUA outlines its expectations in Supervisory Letter No.: 07-01, Evaluating Third Party Relationships. Its guidance is based on three key concepts:

- 1. Risk assessment and planning**
 - 2. Due diligence**
 - 3. Risk measurement, monitoring and control**
-

What NCUA Really Wants II --



Risk assessment should begin by looking within. A credit union should know how much strategic risk its willing to embrace based on its strategic plans, business plans, and philosophies. There should be a discussion about long and short-term goals, and an action plan to address these goals. Similarly, officials should weigh the risks and benefits of outsourcing business functions with the risks and benefits of maintaining those functions in-house. The officials must clearly understand the credit union’s strengths and weaknesses in relation to the third-party relationship. Only then can the credit union conduct an initial assessment of a vendor and follow up with monitoring and regular reviews. The NCUA wants to see “measurable, achievable goals and clearly defined levels of authority and responsibility.” Credit unions should develop detailed financial projections, outlining the range of expected and possible financial outcomes. Credit unions should also project a return on their investment in the proposed third party arrangement, considering expected revenues, direct costs, and indirect costs. including the cost of monitoring vendors.

What NCUA Really Wants III--

If a woman says
'do what you want'



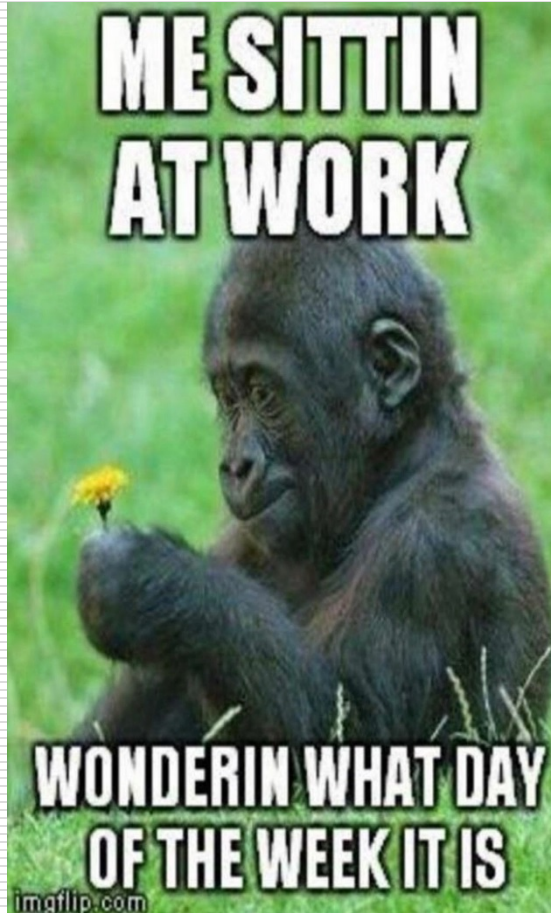
Do not do what you want.
Stand still, do not blink,
do not answer, don't even
breathe, just play dead

The discussion of risk should be detailed. The seven types of risk (credit, interest rate, liquidity, transaction, compliance, strategic, and reputation) should be analyzed with respect to:

- **Expectations for outsourced functions**
- **Staff expertise**
- **Criticality**
- **Risk-reward or cost-benefit of the relationship**
- **Insurance**
- **Impact on membership**
- **Exit strategy**

NOTE: Less complex vendors may be subject to simpler risk assessments that are part of a broader risk management program or documented in proper Credit Union records.

What NCUA Really Wants IV -



Due Diligence

Due diligence should be tailored to the complexity of the third-party relationship. Not every vendor requires the same level of due diligence. More complex relationships mandate a wider breadth of due diligence and requires deeper digging. Examiners, when evaluating a credit union's vendor management program will consider a credit union's "risk profiles, internal controls and overall complexity" when reviewing an institution's approach. Necessary elements may include:

- Background check
 - Business model
 - Cash flows
 - Financial operational control review
 - Accounting considerations.
 - Contract issues and legal review.
-

What NCUA Really Wants V -



Contracts -

The section on contracts is particularly detailed. Credit unions should exercise their rights to negotiate contracts to achieve terms that are mutually beneficial to both parties, such as favorable early termination, escape clauses and default terms. Contracts should emphasize a credit union's safety or soundness and should be reviewed by legal professionals, who are versed in the specific nature of the contact. Special emphasis is placed on reviewing a vendor's practices to ensure they comply with all laws and regulations, including consumer regulations, as ultimately, the risk will rest with the credit union.

What NCUA Really Wants VI -



Risk Measurement, Monitoring and Control of Third Party Relationships

From the beginning of the vendor relationship, a credit union should have clearly outlined expectations and regularly measure performance to ensure those expectations are met. Third party arrangements and risk profiles will vary; thus, credit unions risk mitigation efforts will vary, as well. To assess whether a credit union effectively mitigates risk, examiners will assess the following items in light of the risks identified, the vendor management program and the complexity of the credit union:



What NCUA Really Wants VII -

Risk Measurement, Monitoring and Control of Third Party Relationships

Policies and procedures. Policies should outline expectations and limit risk. Policies, supplemented with procedures should outline staff responsibilities and reporting schedules. Additionally, policies should set forth the content and frequency of vendor management reporting to credit union management and officials.

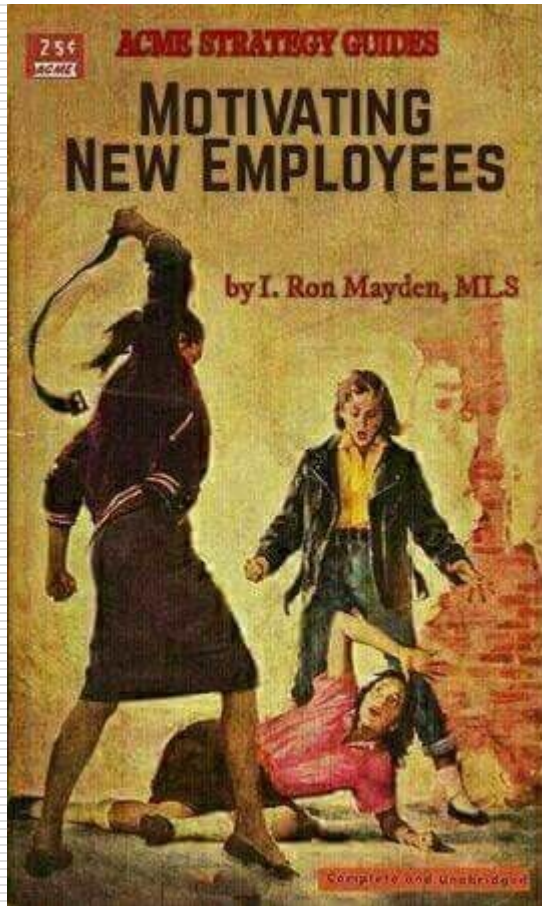
Risk measurement and monitoring. Credit unions need to be able to measure a vendor's risks and performance, including "profitability, benefit, and service delivery." Controls to measure these should be included in the contract. Independent auditors should periodically verify the accuracy of the results. Recognizing that vendor management is a significant task, the guidance also says that examiners want to see that a credit union has the "staff, equipment and technology" to reliably monitor a vendor.

Control systems and reporting. Like all elements of vendor risk management, ongoing controls should depend on the complexity of the vendor and the vendor relationship and be designed to mitigate risk. They should be part of the credit union's ongoing risk management and should be adjusted as needed. The staff responsible for overseeing these controls and reports should be knowledgeable and provide management and others periodic reports with enough detail for them to evaluate a vendor's performance.

Not just a Freakin' Checklist!



It Takes a Team



Vendor Risk Management Framework

First it should be part of larger Enterprise Governance Risk and Compliance Program...

Second it should consider numerous risk types...

Third, it should be based on five main pillars:

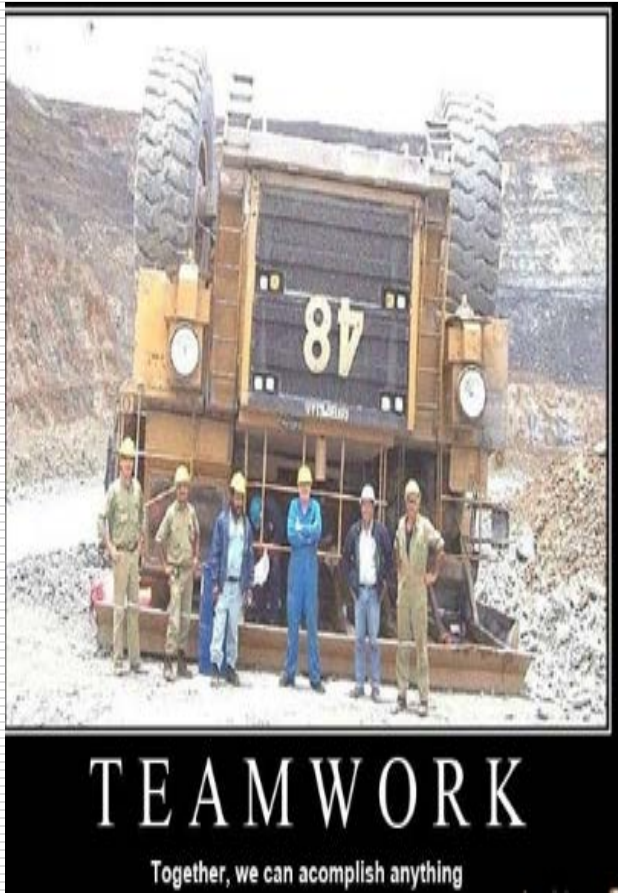
1. Due Diligence & Vendor Selection
2. Risk Assessment
3. Contract Management
4. Monitoring and Oversight
5. Exit Plan



It Takes a Team II



It Takes a Team III













Risks to Consider and Address:

- Inadequate understanding internally and externally of expectations
 - Broader range of risks not considered
 - Lack of expertise within the institution on what the vendor actually does
 - Approaching without a continuous improvement mindset
 - Accountability not clearly defined
 - Lack of investment in internal audits
 - Training and communication not funded
 - Information to support the program and survive an audit was not considered and/or defined
-

Resources:

CUPP (Section E / Subfolder O)

Name	Date modified
 1- Vendor Management Policy (2015)	11/12/2015 12:50 ...
 2- Vendor Management and Due Diligen...	11/12/2015 1:38 PM
 3- Vendor Due Diligence Assessment (20...	4/20/2016 9:59 AM
 4- 712 CUSO Due Diligence	4/16/2008 2:47 PM
 5- Vendor Management Monitoring Chart	9/6/2011 10:28 AM
 6 - OCC Country Risk Assessment Manual	3/11/2008 8:08 AM
 7- Sample Termination - Renewal Letter	4/13/2010 12:16 PM
 8- Vendor Due Diligence Questionnaire	9/21/2013 2:22 PM
 8- Vendor Due Diligence Questionnaire	9/21/2013 2:30 PM
 9- Appendix to Cover Cyber-Security and...	1/18/2018 6:54 AM

Resources:

WebEx

My Event Recordings

Search Result:

Total: 3 recordings

Topic	Security ⓘ	Panelist	Type	Date ▲
Vendor Management Focus – Electronic Services Contracts and Cyber-Security-20170131 1900-1 In this session I will address common issues that are overlooked and are expected per applicable gui...		Todd Shery	Unlisted	January 31, 2017
S&S Units and Credit Union Call Center 20160520 1900-1 In this session we will address a great number of truths about these systems; risks and how to mitig...		Todd Shery	Unlisted	May 20, 2016
Real Vendor Management – “Assessing Vendor Contracts”-20160211 1900-1 In this session we will address the regulatory guidelines on assessing vendor agreements; and then t...		Suzanne Vesper is an Attorney in the Compliance Section of Shery & Jones.	Unlisted	February 11, 2016

Resources:

Recommended Regulatory Reading:

<https://consumercomplianceoutlook.org/2012/fourth-quarter/vendor-risk-management-compliance-considerations/>

<https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>

- **OCC Bulletin 2002-16: Foreign-Based Third-Party Service Providers**
 - **FIL-44-2008: Guidance for Managing Third-Party Risk**
 - **FIL-50-2001: Bank Technology Bulletin: Technology Outsourcing •SR 13-19: Guidance on Managing Outsourcing Risk**
 - **SR 00-4 (SUP): Outsourcing of Information Technology and Transaction Processing**
 - **CFPB Bulletin 2012-03: Service Providers**
-

Resources:

Recommended Reading on ERM / Vendor Management - Series: **NO FIVE**

- <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk/>
 - <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-chapter-two/>
 - <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-chapter-three-risk-assessment/>
 - <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-chapter-four-the-pain-points/>
 - <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-chapter-six-contracting/>
 - <https://iapp.org/news/a/monitoring-third-party-vendors-means-managing-your-own-risk-chapter-seven/>
 - <https://iapp.org/news/a/vendor-management-means-managing-your-own-risk-part-eight/>
 - <https://iapp.org/news/a/monitoring-third-party-vendors-means-managing-your-own-risk-chapter-nine/>
 - <https://iapp.org/news/a/third-party-vendor-management-means-managing-your-own-risk-a-checklist/>
-

Resources:

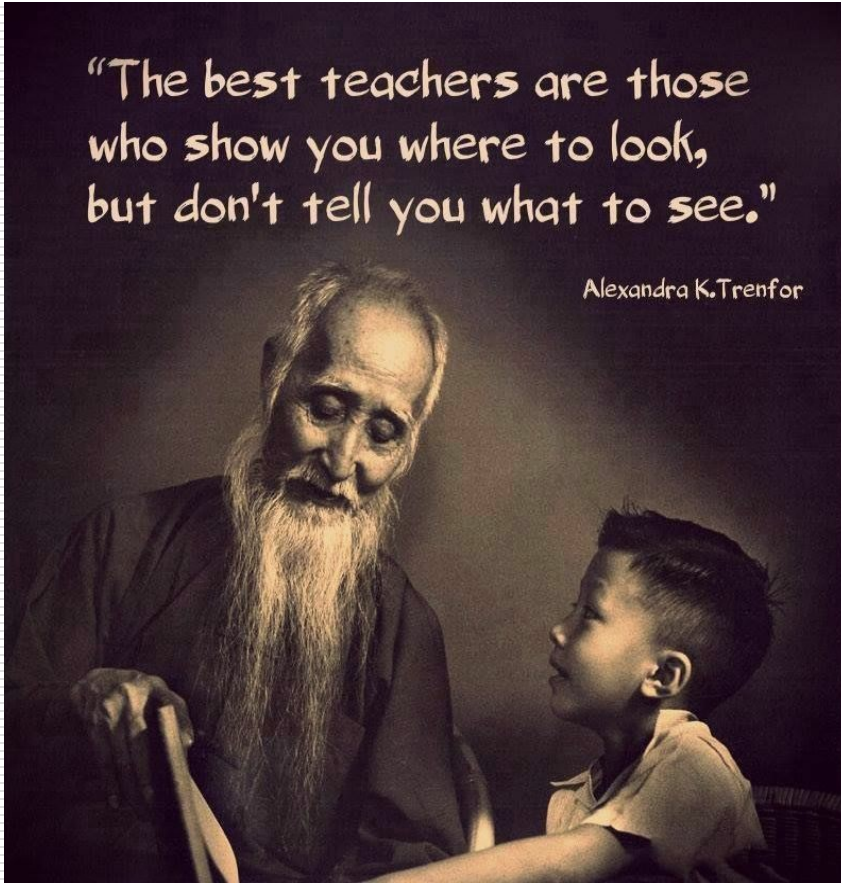
Recommended Reading on Vendor Management :

- <https://www.bridgepointconsulting.com/best-practices-reducing-third-party-risk-vendor-soc-reports/>
 - <https://www.vendorcentric.com/single-post/2017/02/07/3-Types-of-Risk-You-Should-Be-Managing-with-Your-Riskiest-Vendors>
 - <https://www.upguard.com/articles/five-things-to-know-about-third-party-risk>
 - https://www.mckinsey.com/~media/mckinsey/dotcom/client_service/risk/working%20papers/46_third_party_risk.ashx
 - <https://bankingjournal.aba.com/2015/06/vendor-risk-management-when-its-done-right-its-never-done/>
-

Final Notes:

"The best teachers are those
who show you where to look,
but don't tell you what to see."

Alexandra K. Trenfor



Questions:

Sherpy & Jones P.A.
POST OFFICE BOX 2599
LEXINGTON, SC 29071

**CREDIT UNION RESOURCES AND
EDUCATIONAL SERVICES, LLC (“CURES”)
104 PENINSULA DRIVE
PEACHTREE CITY, GA 30269
770-631-3527
PHONE: (803) 3563327
RTS@SHERPY-JONES-LAW.COM**



Need Help
Prepping
for Your
Next
Meeting
with
Regulators?