Equifax Data Breach: Your Vital Next Steps

David A. Reed

Partner, Reed & Jolly, PLLC

Ann Davidson

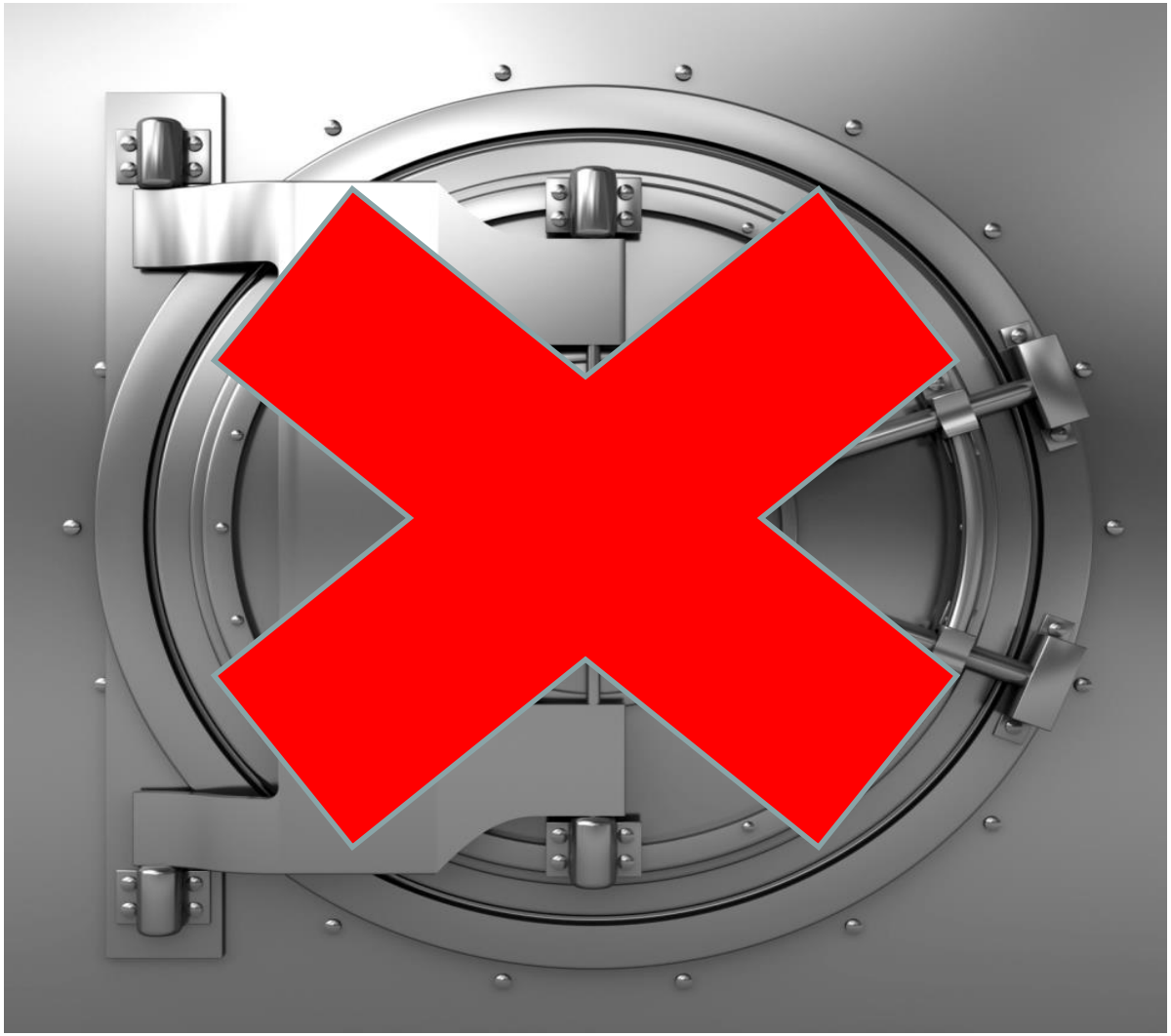
Vice President Risk Consulting/ Bond Division Allied Solutions, LLC

Do You Remember When this Was the Biggest Threat to Data Security?

NAFCU

Reed & Jolly, PLLC

Traditional Security



Reed & Jolly, PLLC

Poll Question 1

- Does your Credit Union have a Data Breach Policy?
  - A) Yes
  - B) No

Data Breach

- So many headlines and so little time……
  - Anthem, OPM, Home Depot, Target, DoD
- There is a significant difference between a card breach and a data breach
- Cards can be re-issued but social security numbers and mother's maiden names cannot!
- This is a HUGE examination issue

This Just In!

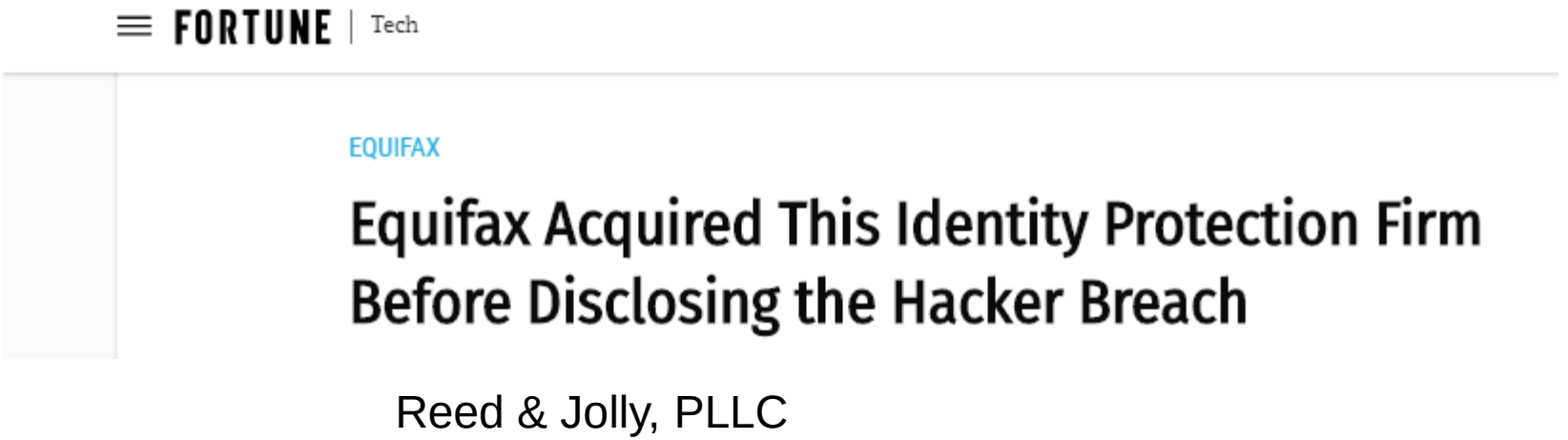
- Equifax credit reporting agency breached!

- The breach lasted from **mid-May through July**.
- The hackers accessed **143 million people's names, Social Security numbers, birth dates, addresses and, in some instances, driver's license numbers**.
- They also stole credit card numbers for about 209,000 people and dispute documents with personal identifying information for about 182,000 people.

Mt. Everest of Data Breaches

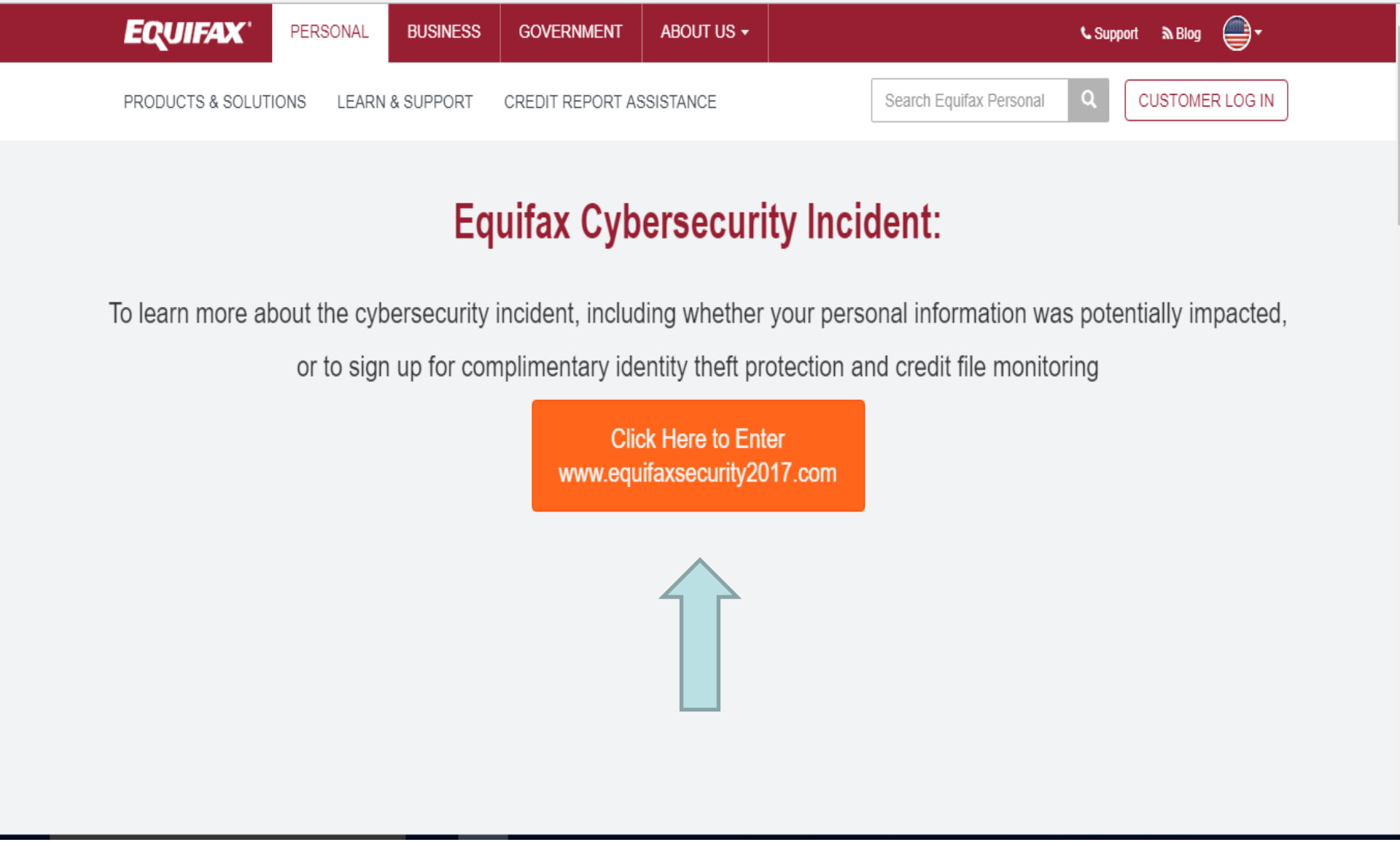
CNBC

NPR



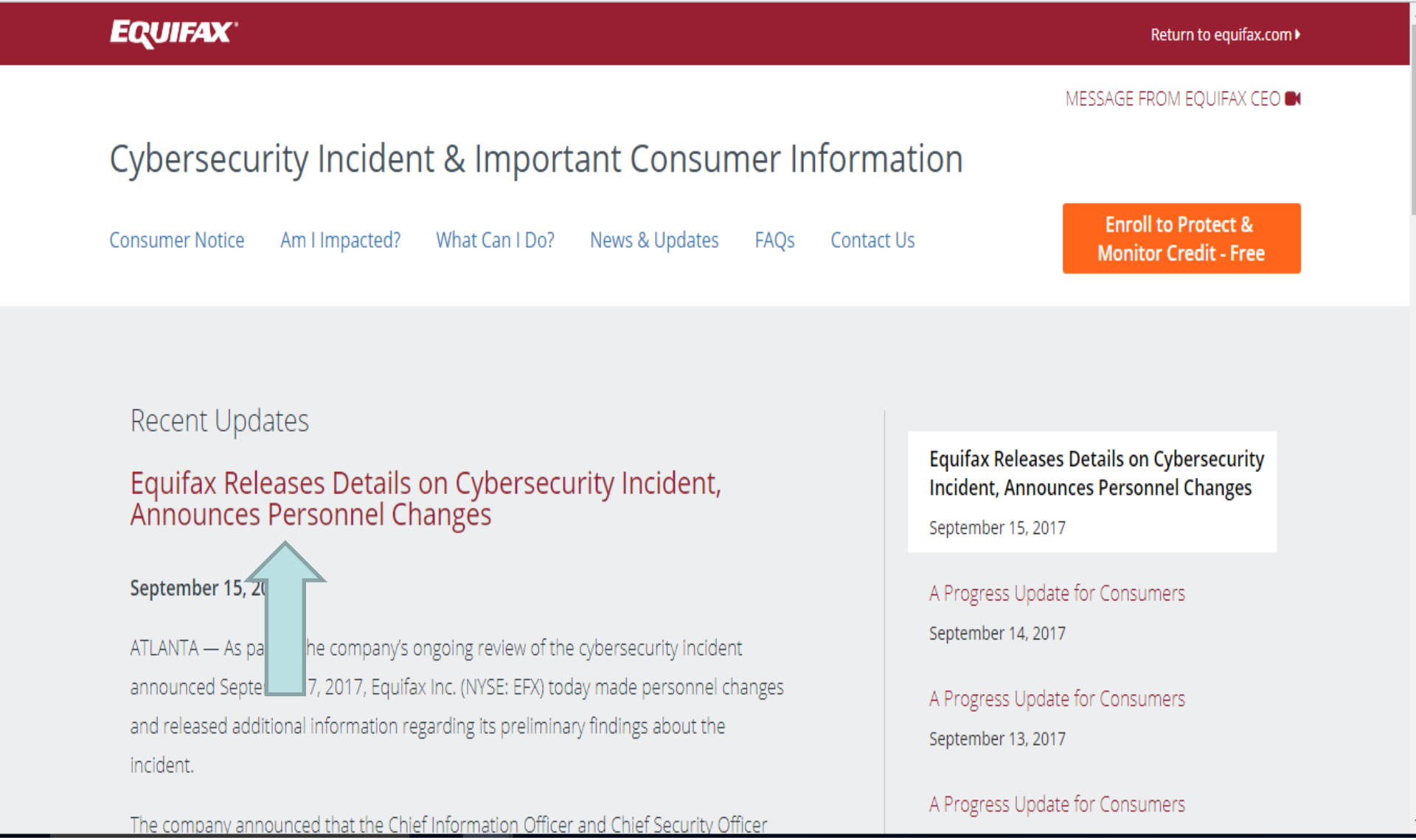
NAFCU

Reed & Jolly, PLLC



NAFCU

Reed & Jolly, PLLC



NAFCU

Reed & Jolly, PLLC

The Pace of Cyber Challenges

What we want.

What we got!

NAFCU

The Time to Prepare Is Now!

- Every time you see another financial institution in the headlines for a negative event you need to ask yourself a very simple question: How would my credit union react to that situation?

- Having a plan in place and training throughout the institution can avoid a world of problems later.

- How quickly would a negative situation in your credit union become VERY public?

Data Security Is Not New

- Graham, Leach, Bliley
- Part 748 Security Program
- Part 748.1 Filing of Reports
  - Compliance Report
  - Catastrophic Act
  - Suspicious Activity Report
- Part 748.2 BSA Compliance
  - Establish a compliance program
  - CIP
- Appendix A Safeguarding Member Information
- **Appendix B Response Program – Unauthorized Access**

Is this a CU Data Breach?

- There is no technical federal regulatory requirement for a credit union to notify its members or NCUA of a merchant data breach.
- Credit unions are only required to notify members and NCUA when there has been a *direct* data breach of the credit union's system maintained by it or its third-party service provider.
- However, member notification, in any data breach context, may help to mitigate against the risk of fraudulent or unauthorized transactions.

Poll Question 2

- When was the last time you reviewed your Red Flags policies and procedures?
  - A) This year
  - B) Within the last 12-18 months
  - C) Currently looking for them

Transaction Fraud Risks to Be Aware of!

- Internal fraud (separation of duties)
- Cash (advance) disbursement fraud
- Loan fraud
- Card fraud
  - Credit card – attacking the line of credit
  - Debit card – skimming and fallback chip fraud
- Remote Deposit capture fraud
- Wire and ACH fraud
- Authentication fraud

Bad guys will continue to find the "weakest link"!
Are you digging deep to find out how
the bad guys are breaking in?

NAFCU

Authentication is KEY!

- Don't just rely on SSNs, birth dates, home addresses or driver's license numbers for granting account access
- Require personal information AND identifying information to prevent identity fraud
- Require that members have a password or passcode to access their account
- Use multi-factor authentication:
  - *Who you are*
  - *What you have*
  - *What you know*
- Adopt advanced tools, like biometric authentication, for verifying the member’s identity

NAFCU

Proactive Member Education

- Create website with info about the breach and actions you are taking
- Post contact info to address breach-related questions and concerns
- Share educational resources and tools with members to help them prevent and manage identity fraud:
  - Tools for preventing fraud (i.e. fraud monitoring services, ID theft protection, etc.)
  - Fraud prevention strategies
  - Recommendations for monitoring accounts to catch the fraud right away
  - Warning signs to look out for
  - Steps for reporting fraud suspicions
- Ensure accounts are password or passcode protected
- Multi-factor authentication requirement on ALL accounts

NAFCU

ID Theft Red Flags

- Now you know its “special purpose”!
- Many credit unions have plugged in a standard policy and give it standard lip service

Identity Theft Prevention Program

- Implement and maintain a program designed to detect, prevent, and mitigate identity theft
- Must be appropriate to the size and complexity of the credit union
- Many similarities to your BSA monitoring program

Identity Theft Prevention Program Elements

- Identify relevant “red flags” and incorporate those “red flags” into the Program
- Detect “red flags”
- Respond appropriately to any “red flags”
- Ensure the Program is updated periodically

Defining Red Flags

- A pattern, practice, or specific activity that indicates the possible existence of identity theft.
- Regulation contains 27 examples of red flags
  - I've seen 72!
- Something that just doesn't "smell" right.
- Update as needed.

All of those remote and convenience services are now going to come back and haunt you.

Poll Question 3

- Has your Credit Union utilized the FFIEC's CAT Tool to measure your cyber security preparedness?
  - A) Yes
  - B) No
  - C) Working on it

NCUA Supervisory Priorities 2017

- LCU 17-CU-01
- Here are their top areas of supervisory focus for the year:
  - Cybersecurity Assessment
  - Bank Secrecy Act Compliance
  - Internal Controls and Fraud Protection
  - Commercial Lending
  - Consumer Compliance

Key Examination Findings

- Failure to encrypt sensitive data
- Failure to deploy data loss prevention software
- Failure to manage vendor security
- Failure to conduct periodic risk assessments or to correct vulnerabilities discovered in assessments
- Failure to change default configurations or passwords
- Absence of appropriate policies
- Insufficient employee training or awareness
- Insufficient dedicated security roles

NAFCU

NCUA Guidance

- NCUA comments on ***Cybersecurity:***
- Cybersecurity remains a key supervisory focus. NCUA will continue to carefully evaluate credit unions' cybersecurity risk management practices. We encourage credit unions to use the **Cybersecurity Assessment Tool** to bolster their security and risk management processes. This tool was issued jointly with the other member agencies of the Federal Financial Institutions Examination Council.
- NCUA plans to increase our emphasis on cybersecurity by enhancing the examination focus with a structured assessment process. We anticipate completing this process by late 2017, and will keep credit union system stakeholders informed as changes occur.

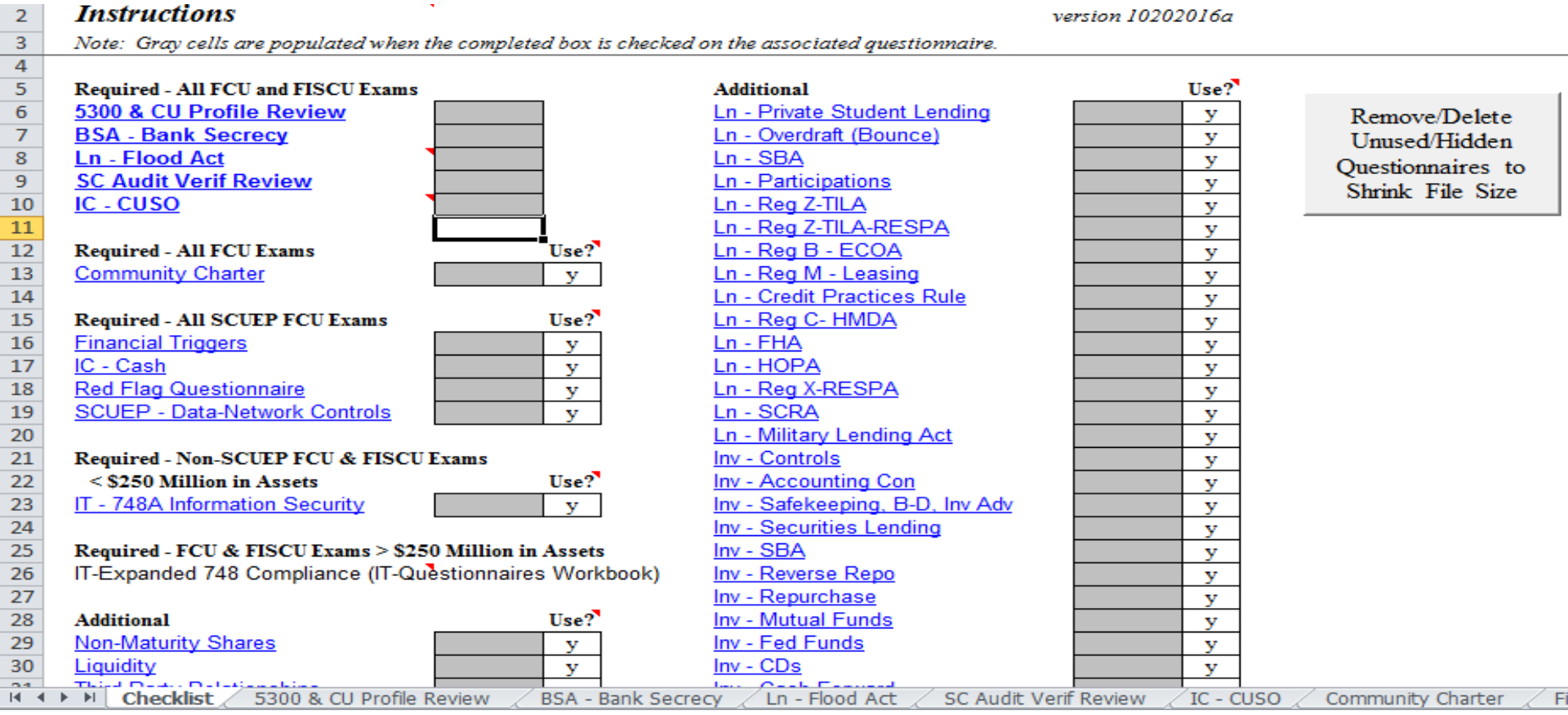
NCUA Guidance

- 2015 NCUA guidance letter identified 6 “proactive measures credit unions can take to protect their data and their members:
  - encrypting sensitive data;
  - developing a comprehensive information security policy;
  - performing due diligence over third parties that handle credit union data;
  - monitoring cybersecurity risk exposure;
  - monitoring transactions; and,
  - testing security measures.”

AIRES Questionnaires

- Automated Integrated Regulatory Examination Software
- They are the audit questions the examiner will use during the examination for each operational area
- Great resource for planning and preparation
- https://www.ncua.gov/regulation-supervision/Pages/regulatory-reporting/aires-exam.aspx

NCUA AIRES Questionnaires



Instructions *version 10202016a*

Note: Gray cells are populated when the completed box is checked on the associated questionnaire.

Required - All FCU and FISCU Exams		
5300 & CU Profile Review		
BSA - Bank Secrecy		
Ln - Flood Act		
SC Audit Verif Review		
IC - CUSO		
Required - All FCU Exams		**Use?**
Community Charter		y
Required - All SCUEP FCU Exams		**Use?**
Financial Triggers		y
IC - Cash		y
Red Flag Questionnaire		y
SCUEP - Data-Network Controls		y
Required - Non-SCUEP FCU & FISCU Exams < $250 Million in Assets		**Use?**
IT - 748A Information Security		y
Required - FCU & FISCU Exams > $250 Million in Assets		
IT-Expanded 748 Compliance (IT-Questionnaires Workbook)		
Additional		**Use?**
Non-Maturity Shares		y
Liquidity		y

Additional		**Use?**
Ln - Private Student Lending		y
Ln - Overdraft (Bounce)		y
Ln - SBA		y
Ln - Participations		y
Ln - Reg Z-TILA		y
Ln - Reg Z-TILA-RESPA		y
Ln - Reg B - ECOA		y
Ln - Reg M - Leasing		y
Ln - Credit Practices Rule		y
Ln - Reg C- HMDA		y
Ln - FHA		y
Ln - HOPA		y
Ln - Reg X-RESPA		y
Ln - SCRA		y
Ln - Military Lending Act		y
Inv - Controls		y
Inv - Accounting Con		y
Inv - Safekeeping, B-D, Inv Adv		y
Inv - Securities Lending		y
Inv - SBA		y
Inv - Reverse Repo		y
Inv - Repurchase		y
Inv - Mutual Funds		y
Inv - Fed Funds		y
Inv - CDs		y

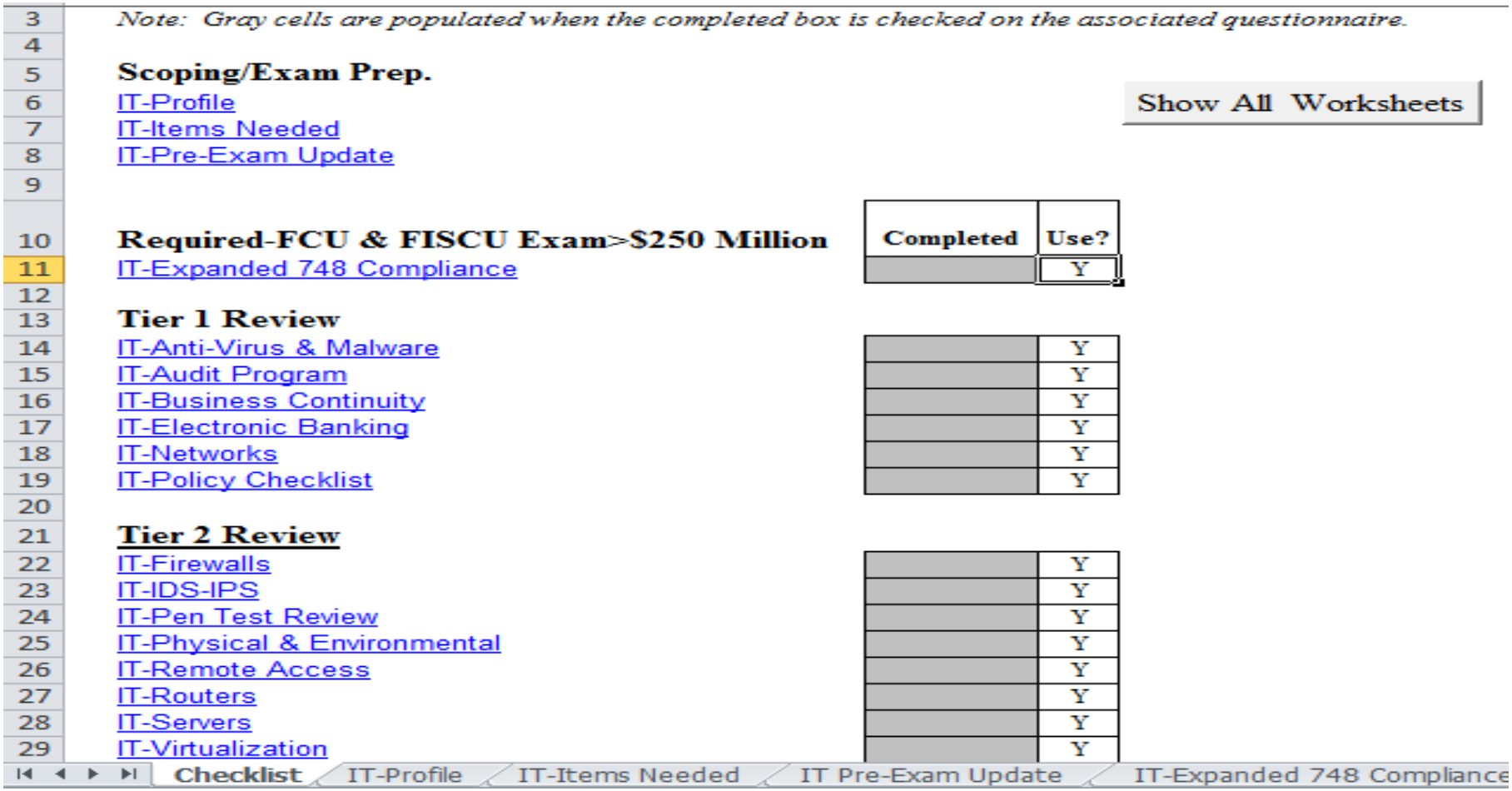
Remove/Delete Unused/Hidden Questionnaires to Shrink File Size

Checklist | 5300 & CU Profile Review | BSA - Bank Secrecy | Ln - Flood Act | SC Audit Verif Review | IC - CUSO | Community Charter

NAFCU

Reed & Jolly, PLLC

NCUA AIRES IT Questionnaires



Note: Gray cells are populated when the completed box is checked on the associated questionnaire.

Show All Worksheets

Scoping/Exam Prep.

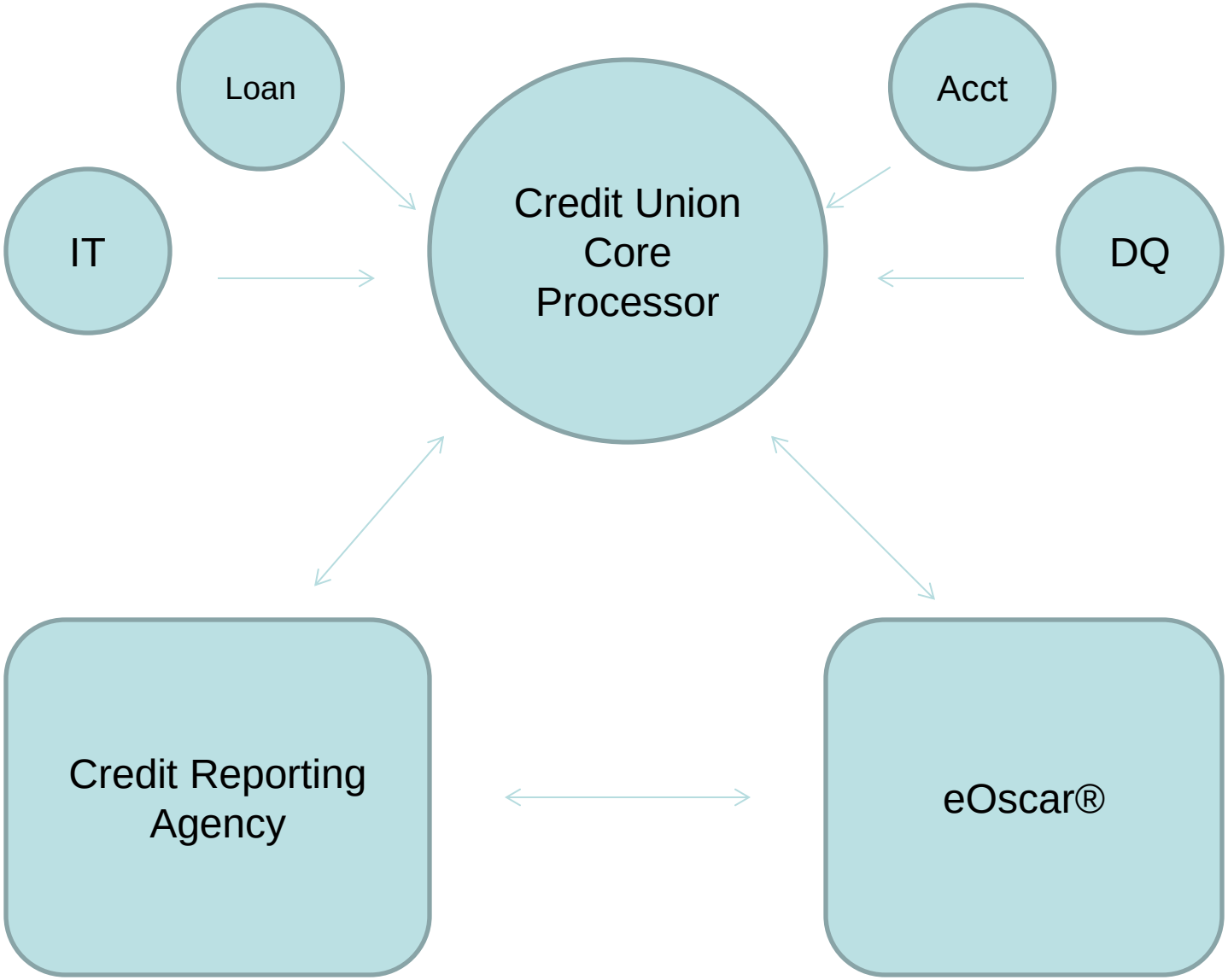
IT-Profile
IT-Items Needed
IT-Pre-Exam Update

Required-FCU & FISCU Exam>$250 Million	**Completed**	**Use?**
IT-Expanded 748 Compliance		Y
Tier 1 Review		
IT-Anti-Virus & Malware		Y
IT-Audit Program		Y
IT-Business Continuity		Y
IT-Electronic Banking		Y
IT-Networks		Y
IT-Policy Checklist		Y
Tier 2 Review		
IT-Firewalls		Y
IT-IDS-IPS		Y
IT-Pen Test Review		Y
IT-Physical & Environmental		Y
IT-Remote Access		Y
IT-Routers		Y
IT-Servers		Y
IT-Virtualization		Y

Checklist | IT-Profile | IT-Items Needed | IT Pre-Exam Update | IT-Expanded 748 Compliance

NAFCU

Reed & Jolly, PLLC


Loan
Acct
IT
Credit Union Core Processor
DQ
Credit Reporting Agency
eOscar®

Third Party Vendors

- It is always advisable to understand the benefits and risks of third party IT vendors
- Specialized due diligence and analysis
- Arms length transactions
- Reasonable paper trail
- Contract language
- Regular communication and reporting

Vendor Risk Assessment

- A proper vendor risk assessment will list all third party relationships and the exact services each provides; identify the strategic importance of each service; and determine the risk each poses to credit union operations.
- Risk assessments are a dynamic process and should be a regular component of a broader risk management strategy.
- Basically an Excel spreadsheet!

5 Questions You Need to Ask

- How do you protect our data?
  - Copies of audits or special reports
- Have you had any data security issues?
- What happens when there is a data breach?
- Who gets notified and when?
- Who pays for the damages?
  - Reputation, re-issue, ID Theft Coverage

Event Messaging

- Stay ahead of the crisis
- Do not apologize for the credit union, this is Equifax's fault!
- We are here to help our members, even if we did not cause the original issue
  - Dust off the white hat and the Mission Statement
- We have programs in place to monitor suspicious activity on the member's accounts.

What Should the Member Do?

- Offer detailed event information
  - Website, newsletter, branches and direct communications
- Link to Equifax website
- Protect themselves!
  - Transaction monitoring
  - Credit monitoring service
    - 12 months of “no strings” coverage
    - November 21, 2017 is the cutoff date
  - Fraud Warning
  - Credit Freeze
  - Fraudulent tax returns

Newton's Third Law

- For every action, there is an equal and opposite reaction.
- All of the defensive moves we recommend to the members will have a negative impact on credit union operations
- Simply put, we must increase all of our due diligence on most member transactions.
  - Understand how to react to freezes and warnings
  - Update procedures and training

What Should the CU Do?

- What happens with all that data now?
  - Existing account access
  - Creating new accounts
- Monitor automated access
- Third party technical assistance
  - SSN and IP Address confirmations
- Verification and confirmation of all remote transactions
  - Manual reviews and verifications

What Should the CU Do?

- ID Theft Red Flags
  - Address discrepancies
  - Mismatched information between CU applications and credit report
  - Fraud and Active Duty Alerts
  - Large number of recent inquiries
  - Verify information
  - Increase in remote service access, from membership to applications

Litigation and Recoveries

- Risk of losses from account fraud as well as the reissuing expenses
- Don’t sign anything……..yet
- Over 50 class action lawsuits filed…so far
  - Who are the plaintiffs (consumers or CUs)?
- Individual lawsuits are springing up in small claims courts across the country
- What is the harm caused by the breach?

The Best Defense

- Effective messaging
- Existing security programs
- Enhanced due diligence on all remote access
  - Anti robot screening
- Keep updated on all aspects of the breach
  - Trades
  - Bond
  - Outside resources

3 Ways to Prevent Fraud

NAFCU

Questions?

David A. Reed

Attorney at Law

david@reedandjolly.com

(703) 675-9578

Reed & Jolly, PLLC

Fairfax, VA

Ann D. Davidson

Vice President Risk Consulting | Bond Division

Allied Solutions, LLC

ann.davidson@alliedsolutions.net

Direct Line:608.250.9617

Please Rate This Webcast

Excellent
Good
Fair
Poor