MEMBER PRIVACY, RISK MANAGEMENT, AND DATA BREACH . . . THE CHALLENGE FOR CREDIT UNIONS

Prepared by:

Raymond J. Gustini
Nixon Peabody LLP
401 9th Street, N.W., Suite 900
Washington, D.C. 20004
(202) 585-8725
rgustini@nixonpeabody.com

Association of Credit Union Internal Auditors
23rd Annual Conference & One-Day Seminar
San Francisco, CA
June 28, 2013

PRIVACY AND SECURITY – OVERVIEW OF THE BASICS

I. THE NATURE OF PRIVACY AND SECURITY

Q: Is Cyber Security an Important Component of Overall Risk Management?

Absolutely. It may, in fact, be among the most important future element of the financial and reputational risk of credit unions.

What the NCUA says – "The increasing frequency of cyber-terror attacks on depository institutions heightens the need for credit unions to maintain strong information security protocols." NCUA Alert No. 13 – Risk-01.

What the OCC says – In its semiannual Risk Perspective released in Spring 2013, the OCC said, "Increasingly sophisticated cyber threats, expanding reliance on technology and changing regulatory requirements are heightening operational risk."

Clearly cyber security is not just an IT issue, but a crucial business imperative for board and management of credit unions and requires an understanding of (i) privacy, (ii) cyber security best practices, and in the event of a breach (iii) effective responses.

Q: What Do We Mean by Privacy?

In general terms, it's "*The ability of individuals to control the terms under which their personal information is acquired and used by others.*" According to NCUA, privacy rules "limit the disclosure" of non-public personal information to unaffiliated third parties. Security or safeguarding addresses the security and confidentiality of information and ensures its proper disposal. Security concerns are in the forefront now.

Privacy in the United States is not an absolute right under federal law or the U.S. Constitution. Individuals' privacy interests are balanced with those of society at large. For U.S. businesses, privacy restrictions arise in relation to the nature of their activities, not the general rights of their customers. Privacy in the financial services sector is the ability to conduct activities anonymously and without misuse of a consumer's non-public personal information. Safeguarding is how a credit union protects the sensitive, non-public information of a consumer.

Q: Why Should Credit Unions Care About Privacy?

Three Reasons:

First - Customer Trust - Any business, but particularly businesses with significant customer contact count customer trust as an important, critical asset. Thus, at worst entities like credit unions will be impacted if members believe that there is incompetence or indifference to maintaining member information security. Protection of privacy is something consumers will shop for. The public is increasingly sensitive to and

increasingly vocal on privacy issues and in particular on the safety and security of member/customer data.

Second - Legal and Fiduciary Obligations - NCUA Rules, Guidelines and Policies mandate both privacy protection and safeguarding of members and others.

Third - Cost – The average per customer cost to business after a data breach is approximately $194 per compromised record, according to Chubb Insurance and Ponemon Institute.

Q: What is the Privacy Calculus of Members?

- It is Relatively Simple - People willingly disclose information to credit unions, banks, hospitals, websites and cable companies to gain the benefits that this limited, protected disclosure of personal information brings. Good privacy protection helps to foster confidence that disclosing personal information is intended to be a low risk exercise.

- Secondary Use of Information Voluntarily Provided - Customers do not object to providing information for matters like credit applications or health insurance. The secondary use or illegal taking of such information raises privacy concerns.

Q: Are Members Privacy Knowledgeable?

For sure. In their personal and financial activities, your members have become sophisticated with respect to privacy. They know about identity theft, pretext calling, cookies, screen scraping, and phishing. Many have been victims of identity theft. Still, they happily take the risk of supplying personal information to gain the benefits of online banking or shopping. Privacy concerns touch a central nerve as more experience personally the abuses which interconnectivity and cheap electronic storage of detailed electronic information can produce.

- The FTC historically reviews over 200,000 identity theft complaints a year.
- In 2012, there were 12.6 million identify theft incidents, costing over $21 billion.
- Consumers now "shop" for privacy
  - How many breaches can your credit union "afford"?
  - How much reputational risk can you afford?

Q: How Do We Regulate Privacy in the U.S.?

The internet is not the perfect vehicle to support confidential communication of personal data. But it is what we have and this information is protected differently in the U.S. than in many countries.

The U.S. Historically Has Had a Self-Regulatory Approach to Privacy - The United States, at the federal and state levels, protects privacy on a patchwork basis through a combination of self-regulation and through regulation of certain activities or economic sectors. In this sectorial approach we are very different than many other countries. There are no overarching federal laws guaranteeing a right to privacy as there are in Europe.

The FTC, the CFPB (for large ($10 billion or more) banks and credit unions) and (in the case of financial privacy) NCUA and bank regulatory agencies are the federal privacy agencies. CFPB still a work in progress but FTC brought a number of privacy and security actions in the past ten years involving express or implicit promises for privacy and security that were not honored.

Laws Governing Privacy:

General - Privacy is capturing legislative attention at every level of government.

- California's constitution recognizes a "fundamental human right to privacy."
- States have adopted data breach notification laws, laws on driver license disclosure, Social Security number use, etc.
- Even local governments are passing privacy laws. San Mateo and San Francisco, California have enacted privacy law applying to financial institutions doing business there.
- Privacy, as it relates to customers of financial institutions, is heavily regulated and the systems architecture of electronic services of entities like credit unions and banks.

Q: Why Has Technology Accelerated Concerns Over Privacy?

- Internet – a miracle, but not designed to do what it now does.
- Digital world has produced efficiencies, but also materially increased risks for consumers and businesses holding their data.
- Mobility Risks – Explosion of mobile, handheld devices containing sensitive data have increased efficiency but greatly increased risks to networks and exposure of sensitive data.

- Devices are now essential but far less secure from both a physical and systems standpoint
- Risks of Wi-Fi use at the local coffee house
- Risk of lost or stolen mobile devices
- Security measures such as passwords can be bypassed or may not exist
- Does your credit union have a policy on how handheld mobile devices may be used?
  - More risks of malware
  - Guidelines should also apply to contractors

The upshot is, because the benefits are great and the world is permanently digital there is no retreat.

Q: What is the Scope and Nature of Data Breaches Since Data Breach Laws Were Enacted?

In 2003, California's law was the first state requiring disclosure of a data breach was enacted. A total of 46 states have enacted data breach laws.* Since 2003, this information is now being regularly reported and the public is informed. The breaches that have been described range from sophisticated hacking (TJX), impersonation (ChoicePoint), to lost or stolen laptops on mobile devices (the Veterans Administration).

- Federal law also requires notice under the Fair Credit Reporting Act and notices are also required of credit unions by NCUA under Part 748, Appendix B when there is "unauthorized access to or use of member information" and the risk of "substantial harm or inconvenience to a member."
- When a data breach occurs, as a credit union you will be notifying affected members in the affected states and NCUA.

State Data Breach Laws—There Are 46 and They Are Not Identical

- Structure – All such laws require a notice to customers/members under the law of the state where they reside when there is unauthorized access to customer information
- State laws are similar but unfortunately they are not identical and differ on whether coverage includes:

* Only Alabama, Kentucky, New Mexico and North Dakota have no data break notification rules.

- Whether "computerized" and/or both computerized and physical documents are covered
- Whether notice is required with a specific timeframe
- Whether notice must be in writing, by telephone or e-mail or any of the above
- Whether the attorney general or a state consumer protection agency must be notified
- What type of data is protected, *i.e.* name in combination with one or more of: account numbers, social security numbers, driver's license, mother's maiden name
- Penalties for non-compliance
- Whether a data breach creates a private right of action for a consumer – Approximately 17 states and territories do
- Whether mandated destruction of data is required as part of data breach law
  - Sixteen states require safe disposal of personally identifiable customer data

II. THE REAL WORLD IMPACT INCLUDING CREDIT UNIONS

Q: How Big is the Data Breach Problem?

It has replaced theft as the number one U.S. fraud. The most concentrated fraud occurs in the financial services area and last year (2012) 37% of data breaches, attacks, etc., occurred in financial services according to the Verizon Data Breach Investigations Report.

- There can be an enormous financial and reputational impact.
  - Michael's Stores – In 2011, a data breach affected consumers in 20 states using fraudulent PIN Pads at the checkout. Class action lawsuits followed.
- Sony PlayStation – In 2011 Sony announced that data on 70 million subscribers obtained by hackers. Remediation cost to Sony was $171 million and significant litigation occurred.
- TJX, the parent of T.J.Maxx stores, had an epic data breach several years ago involving over 45 million credit cards, multiple lawsuits and costs estimated in excess of $1 billion.
- Credit unions are not immune:

- Bethpage Federal Credit Union – In 2012, 86,000 debit card account numbers were inadvertently exposed on the internet. Data also included checking and savings account numbers.
- Pentagon Federal Credit Union – Infected laptop in 2011 may have impacted numerous credit and debit card holders.
- Vermont State Employees Credit Union – Lost unencrypted data tapes on 80,000 customers

Q: What Are the Components of Cost After a Breach?

First parties:

- Privacy Notification
- Crisis Management
- Attorneys
- P.R.
- Systems Investigation, Remediation and Possible Costs
  - Cost of credit monitoring
  - Cost of credit freeze
  - Free credit reports
  - Identify theft insurance
- Business Interruptions
- Reputational Losses/Trust
- Litigation Expense
  - State Attorneys General
  - Class Actions – Big component of TJX data breach
  - Costs
    - Cost to reissue a card: $5.60 (source – NAFCU)
    - Characteristics of Data Breaches in 2012:

- 37% of data breaches targeted at financial institutions
- 92% were outsiders
- 14% were insiders
- 52% were from some form of hacking
- 76% network intrusions
- 40% malware
- 78% were rated low difficulty
- 69% discovered by external parties
- 66% took months or longer to resolve

- Average cost per credit union of clean-up - $86,000

Source: Verizon Data Breach Investigations Report

- Red Flags Rule – Credit unions required by NCUA rules (Part 717, Subpart J) to identify, detect and respond to activities that could signify identity theft by creating a written identity theft prevention program.

NCUA Policy at Part 748 Requires Regulatory Notice to NCUA:

- Notice to appropriate NCUA Regional Director
- Assessing scope of incident
- Notify law enforcement and file SARs, where warranted
- Take remedial steps to control incident. For example, monitoring, freezing or closing affected accounts
- Notify members (when warranted)
- Special requirements when a credit union service provider experiences the breach
- HIPAA and many state laws require notice when healthcare information breached

III. CONGRESS AND NCUA HAVE, THROUGH LAWS AND REGULATION, CREATED PRIVACY AND SECURITY DUTIES FOR CREDIT UNIONS

The Gramm-Leach-Bliley Act is the Foundation of these Duties

Gramm-Leach-Bliley Act ("GLBA") – Title V of GLBA, relating to financial privacy, was controversial when enacted. Under Title V a bank, credit union or other "financial institution" providing "financial products or services to consumers" were required to provide privacy notices to customers and clients and limit third party sharing. The safeguarding guidelines followed the July 1, 2001 financial privacy rules.

Q: What Are the Safeguarding of Consumer Information Rules For Credit Unions?

Security and protection of customer information is the second part of the GLBA entities' privacy rules.

- Published interagency guidelines for financial institutions and credit unions require:
  - Risk assessment approved by the Board of Directors on identifying and assessing risks of security, confidentiality or integrity of customer information;
  - Adequacy of information security systems
  - Service Providers – Vendors such as marketing firms, mailing houses, accountants, etc. must agree with the credit unions they service to meet "objectives" of security guidelines.

CFPB, Privacy and NCUA Guidelines

- CFPB has enforcement authority under privacy rules for credit unions over $10 billion in assets. NCUA has enforcement authority for credit unions under $10 billion in assets.
  - New Interim Final Privacy Rules became effective on December 30, 2011 at 12 C.F.R. Part 1016, Section 1016.1
  - Model Statement – Interim final rules continue model privacy form and permit it in its purest form as a safe harbor to comply with notice content requirements of 12 C.F.R. 1016.6 and 1016.7.
- NCUA Guidelines – See Part 748, Appendix A, Guidelines for Safeguarding Member Information"
  - Objectives – A credit union's information security program should be designed to ensure the security and confidentiality of member information

- Appendix B to Part 748 – Guidance on Response Programs for Unauthorized Access to Member Information. Appendix B provides a set of best practices for safeguarding.
    - Credit unions have an "affirmative duty to protect their members' information against unauthorized access or use."
- Credit unions required to notify members where credit union determines there has been misuse of member information by unauthorized persons or entities
- This, of course, is in addition to state laws requiring notice unless a state, Hawaii for example, allows federal requirements to supersede those of the state.

IV. WHAT DATA SAVVY CREDIT UNIONS ARE DOING BOTH BEFORE AND AFTER A BREACH

Q: What Should the Response Be When There Is a Security Breach of Your Web Site?

Data breaches come in many forms from disabling an entire network to pilfering of selected data or files and from internal or external sources. You should plan ahead:

- Have a written response plan prepared before a breach occurs
- Have a template for a data breach notification letter available reflecting applicable state and federal law
- A privacy officer/risk officer with responsibility in this area
- Create roster of team members with after-hours contact information
    - Critical departments or business units
        - Risk management
    - Internal audit
    - Public relations/communications
    - Counsel
- Determine if the incident requires reporting? Not all incidents do under state law, and response plans should describe those that do require reporting to state and federal officials.
    - Encrypted information generally does not require notice or reporting
- Is the credit union required to file an SAR?

- In many cases it will be

- Reporting under state law generally required if:
  - The data is unencrypted
  - Contains first and last name of a consumer and in combination with one or more of:
    - Social Security Numbers
    - Driver's license number
    - Bank account number; or
    - Credit card number
    - Mother's maiden name
    - Passport number
    - Biometric data
    - Protected healthcare information
- Law enforcement notice – Need to examine state laws to determine if notice to Attorney General or other agencies is required
- Private Causes Action – A number of states (California, for example) permit private causes of action

Q: What Are the First Things We Should Do If We Learn of a Data Breach?

Initially you should:

- Contain the data breach
  - Prompt investigation
  - If on credit union premises:
    - Secure physical site
    - Isolate affected systems
- Convene a response team

- Collect information on nature and specifics of breach, including causes and whether of systems are under threat

- Analyze legal and contractual implications, including litigation risk, breach notification requirements, insurance coverage, law enforcement notice and employee liability

- Contacts with law enforcement

    - Consult with legal advisers before doing so. Law enforcement may require a delay before notifying affected persons

Q: What Do We Do After the Initial Data Breach Notice Has Been Provided?

Recognize that it's not over. You may need to strengthen your defenses and responses. Also:

- Prepare for the possibility of litigation

    - Are you in a private right of action state?

        - California and Massachusetts, for example

- Notify insurance carriers

- Follow-up reviews on integrity of technological and physical security

- Assess and evaluate operational controls

The All Important Data Breach Notification Letter ("DBL") to Members

Data breaches for credit unions and banks are governed by both state and federal (NCUA in the case of credit unions) laws:

- Elements of Notice Letter:

    - Plain English

    - Date of breach (if known)

    - Entity's name

    - Categories of information that may be at risk

        - Note the Massachusetts limits on this disclosure

- Whether notice to members was delayed because of law enforcement investigation
- Advice that affected members should take
- Notice to federal regulator such as NCUA may, in some instances, serve as fulfillment under state law (West Virginia, for example)
- Contact information for credit reporting bureaus

- Elements of Pre-Planning:
  - Mandatory review of letter by counsel, CEO or staff leader
  - Who will be the spokesperson, corporate communications
  - Whether and when substitute notice is permitted
  - Whether state law enforcement (in addition to NCUA) need to be notified

- Practical Considerations:
  - Tone is important
    - Trust must be reestablished and letter is first communication
  - Data breaches often result in litigation so counsel should review
  - Piling on – Fraudsters sometimes use data breach notice letter to commit additional fraud
  - Some states require that letters describe what remediation actions will be taken
  - Others (Massachusetts, for example) prohibit a description of the breach to deter fraudsters
  - Typical perks for victims of data breach:
    - Some or all of:
      - Free credit monitoring for affected customers
      - Coupons or credit on bills for affected customers
      - Credit freeze services for affected customers
      - Free credit reports

- Call center for Q&A with fully informed personnel to answer questions
  - Note that in some jurisdictions, state laws mandate what you are required to do in this area

- Understand how the breach should be explained to customers and what it will take to rebuild trust

Q: How Are Boards Involved?

- Board should be and are increasingly involved as oversight of the risk management function
- Tone at the top
- Board or Board committee kept informed if breach occurs
- Involvement of CEO and Board, not just Chief Technology Officer

Q: Should You Purchase Insurance for Data Breach & Cyber Attacks?

Policies can cover:

- Security Breach Liability
- Programming
- Public Relations
- Security Breach Exposure
- Cost Factors

Q: What Are Companies Doing to Increase Security Awareness?

Security Practices:

- CEO and Board Involvement
  - Chief Privacy and Chief Technology Officers provide more Board access and same reporting lines as internal audit

- Regular Board and Risk Management Reviews
- Board of Directors Education Committee Reports\
- Should approve a written, information security policy
- Oversee development, implementation and maintenance of the credit union's security program

- Credit unions:
  - Regularly test
  - Oversee service providers
  - Report to Board of Directors annually
- Cultural changes at management and workplace level

Q: What Else is Being Done?

- Background checks on employees
- Employee training and education on cyber risks
- Better authentication practices
- Policies on need and efficiency of working remotely from handheld or portable devices
- Passwords – Best practices
  - 8 characters or more
  - Know and prohibit use of 25 most common passwords
    - "12345678"
    - "password"
  - Strengthen passwords
  - Location of sensitive data
  - Periodic security or vulnerability audits by independent third parties
    - White Hat hackers

    - Ongoing Board of Directors or committee of directors involvement and education
    - Identification of risk assets – Particular security risks for specific businesses such as newspapers or cable companies
- Do not overlook physical security
    - Laptops with recovery features (LoJack, for example)
    - Clean desk rule for employees
    - Lock ports on laptops
    - Public areas – monitor screen configuration
- Work from home programs – Adds vulnerability
    - VA data breach, misplaced laptop
    - Mobile device risks
- Employee termination
    - Exit procedures relating to data access
- Trash disposal
- Electronic equipment disposal – wipe clean policies