Combating Online Fraud

Prevention, Detection and Response

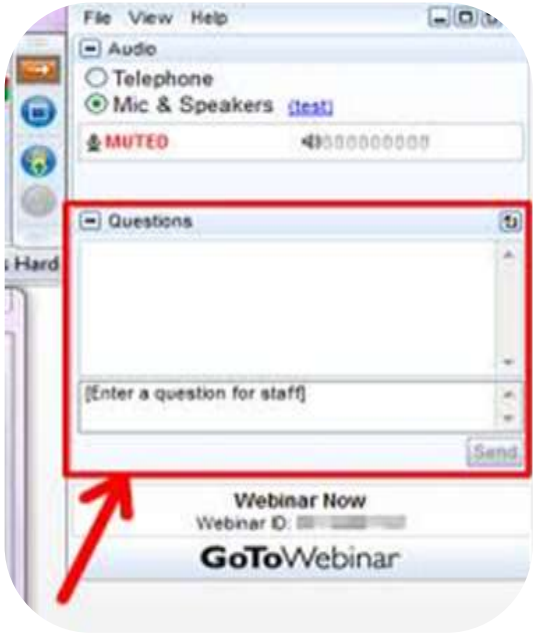
September 26, 2012

Michael Barrack | Director – IT Security and Compliance
Compushare, Inc.

Mary Thorson | Vice President
Chartwell Compliance

Housekeeping Items

All Lines are Muted



Technical Difficulty? Questions?

Special offer announcement


QUIET PLEASE!
Recording in Progress

AGENDA

Introductions

ICBA Compliance and Risk Management

Chartwell Compliance and Compushare

Online Fraud - Prevention, Detection and Response

Discussion

Michael Barrack

Director – IT Security and Compliance | Compushare

- Provides IT security and risk and compliance consulting services for community banks nationwide
- More than 20 years of serving community banks
- Understands how banks apply technology to support the business, and what the regulators expect
- Has been the accountable executive in IT regulatory examinations as both a banker and service provider
- Compushare has incorporated this insight in its offerings

Mary Thorson

Vice President | Chartwell Compliance

- Financial services examiner, consultant, and compliance officer
- Over 28 years of experience
  - regulatory compliance
  - technical risk management
  - Training
  - program implementation, reviews & exams
- Risk Management expertise
  - consumer protection
  - Third-party management

ICBA Compliance and Risk Management Division

Chartwell Compliance

ICBA Compliance and Risk Management Provider

- Credentials of big 4 consultants

Risk Management & Compliance Leaders

Bank Secrecy Act Solutions

Anti-Money Laundering Solutions

Consumer Risk & Compliance Solutions

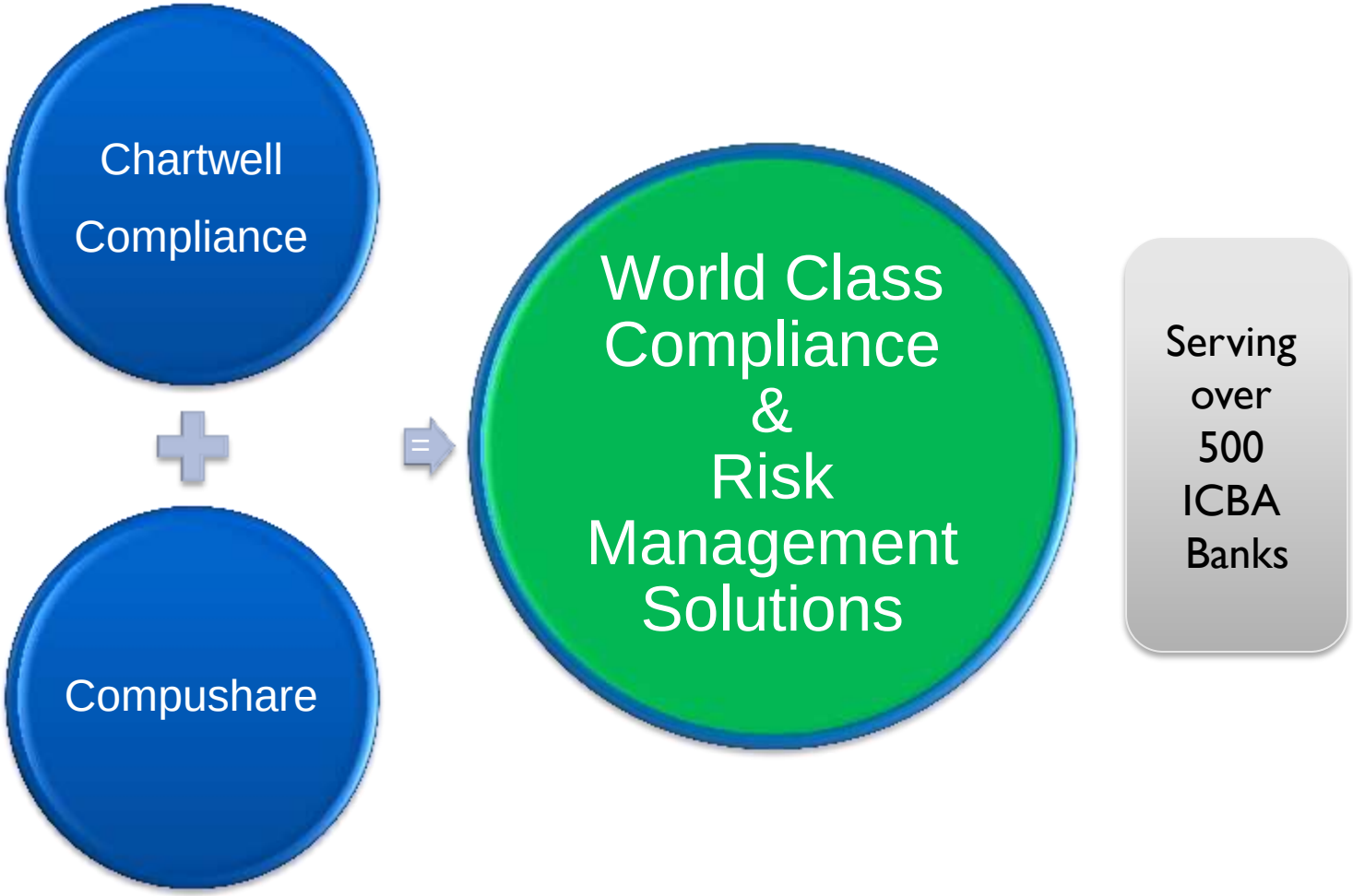
ICBA Compliance and Risk Management Division

Compushare

ICBA Preferred Service Provider

- ✓ The leader in financial technology management solutions
- ✓ IT risk and compliance experts

ICBA Compliance and Risk Management Division



ICBA Compliance Powered by Chartwell

COMPLIANCE & RISK MANAGEMENT

Chartwell Compliance Experience

Subject matter focus	Benefits	Experience	Services
✓ Regulatory compliance	✓ Well-rounded expertise	✓ 30 years of experience	✓ Compliance audits
✓ Anti-money laundering	✓ "all-in-one solution"	✓ Compliance	✓ Outsourced compliance admin
✓ Fraud, safety and soundness	✓ reasonable price	✓ Risk Management	✓ All-purpose advisor
✓ Risk management	✓ small firm	✓ AML	✓ Risk assessments
	✓ customer focus	✓ Safety & Soundness	✓ Policies & procedures
		✓ Leadership Roles	✓ Training
		✓ Regulatory Agencies	✓ Remedial work
		✓ Financial Institutions	✓ Regulatory relationships
		✓ Consulting	✓ Loan review

CHARTWELL

ICBA Compliance & Risk Management™

COMPUSHARE

Chartwell Compliance Experience

Value Proposition for Financial Institutions

- Provide technical expertise
- Independent views
- Industry perspective
- Translate ‘regulator speak’ to ‘nuts and bolts’
- Become the team SME that the institution may not be able to justify on a full-time basis

Vulnerability & Inherent Risk

"YOU'LL ALWAYS MISS 100% OF THE SHOTS YOU DON'T TAKE."

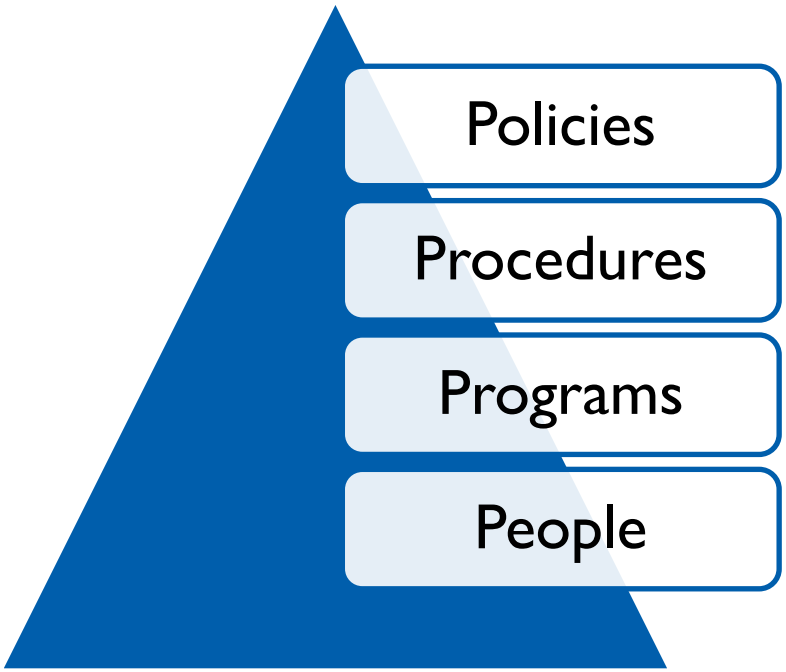
Wayne Gretzky

ALL financial institutions are vulnerable

- Rapid expansion of e-money products and services
  - Convenience vs. Risk
  - Balance of bank compliance and operational costs
  - Rapid expansion
  - Highly available
  - Easily accessible

Vulnerability & Inherent Risk

Preventing Financial Crimes



Implement controls to

- Prevent Risk
- Mitigate Risk

- The back office and supporting systems have evolved into the front line in the fight against fraud, money laundering, and terrorist financing
- Transactional volumes and types of vehicles have necessitated systemic support

Cybercriminals attempted to steal at least US$75 million from high-balance business and consumer bank accounts by using sophisticated fraud automation techniques that can bypass two-factor authentication, according to a report released in June 2012 by antivirus firm McAfee.

Preventing Financial Crimes

Fraud typically targets businesses and high net worth individuals

Risk Management – Prevention

Policies and Programs

- Risk Management
- Compliance
- Loss Prevention
- Financial Intelligence
- Fraud Prevention

Procedures

- Monitoring transactional evidence
- Internal audit for periodic testing
- External resources to inject independence and expertise

People

- Training technical skills & Awareness
- Interactions across the organization to expand the view

Detection

Key to Risk Management >>>Evaluating Available Data

- Where is the trail?
- Who is watching and evaluating the movement of funds?
- Importance of "unusual" activity as a "pointer"

Risk Inhibitors >>> Who is watching & monitoring?

- Systems
- Firewalls
- Authentication Procedures
- Controls

Detection – Know How Systems are Exploited

Fraudsters and money launderers

- Identify and exploit systemic control weaknesses
- Funds deposited into financial institutions
- Implement control mechanisms to exploit the opportunities
- Cash couriers and bulk cash shipment
- New electronic payment methods
  - Account information that directs user "footprints"
    - Addresses
    - Telephone numbers
    - Personal information

Money Laundering and Fraud – Responding Effectively

Investigative method – "Share Everything"

- Compliance, IT, Security, Marketing, Who Else?
- Suspicious activity reporting (SAR) process – It's not just for money laundering

"Know Everyone" and "Know Everything"

- Knox your customer
- Know your business partner
- Know your employee
- Know your systems

Challenges in Response

Facilitation tools and Challenges…

Incomplete picture of transactional data across the enterprise

The system would interface and it has the capacity, but, it's not set up to effectively deliver meaningful information

Capacity is not there to handle the demand (the tail that wags the dog)

Gaps caused my legacy system "add-ons"

How Chartwell Compliance Assists Financial Institutions

- Independent assistance to support robust risk management
- Industry experts to assist in – testing, consulting, & training
- Risk Assessment(s) and/or critical review of Risk Assessment(s)
- Enterprise-wide reviews of risk management functions
- Identify gaps and recommend corrective actions & enhancements
- Advise on regulatory risk management issues

Compushare – A Preferred Service Provider of the ICBA

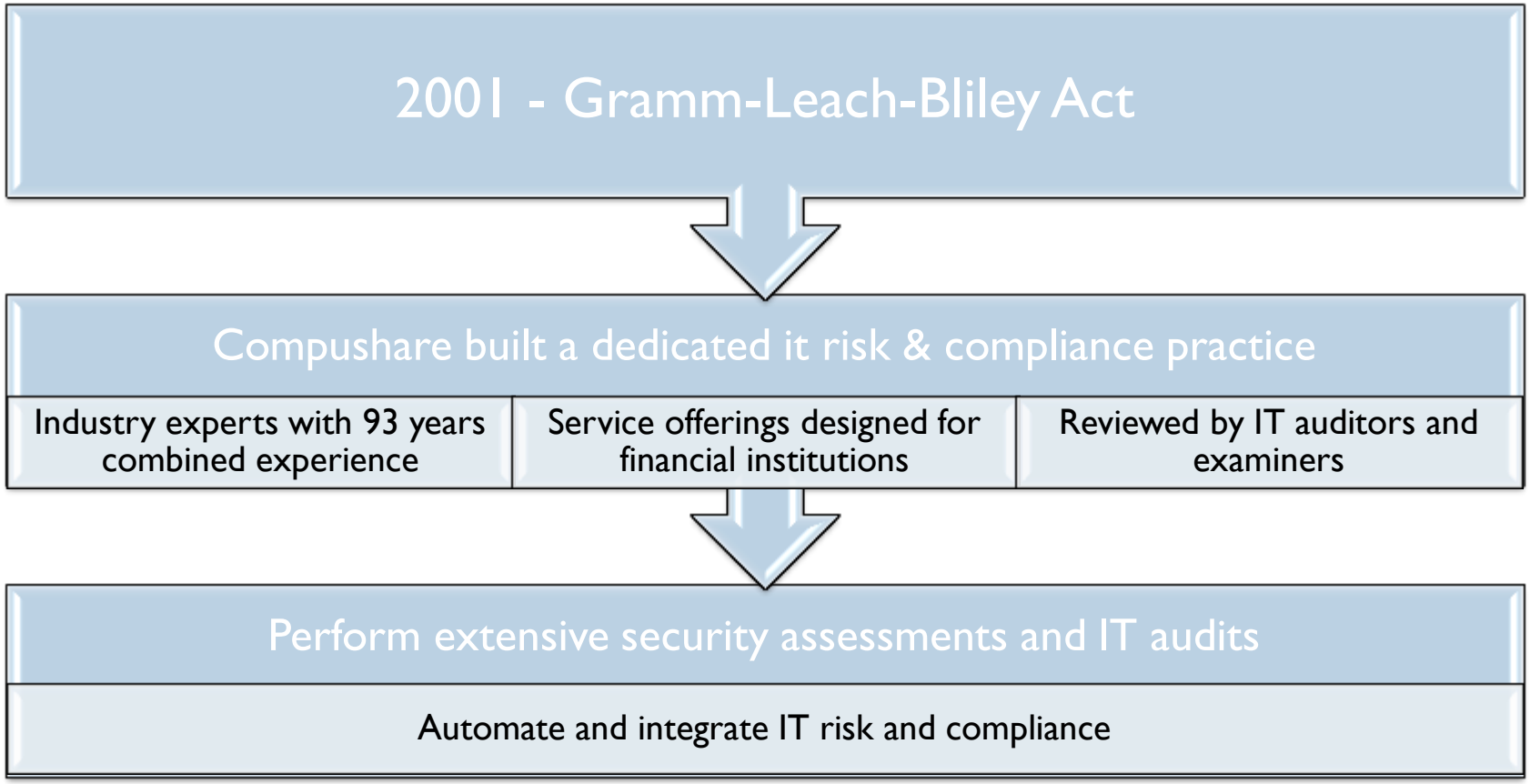
IT RISK & COMPLIANCE

Compushare Relevant Experience

Dedicated experienced IT risk and compliance practice

- Replace failing IT infrastructure
- Turnaround poorly performing IT organizations
- Address critical findings in IT audits/regulatory exams
- Perform IT security investigations and forensics in incidents

Risk and Compliance Practice



A Daily Example

WELLS FARGO

wellsfargo.com

Bill Pay payment was sent

We have sent the following Bill Pay payment(s):

Payee Name (Nickname)	Amount Sent	Date Sent	Delivery Date
SANYO Electric Co., Ltd.	$1,632.53	09/10/2012	09/11/2012

Please note: We have debited your Bill Pay payment account(s) for the above payment amount(s). It may take up to three business days for payments sent electronically to be posted to your payee account. It may take up to five business days for payments sent by check to be delivered to your payee.

If you have questions, we are available 24 hours a day, 7 days a week. Call Wells Fargo Online Customer Service at 1-800-956-4442 or sign on to send a secure email.

To unsubscribe from this notification:

Currents in Web Fraud - Recent Examples

CASE STUDY

SOUTHWEST CLIENT

ABC Bank

$XXX million in assets

Based in Southern California

Facing regulatory pressure for increased capital, and improved control structure to name a few

CASE STUDY

PROBLEM

Bank's insurance company client had 2 fraudulent ACH transactions initiated through the Bank's system using their credentials. They totaled $90K.

Bank needed to find a way to protect itself without losing this long-standing client .

SOLUTION

Bank engaged Compushare to perform forensics to determine:

- What caused the compromise?
- The strength of the client's IT controls
- What the client could do to prevent a recurrence.

RESULTS

Compushare found the client's controls on its desktop computers and its perimeter were lacking substantially, and that this weakness in controls were exploited by an unauthorized individual.

The Bank avoided any liability of the $90K in fraudulent transactions, while preserving the client relationship with a report that indicated how the client could protect itself for the future.

Compushare secured other technology management services and became this Bank's trusted service provider partner, winning its confidence and substantial additional business.

CASE STUDY

MOUNTAIN CLIENT

XYZ Bank

$XX million assets

Based in the Mountain region

CASE STUDY

PROBLEM

Like the first institution, some fraudulent transaction(s) were initiated from a client's PC, and the Bank needed to determine how to respond.

While Bank has an active IT department, they lacked forensic expertise.

SOLUTION

Compushare provided a fully trained, experienced forensic analyst to study the equipment that was used to determine source and help Bank limit its liability.

RESULTS

Compushare found the client's controls on its desktop computers lacking substantially, and that this weakness in controls were exploited by an unauthorized individual.

Specifically, several pieces of malware were identified which enabled the unauthorized user to uncover the credentials of the Bank's clients, and exploit these credentials for unauthorized use.

Compushare provided a report that protected the institution and was rendered in such a way as to be admissible in a court of law.

CASE STUDY

MIDWEST CLIENT

Midwest Banking Company

$XXX million assets

Based in the Chicagoland Region

CASE STUDY

PROBLEM

The bank identified that a security breach had occurred.

After several weeks of trying to determine the issue's source, the client brought in Compushare.

SOLUTION

Compushare performed a forensic analysis against the desktop computer(s) that were involved.

Too much time had passed and chain of custody was not performed on the equipment.

A report was generated on controls that could be implemented in the future.

RESULTS

Because the client failed to engage a forensic specialist quickly enough, the results of the analysis were inconclusive and the source of the issue was not definitively identified.

This leaves open the question on whether malware was the source, whether it could have been a non technical "inside job" and whether the situation could recur. No financial losses were sustained.

CASE STUDY

Any Community Bank

$XX million assets

Based in Southern Maine

CASE STUDY

PROBLEM

The Bank had one of its business clients suffer fraud initiated against it totaling $589K.

The client sought recourse through the court system and accused the Bank of negligence in its handling of money transfers.

SOLUTION

Federal Appeals court in July of this year allowed a lawsuit against the Bank to proceed, although it suggested the two parties settle out of court.

It reversed a lower district court that found the Bank was not responsible for losses tied to fraud attack.

CASE STUDY

RESULTS

The key here was that it appears the Bank's technology was sound and in line with federal security guidelines.

The court established a precedent that put financial institutions on notice that necessary technical controls may not be sufficient to protect the Bank from liability in the event of web fraud against its business client(s). The institution must also follow up on its process and policies:

http://www.americanbanker.com//issues/177_131/appeals-court-allows-business-fraud-suit-1050715-1.html?zkPrintable=1&nopagination=1

Key Takeaways

What Do These Cases Have in Common?

- The Banks in question had no technical IT forensic capability
- Malware on the desktop appears to have played a role in the incident
- Each of the Banks were unaware of their legal liability and those who escaped it did so with luck and not by design
- The institutions were lacking in preventative controls
- The incident response programs were academic and not tested

EACH BANK HAD A VERY **BIG** WAKE UP CALL!

Compushare Observations

- Community Banks operate under the faulty notion that:

"it won't happen to our bank"

What Banks Can Do?

Prevention

1. Update the bank's IT risk assessment

- ACH
- Wire transactions
- Remote deposit capture
  http://www.Ffiec.Gov/pdf/pr011409_rdc_guidance.Pdf
- Internet banking/bill payment

2. Identify controls that are missing

- Preventive and detective controls
- Administrative, physical and technical controls

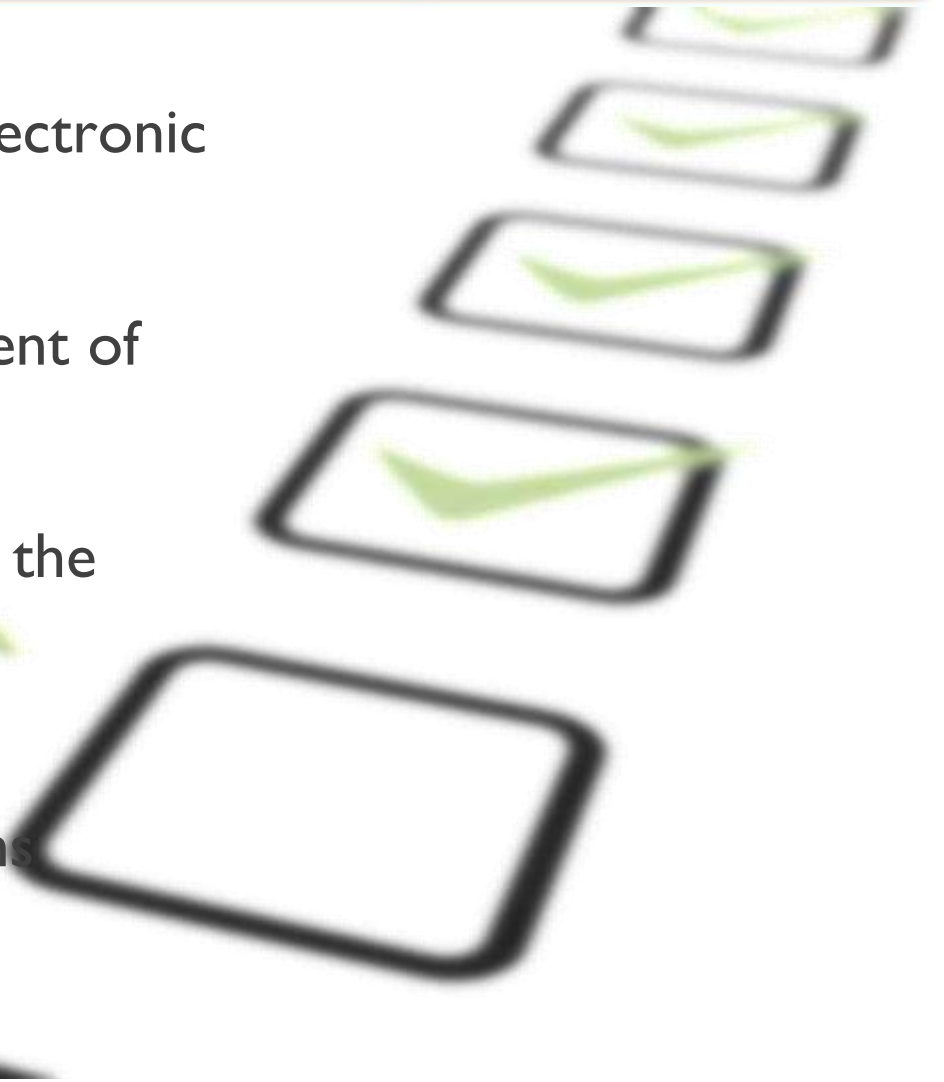
3. Research additional controls - internet banking and/or ACH

Prevention

- Perform Information Security Training with your staff
- Perform an overall regulatory preparedness review against IT-related control programs
- Evaluate the contractual language of your ACH contracts with clients
- Research the new threats emerging in the market
- Ensure that the antivirus and patch management solution the bank is using is effective
- Know the controls your key corporate customers are using

Detection

- ✓ Review the frequency of Electronic Banking Audit program
- ✓ Obtain an outside assessment of control strength
- ✓ Stay current with trends in the market
- ✓ Simplify with automation & integrated control programs



Response

Perform a test of the Bank's Incident Response Program	• tabletop exercise using the scenario of a fraudulent web-based transaction
Research firms with IT Security resources	• particularly those with forensic capabilities
Network with other community banks	• Learn from their successes and failures

Response

How Compushare currently Assists other financial institutions

- ✓ Can help review the Institution's existing control structure
- ✓ Can identify what other Banks are doing that you are not
- ✓ Intrusion Prevention/Detection Services 24 X 7
- ✓ In the area of response, we offer forensic skills and experience that most community banks cannot afford in-house

Q&A

Special Offer

Compushare is offering an Exclusive promotion on our *Information Security Health Check* testing service to ICBA member banks including:

- ❑ Penetration Test
- ❑ Firewall Review
- ❑ Social Engineering

Offer good through December 31st

CHARTWELL

ICBA Compliance & Risk Management™

COMPUSHARE

Contact Information

Questions? Suggestions? Feedback?

EMAIL US!

COMPUSHARE
webinars@compushare.com

CHARTWELL
marythorson@chartwellcompliance.com