

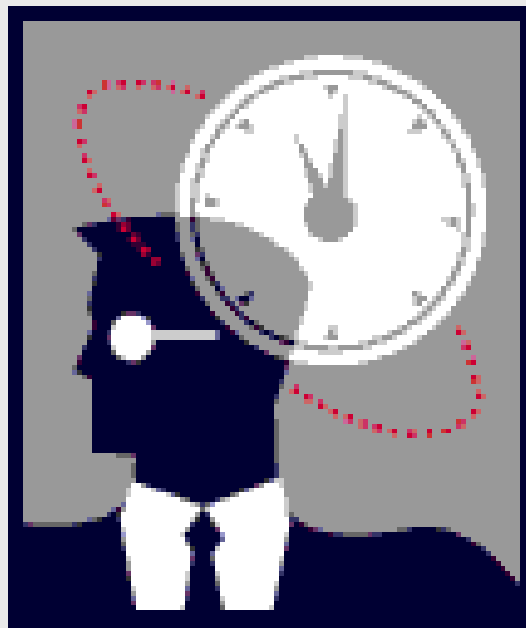
Beyond IT Compliance...
Responding to Current Cyber Threats in
Financial Services

Legal Responsibilities
with Cyber Fraud

James E. O'Connor
402.636.8332
joconnor@bairdholm.com

BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Hmmm... Legal Responsibilities with Cyber Fraud



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Schwarzenegger v. Entertainment
Merchants Association et al.

Hot Off the Press

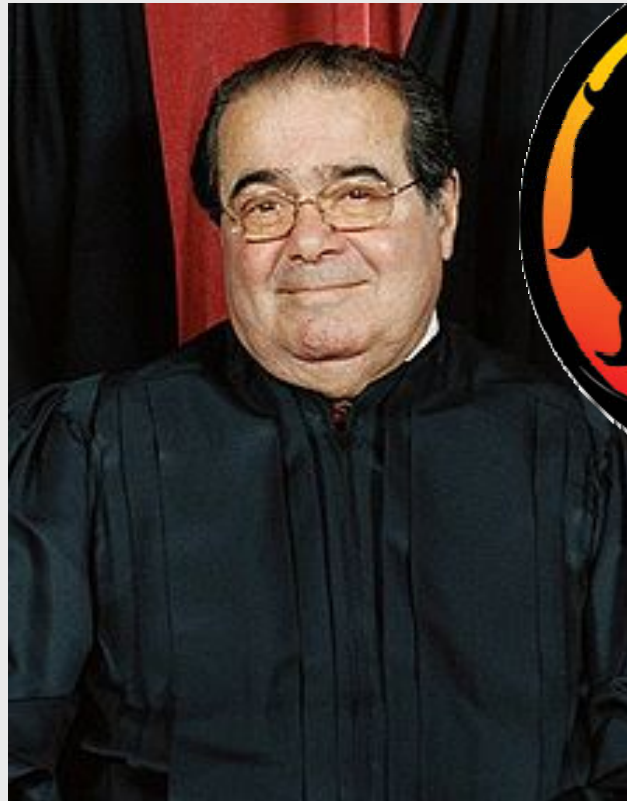
Case No. 08-1448

Oral Arguments

November 2, 2010

BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Justice Antonin Scalia



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Justice Sonia Sotomayor



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Agenda

Legal Responsibilities...

- Before
- After

a Cyber Fraud Event

Some Potential Theories of Liability

- Breach of Contract
- Negligence
- Invasion of Privacy
- Statute
- Regulation

Class Action Litigation

- Several class action lawsuits resulting from a security breach
- Targets:
 - Wells Fargo
 - Bank of New York
 - Mellon
 - Countrywide
 - Aflac
 - TJX

Some Potential Theories of Liability

- Breach of Contract
- Negligence
- Invasion of Privacy
- Statute
- Regulation

Regulations

HIPAA

Fair Credit Billing Act

FERPA

COPPA

EFTA

American Procedure Act

GLBA

Fair Credit Reporting Act

Cable Communications Policy Act

ECPA

Drivers Privacy Act

Computer Security Act

BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

Overview of U.S. Laws

- Gramm-Leach-Bliley Act (GLBA)
- Fair Credit Reporting Act (FCRA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- Children's Online Privacy Protection Act (COPPA)

ISO 27002

1. Risk Assessment
2. Security Policy
3. Security Organization
4. Asset Classification and Control
5. Personnel Security
6. Physical and Environmental Security
7. Communications and Operations Management
8. Access Control
9. Systems Development and Maintenance
10. Security Incident Management
11. Business Continuity Management
12. Compliance

Before the Breach

- **FTC Enforcement Actions**
 - "All companies must implement reasonable security for and limit their retention of sensitive consumer data. All companies must keep their promises about how they will use consumers' information. If they fail to do so – whether first party or third party, online or offline – we will go after them."
 - FTC Chairman Jon Liebowitz

Overview of State Laws

- Data breach notification laws
- Data encryption requirements
- Healthcare privacy laws
- Business privacy guides
- Laws mirroring federal requirements (GLBA, HIPAA) with distinct penalties

After the Breach



BAIRD HOLM^{LLP}
ATTORNEYS AT LAW

State Data Breach Notification Laws

- As of October 12, 2010, 46 states have security breach laws.
- The following states do not have security breach laws:
 - Alabama
 - Kentucky
 - New Mexico
 - South Dakota
- However, the following territories do have some form of data breach notification laws:
 - District of Columbia
 - Puerto Rico
 - Virgin Islands

State Data Breach Notification Laws (cont.)

- Varying triggers for reporting:
 - Likelihood PII has been or will be used for unauthorized purposes (NE)
 - Any breach (IL)
 - Paper as well as electronic (MA)

State Data Breach Notification Laws (cont.)

- The specific notice requirements vary by state. For example:
 - Florida and Ohio require notice within 45 days of the discovery of the breach.
 - Wisconsin requires notice within 15 days after the company learns of the breach.
 - North Carolina security breach notification law covers both electronic and hard copy documents.
 - Some states require notice only if a certain number of consumers or residents are affected (e.g., more than 1,000).
 - Some states require the company affected by the breach to notify all credit reporting agencies and the state's Attorney General's office.

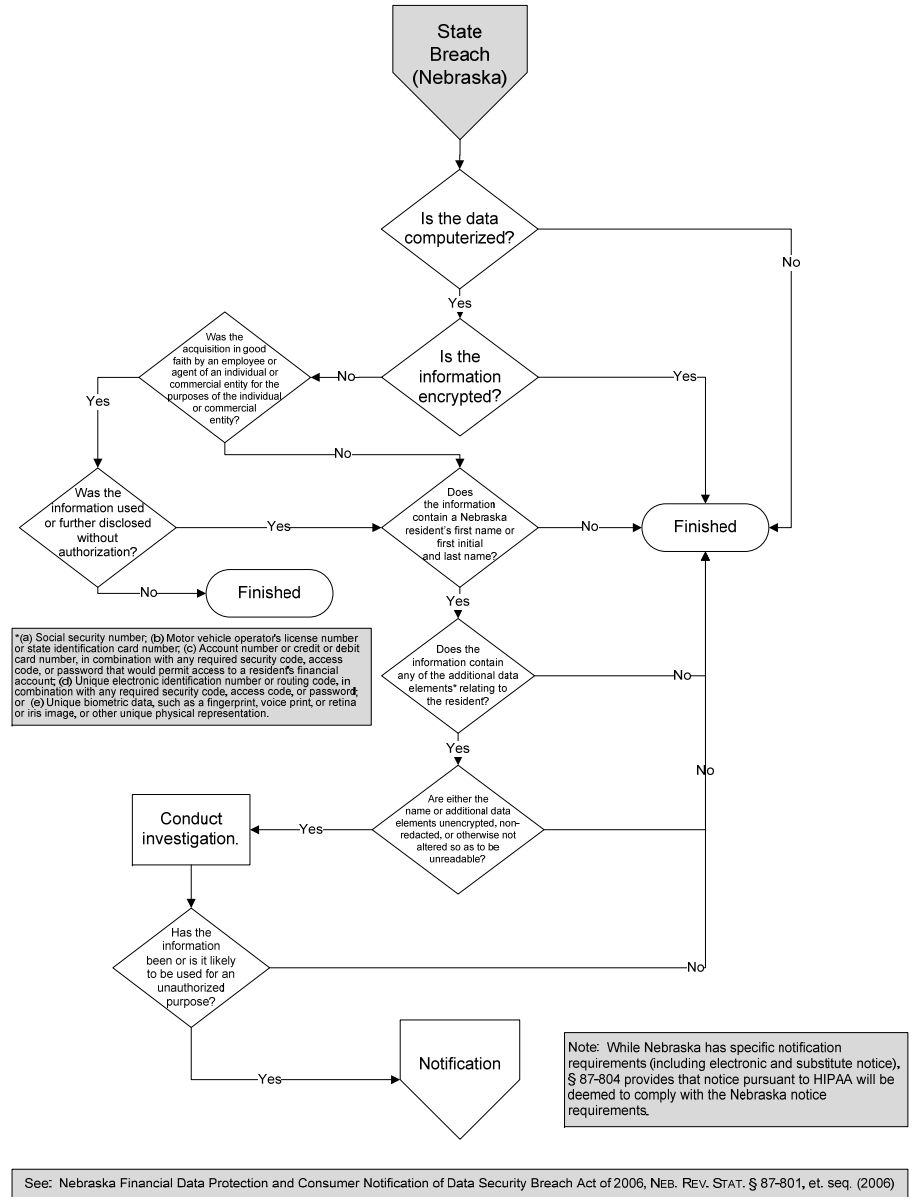
Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006

- Conduct business in Nebraska and system has personal information about a resident of Nebraska
- Become aware of a breach of the security of the system:
 - conduct in good faith a reasonable and prompt investigation to determine the likelihood that personal information has been or will be used for an unauthorized purpose
 - If the investigation determines that the use of information has occurred or is reasonably likely to occur, the individual or commercial entity shall give notice to the affected Nebraska resident.

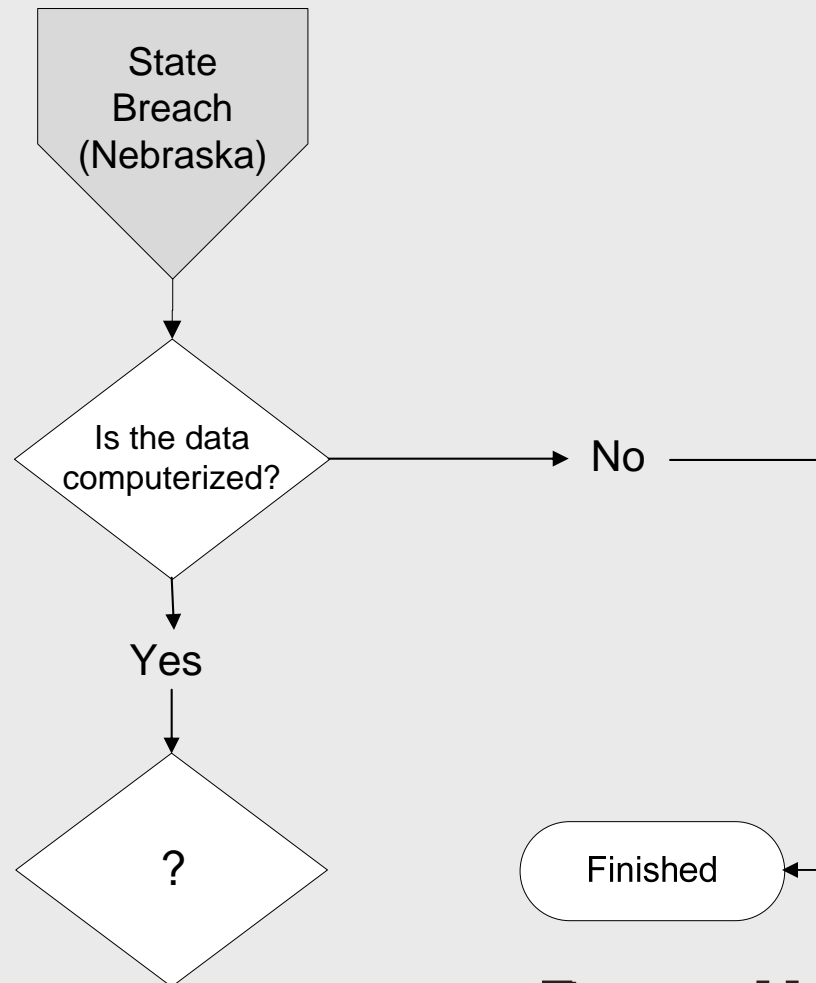
Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (cont.)

- Notice shall be made as soon as possible and without unreasonable delay.
- Attorney General may seek direct economic damages for each affected Nebraska resident.

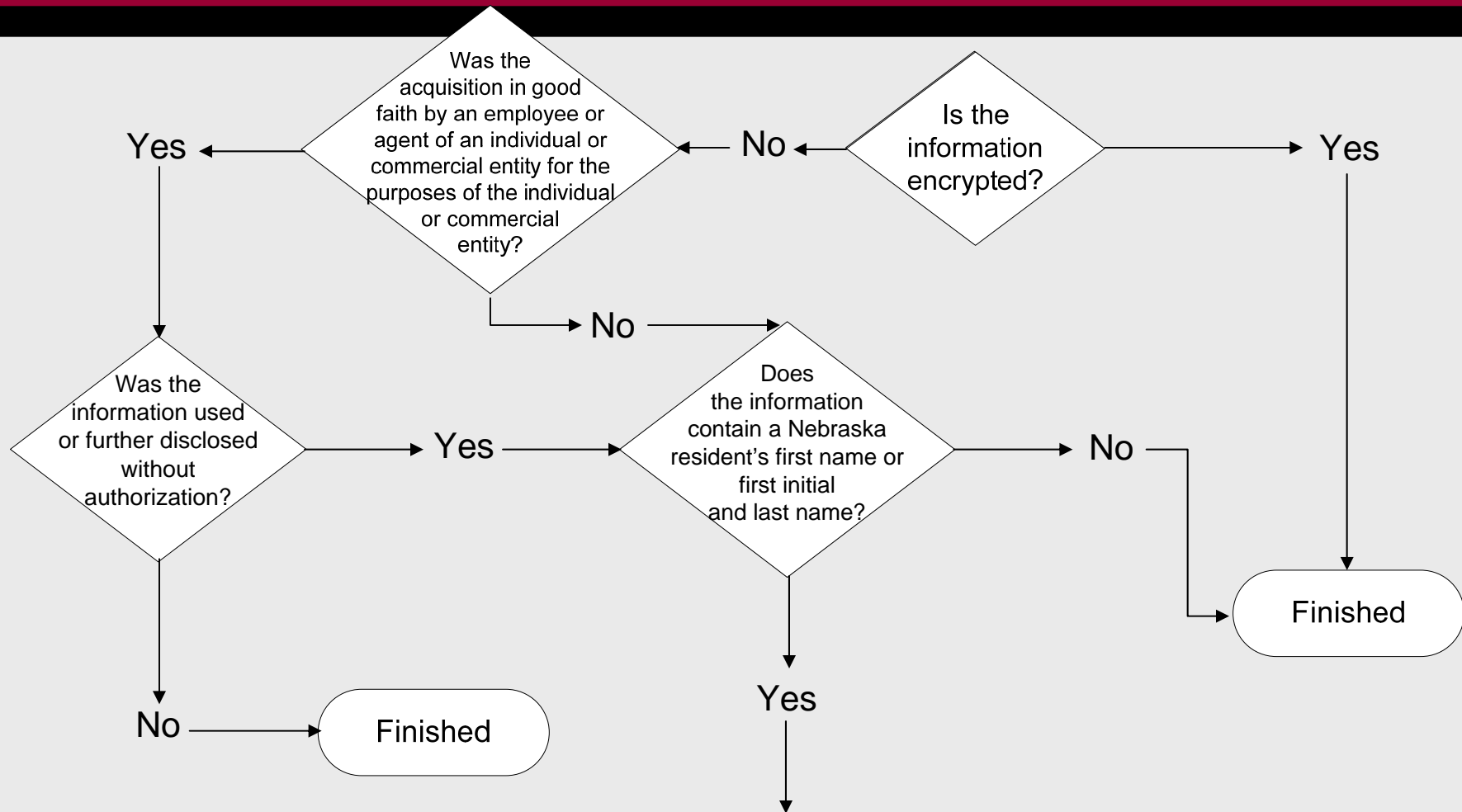
Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006 (cont.)



A Closer Look...

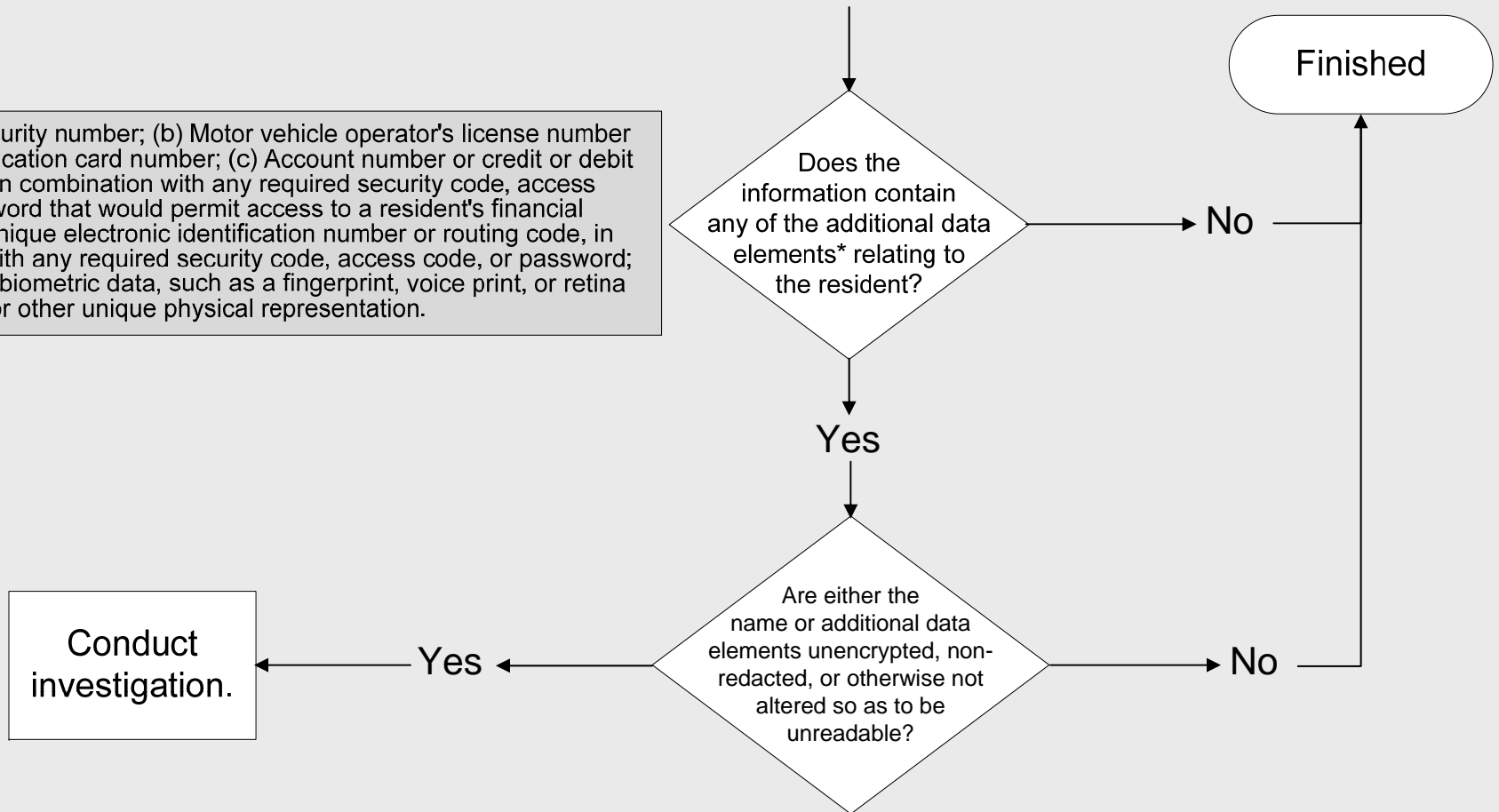


A Closer Look (cont.)

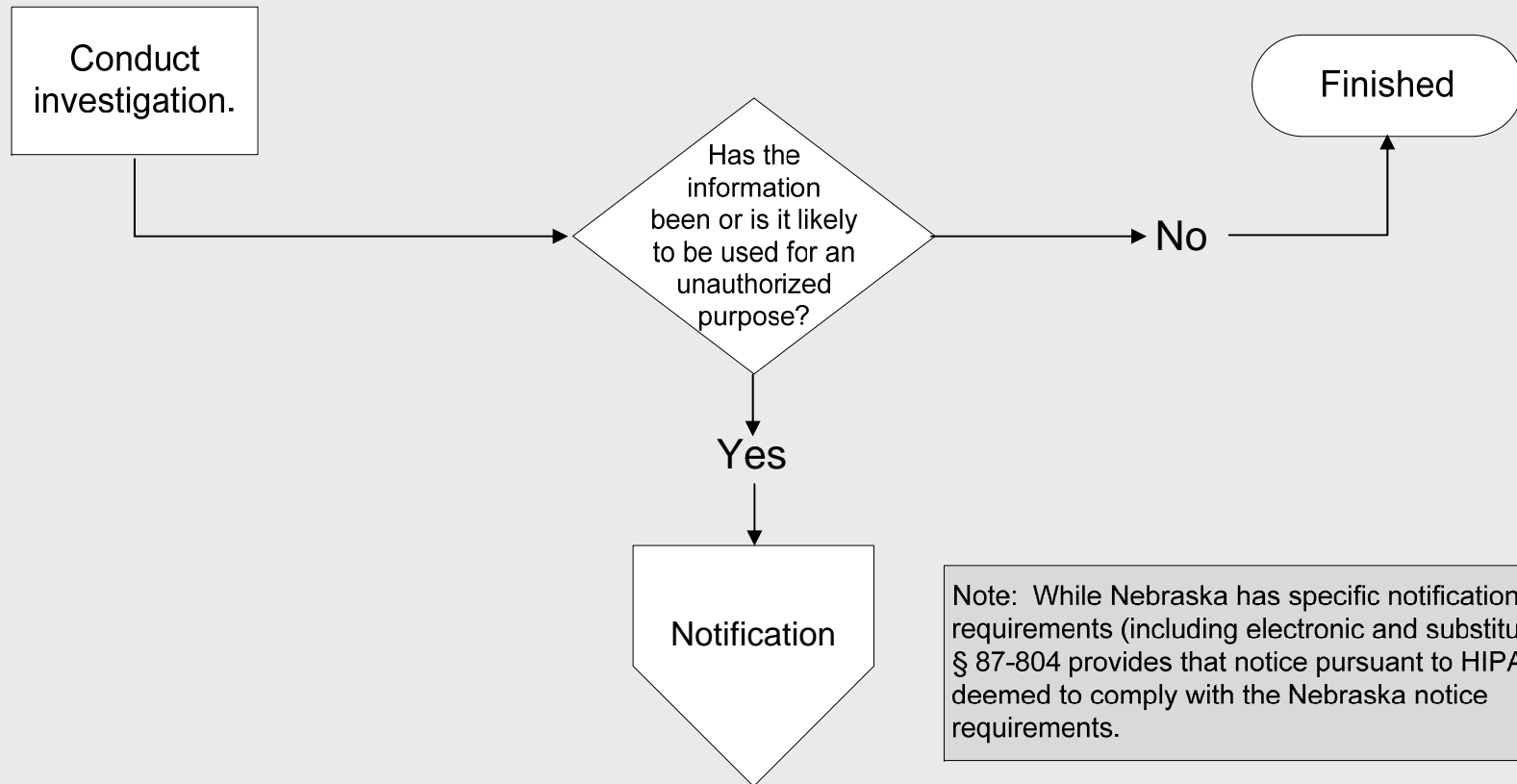


A Closer Look (cont.)

*(a) Social security number; (b) Motor vehicle operator's license number or state identification card number; (c) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial account; (d) Unique electronic identification number or routing code, in combination with any required security code, access code, or password; or (e) Unique biometric data, such as a fingerprint, voice print, or retina or iris image, or other unique physical representation.



A Closer Look (cont.)



See: Nebraska Financial Data Protection and Consumer Notification of Data Security Breach Act of 2006, NEB. REV. STAT. § 87-801, et. seq. (2006)

Notice Requirements

- Notice provided pursuant to the "Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice" is sufficient (except NY and GA):
 - A description of the incident in general terms and the type of customer information that was subject to the unauthorized access or use
 - A description of what the institution has done to protect the customer's information from further unauthorized access

Notice Requirements (cont.)

- A telephone number customers may call for further information and assistance
- A reminder that customers need to be vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution
- FTC has additional guidance "best practices"

Additional Obligations

- Notice may be required to national credit bureaus and consumer protection agencies
- Suspicious Activity Report (SAR) required if criminal violations suspected
- PCI Requirements

Additional State Laws

- Massachusetts *Standards for the Protection of Personal Information of Residents of the Commonwealth* (201 CMR 17.00)
- Comprehensive written information security program including:
 - risk assessment, policies, access controls, monitoring, annual review, user authentication, encryption (transmission, portable devices), etc.

Additional State Laws (cont.)

- Nevada Senate Bill 227 (signed into law May 29, 2009)
 - requires those accepting a payment card in connection with transaction to comply with Payment Card Industry (PCI) Data Security Standards
 - Others collecting or transmitting personal information must encrypt when in "an electronic nonvoice transmission other than a facsimile" or moving the data "beyond the logical or physical controls."

Recommendations

- Comprehensive privacy and security program
- Team: technical and legal
- Focus on culture – educate
- Limit collection of personal information
- Encrypt data at rest and in motion
- Portable devices
- Remote access - authentication

Best Practices

- Establish a security and privacy officer
- Internally assess risks to personal information
- Design a program that addresses:
 - System access controls
 - Physical access controls
 - Data encryption

Best Practices (cont.)

- Design a program that addresses:
 - Implementation of appropriate technological safeguards:
 - Firewalls
 - Monitoring software
 - Intrusion detection
 - Data breach and continuity response plans
 - Due diligence (SLAs, contract, compliance)

Best Practices (cont.)

- Design a program that addresses:
 - Employee screening procedures
 - Employee training
 - Records retention policies
- Test and monitor system
- Adjust to developing threats (internal and external)

Emerging Regulatory Trends

- 1.0 Incident based – breach notification
- 2.0 Reasonable requirements (GLB, HIPAA, FTC)
- 2.5 Encryption in transmission
- 3.0 More specific standards (including encryption at rest, user authentication, etc.)

Beyond IT Compliance...
Responding to Current Cyber Threats in
Financial Services

Legal Responsibilities
with Cyber Fraud

James E. O'Connor
402.636.8332
joconnor@bairdholm.com

BAIRDHOLM^{LLP}
ATTORNEYS AT LAW