

8th Annual

DIGITAL ID WORLD

“Driving Innovation with Identity”

PRODUCED BY CSO

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Enabling Legal SSO: **Traversing Applicable Laws and Liabilities**

Marc Lindsey

Partner

***Levine, Blaszak, Block &
Boothby, LLP ("LB3")***

www.lb3law.com

Disclaimer

This presentation is for informational purposes only and does not constitute legal advice. Discussions or answers to questions during the presentation should also not be relied upon as legal advice, and no attorney-client relationship will attach as a consequence of participation in this session.

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Introduction

- IdM and SSO, in particular, may trigger several information security and privacy laws
 - What identity attributes are collected, and how is personal information used and protected?
 - What legal liability attaches for failed / improper authentication or misuse of assertions?
 - Identity theft
 - Unauthorized access to information assets
 - Breach of privacy
 - Charges or obligations arising out of fraudulent and improperly authorized transactions
 - What are the minimum information security duties imposed on ID providers and relying organizations?

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Information Security Laws

- **E-Sign Act**
 - Federal law enacted in 2000
 - Preempts inconsistent state laws, but tolerates UETA
 - Consenting parties can conduct business electronically
 - Electronic transactions, notices and records must be given same legal effect as hard copy
 - No specific medium or technology for electronic records or signatures
 - Does not establish authentication standards

- **Sarbanes-Oxley Act**
 - Federal law enacted in 2002 in response to accounting scandals
 - Used to promote investor confidence in financial reporting
 - Applies to publicly traded companies
 - Imposes obligations for companies to adopt adequate internal controls
 - Requires annual reporting on controls, which must be certified by a corporate officer

- **FTC Red Flag Rules**
 - Takes effect November 1, 2009
 - Applies to financial institutions and **“creditors”** who regularly extend credit
 - Imposes an obligation to develop and implement an ID theft prevention program
 - Identify relevant patterns, practices, and specific forms of activity that signal possible identity theft (the “red flags”)
 - Incorporate the red flags into the ID theft program
 - Detect red flags
 - Respond to detected red flags
 - Update the program to reflect changes in ID theft risks

- **FTC Act, and Related Guidelines**
 - The FTC Act grants the FTC broad powers to protect consumers against unfair, deceptive acts or practices
 - Personal information collection best practices
 - Notice/awareness
 - Choice/consent
 - Access/participation
 - Integrity/security
 - Enforcement/redress

- FTC
 - Under the FTC Act, the FTC actively pursues unfair and deceptive practices related to personal information
 - Deceptive practices include a company's failure to follow or implement its own privacy policy to the detriment of consumers
 - Unfair practices include failure to adopt minimal levels of security (BJ's case)
 - *De facto* standard directs companies to implement reasonable information security programs to protect personal information

- **FTC**
 - *Remedies for violations of the FTC Act*
 - The FTC may seek relief in a civil suit based on the nature of the violation
 - Types of relief available to the FTC include
 - Contract rescission or reformation
 - Refunds to affected consumers
 - Payment of damages
 - Public notification of the violation
 - No private rights of action under the FTC Act
 - The FTC Act does not permit exemplary or punitive damages

- **Computer Fraud and Abuse Act (CFAA)**
 - *Who must comply?*
 - Generally applicable federal criminal statute
 - *What activities and information are covered?*
 - Accessing protected computer resources
 - Intercepting information or communications
 - Accessing government computers or national security information
 - Accessing computers to commit a crime
 - Causing damage to a protected computer
 - Trafficking in passwords
 - Threatening computer resources to cause damage

- CFAA (cont.)
 - *What are the key rules?*
 - May not access computer resources (without authorization) to intentionally engage in any of prohibited acts
 - **Exceeding authorization and then engaging in prohibited act is also a crime**
 - Damage threshold of \$5,000 over a 12 month-period for civil actions and felony criminal prosecution
 - Satisfying the loss threshold is the trick
 - Aggregating claims across victims and time requires a single act

- CFAA (cont.)
 - *Penalties for violations*
 - Private parties adversely affected can seek compensatory damages, injunctive relief and equitable remedies
 - Criminal fine and/or up to 10 years' imprisonment for the first offense and up to 20 years' imprisonment for repeat offenders

- **Federal “Common Law”**
 - Evolving standards imposing duty on corporations to adopt reasonable safeguards
 - Focus has been on employing adequate authentication measures and protecting personal information – particularly for identity theft prevention
 - Courts have examined information security measures to determine admissibility of electronic evidence
 - Deemed inadmissible where party offering electronic evidence can’t show proper information security establishes data is reliable

- Invasion of privacy under state common law
 - Elements: (1) unauthorized intrusion; (2) level of intrusion is offensive to a reasonable person; (3) intrusion relates to private matters; and (4) results in anguish or suffering
 - Most states recognize the tort
 - NY - No
 - CA - Yes

- 45 States (+P.R.) have **breach - notice** laws
- Typical statutory elements
 - Protected personal information covered
 - Name plus one or more identifying element
 - Social security #, driver's license #, other government ID #, financial account numbers and account access credentials
 - Health insurance or medical records
 - Applies to owners or delegated custodians of covered personal information of a citizen of the state
 - Notice triggering events
 - Actual unauthorized access or disclosure of unencrypted personal information
 - Reasonable belief of unauthorized access to such data

- Typical statutory elements (cont.)
 - Nature of the notice
 - Expediently inform affected individuals unless law enforcement directs otherwise
 - Some require notice to attorney general's office or equivalent
 - First class mail, e-mail if used in normal course and customer prior consent, if large number of affected consumers, public notice may be permitted.
 - Other factors and obligations
 - Some states require automatic notice when breach occurs (e.g., CA, NY)
 - Other states allow data handler to assess risk before issuing notice (e.g., CT, NJ, WA)
 - Data handlers required to employ reasonable safeguards to prevent breaches

8th Annual

DIGITAL ID WORLD

“Driving Innovation with Identity”

PRODUCED BY

CSO

Tips for Providers and Relying Parties to Consider

- Implement IdM solution around an assurance scheme
 - Design IdM that meets the required level of assurance
 - Enforce limits on scope of assertion
 - Only collect personal attribute data as required to satisfy level of assurance designated
- ICAM’s level of assurance scheme is a good reference
 - Level 1: Little or no confidence in the asserted identity’s validity
 - Level 2: Some confidence in the asserted identity’s validity
 - Level 3: High confidence in the asserted identity’s validity
 - Level 4: Very high confidence in the asserted identity’s validity

- Follow the FTC's general rule of reason to prepare information security measures:
 - Employ privacy protections that are based on the sensitivity of the personal data and the nature of assurance at issue, the types of risks faced, and the reasonable protections available to avoid/mitigate those risks.
- Adopt and implement data breach and notice policies that comply with *applicable* state laws:
 - Start with the states where your subjects' personal data is stored
 - Look to the states where you have principal offices
 - Examine states where you'll likely have subjects
 - Decide which laws are most applicable
 - Embrace the single, most restrictive, state law
 - Employ a patchwork based on each relevant state's statute
 - Safe harbors are available for data handlers that encrypt

- Key features providers to include in IdM solutions that collect personal information of subjects
 - Clear written privacy policy presented to subjects
 - Opt-in feature, with ability to opt-out easily
 - Allow subjects to select/de-select which and when third parties can obtain their personal information
 - Encrypt or redact personal information at rest and in storage
 - Destroy personal information after it is no longer used / required

- Adopt information security programs with key controls applicable to the IdM systems
 - Designate a security program responsible party
 - Initial risk assessment for each area of relevant operation
 - Employee training and management
 - Examine relevant information systems for vulnerabilities
 - Prevention, detection, and response to attacks, intrusions, or other systems failures
 - Design and implement reasonable safeguards
 - Regularly test and monitor the safeguards
 - Evaluate and adjust the key controls
 - Document the program and its outputs

- Relying entities should vet downstream/upstream vendors, not just the primary identity provider
- Trust partners should negotiate effective service and product agreements
 - Bind all parties in the trust circle, including identity providers
 - Monitoring conditions and incident response measures
 - Representations and warranties from identity providers
 - Service levels covering, at least, availability, accuracy, incident response/resolution, and compliance audit corrective action
 - Indemnifications covering losses/liabilities for non-compliance
 - Create remedies that address true cost of data breach, improper authentication and misuse of assertions

8th Annual

DIGITAL ID WORLD

"Driving Innovation with Identity"

PRODUCED BY

CSO

Questions?

Contact Information

Marc Lindsey

Levine, Blaszak, Block & Boothby, LLP

MLindsey@LB3Law.com

202.857.2550