VENABLE® LLP

Top Five Privacy and Data Security Issues for Nonprofit Organizations

Association of Corporate Counsel
Nonprofit Organizations Committee
Legal Quick Hit

Julia K. Tama, Esq.
Jeffrey S. Tenenbaum, Esq.

MAY 10, 2011

VENABLE® LLP

What Personal Information Do You Collect?

- Computerized or paper
- Collected from or about *individuals*
  - Clients, donors, supporters, members, volunteers, employees
- Common types of data:
  - Names and contact information
  - Payment card information
  - Social security or driver's license

VENABLE® LLP

Liability and Other Risks

- Federal laws – sector specific
- State "unfair or deceptive acts or practices" laws
  - Modeled on Federal Trade Commission Act
  - Enforced by state attorneys general
  - Private rights of action
- Reputational risks
  - Consumers are concerned about privacy and security
  - Potential for loss of public trust

VENABLE® LLP

Top Five Privacy and Data Security Issues

- Privacy policies
- Maintaining data security
- Preparing for the possibility of a breach
- Data-sharing and working with vendors
- Sensitive data

VENABLE® LLP

Privacy Policies: Basics

- Privacy policies = promises to the public
- Generally available when data is collected
- May apply to specific data collection streams – website, paper forms, etc.
- Must not be deceptive
- Promises travel with the data

VENABLE® LLP

Privacy Policies: Common Elements

- Scope of the policy
- What data you collect
- How you use data
- How you share data
- Individual choices or access rights (if any)
- Contact information
- Effective date

VENABLE® LLP

Privacy Policies: Common Pitfalls

- Forgetting to follow the policy
  - Exposure to liability for deception
- Promising too much
  - Avoid: “We will never share your information with anyone.”
  - Instead: No promise or “We may share data for purposes [such as]…” (e.g. if nonprofit becomes part of another organization)
- Updates: material changes should not be applied to data already collected, without notice and choice

VENABLE® LLP

Data Security: Duties and Guidance

- Privacy policies
- Massachusetts regulations (MA-201)
  - If data collected on MA resident
- Breach notification laws
  - May provide safe harbor for encryption or other protections
- Payment Card Industry Data Security Standards
- Enforcement precedents

VENABLE® LLP

Data Security Program: Process

- Identify responsible manager
- Assess risks and vulnerabilities
- Develop and implement data security program
- Train and discipline employees
- Re-assess and update regularly

VENABLE® LLP

Data Security Program: Contents

- Proportional to:
  - Data handled
  - Size and nature of organization
- Safeguards covering lifecycle of data
  - Administrative
  - Technical
  - Physical
- Employee policies
- Oversight of third parties

VENABLE® LLP

Preparing for Possible Data Breach

- Data breach can take many forms
- How to prepare:
  - Establish written incident response plan
  - Train all employees to identify and report
  - Designate employees to respond
  - Know where to get help
- Learn from experience

VENABLE® LLP

Incident Response Plan

- Proportional to organization's needs
- Assign responsibilities
- Secure the system
- Assess legal obligations (notification laws)
- Public and client relations
- Afterward:
  - Improve data security
  - Improve incident response plan

VENABLE® LLP

Data Breach Notification Laws

- Almost all states have data breach notification laws, which may apply to nonprofits
- Comply with laws of state with *affected individuals*, not where organization is located
- **Even if law applies, not all incidents require notification**
  - Exceptions and safe harbors, such as encryption

VENABLE® LLP

If Notification Is Required

- Generally, burden on “owner or licensor” of data
- Notice provided to:
  - Individuals
  - State authorities
  - Credit reporting agencies
- Required content, method, deadlines

VENABLE® LLP

Data Sharing: Sales or Rentals

- In accord with privacy policy and other promises
- Privacy promises travel with data
- Consider offering individual choice
  - Usually opt-out

When obtaining data, the same considerations apply to your data supplier

VENABLE® LLP

Data Sharing: Vendors and Service Providers

- In accord with privacy policy and other promises
- Contracting considerations:
  - Restrictions on use/disclosure of data
  - Reps and warranties of compliance with privacy and security obligations
  - Can assign breach notification duties
- Adequate supervision
- Cloud computing: pros and cons

VENABLE® LLP

Sensitive Data

- Additional federal or state obligations may apply
- Examples of sensitive data:
  - Financial
  - Payment card
  - Health
  - Children
  - Social Security numbers
  - Other data, depending on context

VENABLE® LLP

Payment Card Data

- Payment Card Industry Data Security Standards (PCI DSS)
  - 12 security standards created by the credit card industry
  - Practices and policies to protect accountholder data
- Implementation
  - Compliance steps depend on card processing volume
  - Qualified Security Assessors (QSAs) can assist
  - Information security policy is required
  - Service providers should be PCI DSS compliant
- Enforcement
  - Credit card brands require merchant banks to enforce compliance by their clients
    - Fines imposed on banks can be passed on to organizations
  - States, including Minnesota, have recently enacted statutory requirements similar to PCI DSS

Contact Information

Julia K. Tama, Attorney
jktama@venable.com
t 202.344.4738

Jeffrey S. Tenenbaum, Partner
jstenenbaum@venable.com
t 202.344.8138

www.venable.com/nonprofits/publications

www.venable.com