An abstract graphic on the left side of the page, consisting of several overlapping, translucent, geometric shapes in shades of blue, teal, and grey, creating a sense of depth and movement.

A Breach Can Happen to You (or Already Has, and You Just Don't Know It Yet): How Nonprofits Can Best Manage Cybersecurity Risk

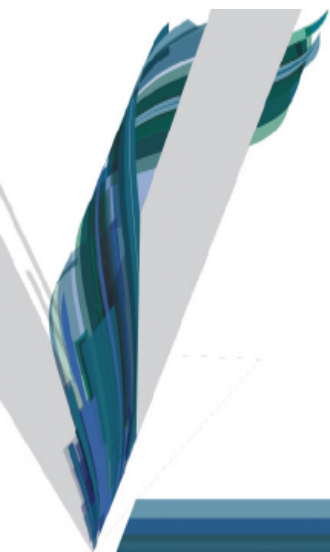
Thursday, December 10, 2015, 12:30 – 2:00 pm ET
Venable LLP, Washington, DC

Moderator

Jeffrey S. Tenenbaum, Esq., Partner and Chair of
the Nonprofit Organizations Practice, Venable LLP

Speakers

Erik Jones, Esq., Partner, Venable LLP
Bobby N. Turnage, Jr., Esq., Partner, Venable LLP
Dan Koslofsky, Esq., Chief Privacy & Compliance
Officer, AARP



Presentation



A Breach Can Happen to You (or Already Has, and You Just Don't Know It Yet): How Nonprofits Can Best Manage Cybersecurity Risk

Thursday, December 10, 2015, 12:30 – 2:00 pm ET

Venable LLP, Washington, DC

Moderator

Jeffrey S. Tenenbaum, Esq., Partner and Chair of the Nonprofit
Organizations Practice, Venable LLP

Speakers

Erik Jones, Esq., Partner, Venable LLP

Bobby N. Turnage, Jr., Esq., Partner, Venable LLP

Dan Koslofsky, Esq., Chief Privacy & Compliance Officer, AARP

© 2015 Venable LLP



CAE Credit Information

***Please note that CAE credit is available only
to registered participants of the live
program.**


As a CAE Approved Provider educational program related to the
CAE exam content outline, this program may be applied for
1.5 credits toward your CAE application
or renewal professional development requirements.

Venable LLP is a CAE Approved Provider. This program meets the requirements for fulfilling the professional development requirements to earn or maintain the Certified Association Executive credential. Every program we offer that qualifies for CAE credit will clearly identify the number of CAE credits granted for full, live participation, and we will maintain records of your participation in accordance with CAE policies. For more information about the CAE credential or Approved Provider program, please visit www.whatiscae.org.

Note: This program is not endorsed, accredited, or affiliated with ASAE or the CAE Program. Applicants may use any program that meets eligibility requirements in the specific timeframe towards the exam application or renewal. There are no specific individual courses required as part of the applications—selection of eligible education is up to the applicant based on his/her needs.

© 2015 Venable LLP

VENABLE 2




Upcoming Venable Nonprofit Events

Register Now

- **January 14, 2016:** [Impact Investing and Nonprofits: Opportunities, Innovative Structures, and Creative New Ways to Raise Funds and Further Your Mission](#)
- **February 4, 2016:** Nonprofit Chapters and Affiliates: Finding Structures and Relationships That Address Your Challenges and Work Well for Everyone (*details and registration available soon*)
- **March 10, 2016:** Nonprofit Federal Award Recipients: Meeting New Requirements, Avoiding Dangerous Pitfalls, and Adding Value through a Strong Compliance Program (*details and registration available soon*)

© 2015 Venable LLP

VENABLE 3



Agenda

- What do the bad guys want?
- Who are they?
- How do they do it?
- What are the potential harms?
- What can I do now to help prevent a breach?
- What can I do now to help mitigate the harm of a breach?
- What should I do when there's a breach?
- Q&A

© 2015 Venable LLP

VENABLE 4



What Do the Bad Guys Want?

- Customer or Client Data
- Trade Secrets/IP/Confidential Information
 - Includes 3rd party information
- Employee Data
- Financial Assets
 - Payment cards; banking information
- Disruption/Destruction
 - Extortion, revenge or just for kicks



Who Are the Bad Guys?

- Nation-state sponsored (APT)
 - Intelligence gathering or disruption
 - Political, economic or military
- Organized crime – financially motivated
- “Hacktivists” – focused on notoriety or a cause
- Disgruntled employees and customers
 - Former and current



How Do They Do It?

- Vulnerabilities in system
 - Very patient and probing
 - Will move laterally through system
- Third-party vendors
- Rogue employees with inside access
- Well-meaning employees – inadvertently:
 - Social engineering
 - Phishing
 - Malware in email
- DDOS attacks

© 2015 Venable LLP

VENABLE 7



What Are Some of the Potential Harms?

- Loss of IP
- Loss of financial assets
- Loss of customer data
- Loss of trade secrets/confidential information
- Loss of reputation
- Loss of business (due to interruption)
- Costs of forensic investigation
- Costs of legal counsel

© 2015 Venable LLP

VENABLE 8



What Are Some of the Potential Harms?

- Costs of 3rd party claims and damages
- Costs of contractual liability claims/damages
- Costs of regulator investigations and penalties
- Costs of notification/credit monitoring
- Costs of customer call center
- Costs of crisis management/PR firm
- Costs of remediation

© 2015 Venable LLP

VENABLE 9



What Can I Do Now to Help Prevent a Breach?

- Designate responsible individual
- Review current systems, physical facilities and processes for vulnerabilities
 - Consider security consultant (and remember attorney-client privilege)
- Conduct regular security audits
- Review contracts with relevant vendors
 - Require data security commitments
 - Require reps & warranties
 - Helps flush out important issues
 - Forces vendor to take it seriously
 - Caution: "I'll sign your paper today"

© 2015 Venable LLP

VENABLE 10



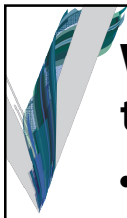
What Can I Do Now to Help Prevent a Breach?

- Perform due diligence around vendor systems and facilities
- Perform due diligence of acquisition target systems
- Ensure system updates and maintenance are performed in a timely manner



What Can I Do Now to Help Prevent a Breach?

- Train employees on security do's and don'ts
 - Regularly
- Maintain written security policy (will address things like destruction of documents, safeguarding and destruction of computer [including copier] hard drives, physical security, passwords, etc.)
- Maintain top-down emphasis (from board level and executive team) on security



What Can I Do Now to Help Mitigate the Harm of a Breach?

- Review compliance with legal and contractual data security requirements
 - Health care
 - Financial services
 - PCI-DSS
 - 3rd party contracts
- Consult Government Resources
 - NIST Cybersecurity Framework
 - “Lessons Learned from FTC Cases”
 - State AG Guidance

© 2015 Venable LLP

VENABLE 13



What Can I Do Now to Help Mitigate the Harm of a Breach?

- Maintain appropriate insurance coverage
 - Include cyber insurance
 - Use a knowledgeable broker/consultant
- Prepare incident response plan
 - “The Game Plan”

© 2015 Venable LLP

VENABLE 14



What Can I Do Now to Help Mitigate the Harm of a Breach?

- Review privacy promises to ensure consistency with actual practices
- Review vendor and customer contracts
 - **Appropriate** risk shifting (includes insurance)
 - Notification obligations
- Confirm vendor insurance

© 2015 Venable LLP

VENABLE 15



What Should I Do When There's a Breach?

- Isolate compromised systems, if applicable
- Preserve relevant logs and other IT data
- Activate incident response plan and notify relevant POCs
- Retain data breach law firm to:
 - Advise on notification and messaging
 - Retain forensic firm (for privilege)
 - Help avoid missteps that will be second-guessed later

© 2015 Venable LLP

VENABLE 16



What Should I Do When There's a Breach?

- Notify insurance carrier
 - Coordinate with carrier throughout
 - Carrier may have experience to share
 - Coordination reduces chances of misunderstanding leading to coverage issues
- Retain forensic firm (if applicable)
 - Have law firm retain (for privilege/work product)

© 2015 Venable LLP

VENABLE 17



What Should I Do When There's a Breach?

- Exercise caution with written communications
- Refer all press inquiries to PR department or designated individual
- Add additional members to response team as needed
 - Public relations (internal and/or external)
 - Customer service
 - HR

© 2015 Venable LLP

VENABLE 18



What Should I Do When There's a Breach?

- Establish command center (law department) for coordination of all activities related to breach
- Review contracts for notification obligations
- Notify 3rd parties (law enforcement, regulators, individuals and 3rd party businesses) where required by law



Questions?

Jeffrey S. Tenenbaum, Esq.,
Partner and Chair of the Nonprofit Organizations Practice, Venable LLP
jstenenbaum@Venable.com
t 202.344.8138

Erik Jones, Esq., Partner, Venable LLP
ecjones@Venable.com
t 202.344.4438

Bobby N. Turnage, Jr., Esq., Partner, Venable LLP
bturnage@Venable.com
t 703.760.1600

Dan Koslofsky, Esq., Chief Privacy & Compliance Officer, AARP
Dkoslofsky@aarp.org
t 202.434.3525

To view an index of Venable's articles and presentations or upcoming programs on nonprofit legal topics, see www.Venable.com/nonprofits/publications or www.Venable.com/nonprofits/events.

To view recordings of Venable's nonprofit programs on our YouTube channel, see www.YouTube.com/VenableNonprofits or www.Venable.com/nonprofits/recordings.

Follow [@NonprofitLaw](https://twitter.com/NonprofitLaw) on Twitter for timely posts with nonprofit legal articles, alerts, upcoming and recorded speaking presentations, and relevant nonprofit news and commentary.



Speaker Biographies



Jeffrey S. Tenenbaum

Partner

Washington, DC Office

T 202.344.8138 F 202.344.8300

jstenenbaum@Venable.com

AREAS OF PRACTICE

Tax and Wealth Planning
Antitrust
Political Law
Business Transactions Tax
Tax Controversies and Litigation
Tax Policy
Tax-Exempt Organizations
Wealth Planning
Regulatory

INDUSTRIES

Nonprofit Organizations and Associations
Financial Services

GOVERNMENT EXPERIENCE

Legislative Aide, United States House of Representatives

BAR ADMISSIONS

District of Columbia

EDUCATION

J.D., Catholic University of America, Columbus School of Law, 1996

Jeffrey Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. He is one of the nation's leading nonprofit attorneys, and also is a highly accomplished author, lecturer, and commentator on nonprofit legal matters. Based in the firm's Washington, DC office, Mr. Tenenbaum counsels his clients on the broad array of legal issues affecting charities, foundations, trade and professional associations, think tanks, advocacy groups, and other nonprofit organizations, and regularly represents clients before Congress, federal and state regulatory agencies, and in connection with governmental investigations, enforcement actions, litigation, and in dealing with the media. He also has served as an expert witness in several court cases on nonprofit legal issues.

Mr. Tenenbaum was the 2006 recipient of the American Bar Association's Outstanding Nonprofit Lawyer of the Year Award, and was an inaugural (2004) recipient of the *Washington Business Journal's* Top Washington Lawyers Award. He was one of only seven "Leading Lawyers" in the Not-for-Profit category in the prestigious 2012 *Legal 500* rankings, one of only eight in the 2013 rankings, one of only nine in the 2014 rankings, and also one of only 10 in the 2015 rankings. Mr. Tenenbaum was recognized in 2013 as a Top Rated Lawyer in Tax Law by *The American Lawyer* and *Corporate Counsel*. He was the 2015 recipient of the New York Society of Association Executives' Outstanding Associate Member Award, the 2004 recipient of The Center for Association Leadership's Chairman's Award, and the 1997 recipient of the Greater Washington Society of Association Executives' Chairman's Award. Mr. Tenenbaum was listed in the 2012-16 editions of *The Best Lawyers in America* for Non-Profit/Charities Law, and was selected for inclusion in the 2014 and 2015 editions of *Washington DC Super Lawyers* in the Nonprofit Organizations category. In 2011, he was named as one of Washington, DC's "Legal Elite" by *SmartCEO Magazine*. He was a 2008-09 Fellow of the Bar Association of the District of Columbia and is AV Peer-Review Rated by *Martindale-Hubbell*. Mr. Tenenbaum started his career in the nonprofit community by serving as Legal Section manager at the American Society of Association Executives, following several years working on Capitol Hill as a legislative assistant.

REPRESENTATIVE CLIENTS

AARP
Air Conditioning Contractors of America
Airlines for America
American Academy of Physician Assistants
American Alliance of Museums
American Association for the Advancement of Science
American Bar Association
American Cancer Society
American College of Cardiology
American College of Radiology

B.A., Political Science, University of Pennsylvania, 1990

MEMBERSHIPS

American Society of Association Executives

New York Society of Association Executives

American Council of Education
American Friends of Yahad in Unum
American Institute of Architects
American Red Cross
American Society for Microbiology
American Society of Anesthesiologists
American Society of Association Executives
America's Health Insurance Plans
Association for Healthcare Philanthropy
Association for Talent Development
Association of Clinical Research Professionals
Association of Corporate Counsel
Association of Fundraising Professionals
Association of Global Automakers
Association of Private Sector Colleges and Universities
Auto Care Association
Biotechnology Industry Organization
Brookings Institution
Carbon War Room
CFA Institute
The College Board
CompTIA
Council on Foundations
CropLife America
Cruise Lines International Association
Design-Build Institute of America
Erin Brockovich Foundation
Ethics Resource Center
Foundation for the Malcolm Baldrige National Quality Award
Gerontological Society of America
Global Impact
Goodwill Industries International
Graduate Management Admission Council
Habitat for Humanity International
Homeownership Preservation Foundation
Human Rights Campaign
Independent Insurance Agents and Brokers of America
Institute of International Education
International Association of Fire Chiefs
International Sleep Products Association
Jazz at Lincoln Center
LeadingAge
The Leukemia & Lymphoma Society
Lincoln Center for the Performing Arts
Lions Club International
March of Dimes
ment'or BKB Foundation
Money Management International
National Association for the Education of Young Children
National Association of Chain Drug Stores
National Association of College and University Attorneys
National Association of County and City Health Officials
National Association of Manufacturers
National Association of Music Merchants
National Athletic Trainers' Association
National Board of Medical Examiners
National Coalition for Cancer Survivorship
National Coffee Association
National Council of Architectural Registration Boards
National Council of La Raza
National Defense Industrial Association
National Fallen Firefighters Foundation
National Fish and Wildlife Foundation
National Propane Gas Association
National Quality Forum

National Retail Federation
National Student Clearinghouse
The Nature Conservancy
NeighborWorks America
New Venture Fund
NTCA - The Rural Broadband Association
Nuclear Energy Institute
Peterson Institute for International Economics
Professional Liability Underwriting Society
Project Management Institute
Public Health Accreditation Board
Public Relations Society of America
Romance Writers of America
Telecommunications Industry Association
Trust for Architectural Easements
The Tyra Banks TZONE Foundation
U.S. Chamber of Commerce
United States Tennis Association
Volunteers of America
Water Environment Federation
Water For People

HONORS

Recipient, New York Society of Association Executives' Outstanding Associate Member Award, 2015

Recognized as "Leading Lawyer" in *Legal 500*, Not-For-Profit, 2012-15

Listed in *The Best Lawyers in America* for Non-Profit/Charities Law (Woodward/White, Inc.), 2012-16

Selected for inclusion in *Washington DC Super Lawyers*, Nonprofit Organizations, 2014-15

Served as member of the selection panel for the inaugural *CEO Update* Association Leadership Awards, 2014

Recognized as a Top Rated Lawyer in Taxation Law in *The American Lawyer* and *Corporate Counsel*, 2013

Washington DC's Legal Elite, *SmartCEO Magazine*, 2011

Fellow, Bar Association of the District of Columbia, 2008-09

Recipient, American Bar Association Outstanding Nonprofit Lawyer of the Year Award, 2006

Recipient, *Washington Business Journal* Top Washington Lawyers Award, 2004

Recipient, The Center for Association Leadership Chairman's Award, 2004

Recipient, Greater Washington Society of Association Executives Chairman's Award, 1997

Legal Section Manager / Government Affairs Issues Analyst, American Society of Association Executives, 1993-95

AV® Peer-Review Rated by *Martindale-Hubbell*

Listed in *Who's Who in American Law* and *Who's Who in America*, 2005-present editions

ACTIVITIES

Mr. Tenenbaum is an active participant in the nonprofit community who currently serves on the Editorial Advisory Board of the American Society of Association Executives' *Association Law & Policy* legal journal, the Advisory Panel of Wiley/Jossey-Bass' *Nonprofit Business Advisor* newsletter, and the ASAE Public Policy Committee. He previously served as Chairman of the *AL&P* Editorial Advisory Board and has served on the ASAE Legal Section Council, the ASAE Association Management Company Accreditation Commission, the GWSAE Foundation Board of Trustees, the GWSAE Government and Public Affairs Advisory Council, the Federal City Club

Foundation Board of Directors, and the Editorial Advisory Board of Aspen's *Nonprofit Tax & Financial Strategies* newsletter.

PUBLICATIONS

Mr. Tenenbaum is the author of the book, *Association Tax Compliance Guide*, now in its second edition, published by the American Society of Association Executives. He also is a contributor to numerous ASAE books, including *Professional Practices in Association Management*, *Association Law Compendium*, *The Power of Partnership*, *Essentials of the Profession Learning System*, *Generating and Managing Nondues Revenue in Associations*, and several Information Background Kits. In addition, he is a contributor to *Exposed: A Legal Field Guide for Nonprofit Executives*, published by the Nonprofit Risk Management Center. Mr. Tenenbaum is a frequent author on nonprofit legal topics, having written or co-written more than 700 articles.

SPEAKING ENGAGEMENTS

Mr. Tenenbaum is a frequent lecturer on nonprofit legal topics, having delivered over 700 speaking presentations. He served on the faculty of the ASAE Virtual Law School, and is a regular commentator on nonprofit legal issues for *NBC News*, *The New York Times*, *The Wall Street Journal*, *The Washington Post*, *Los Angeles Times*, *The Washington Times*, *The Baltimore Sun*, *ESPN.com*, *Washington Business Journal*, *Legal Times*, *Association Trends*, *CEO Update*, *Forbes Magazine*, *The Chronicle of Philanthropy*, *The NonProfit Times* and other periodicals. He also has been interviewed on nonprofit legal topics on Fox 5 television's (Washington, DC) morning news program, Voice of America Business Radio, Nonprofit Spark Radio, and The Inner Loop Radio.



Erik Jones

Partner

Washington, DC Office

T 202.344.4438 F 202.344.8300

ecjones@Venable.com

AREAS OF PRACTICE

Congressional Investigations
State Attorneys General
Investigations and White Collar
Defense
Privacy and Data Security
Regulatory
Legislative and Government Affairs
Communications

INDUSTRIES

Cybersecurity

GOVERNMENT EXPERIENCE

Assistant Attorney General and
Director of the Policy Bureau,
Office of the Illinois Attorney
General
Deputy General Counsel and Chief
Investigative Counsel, United
States Senate Committee on
Commerce, Science, and
Transportation
Counsel, United States House
Energy and Commerce Committee
Counsel, United States House
Oversight and Government Reform
Committee

Erik Jones is a partner in Venable's Washington, DC office, where he helps lead the firm's Congressional Investigations practice and works closely with the State Attorneys General and E-Commerce, Privacy and Data Security practices. He has significant investigatory and policy experience in state and federal government, as well as the private sector.

Prior to joining Venable, Mr. Jones served as an Assistant Attorney General and Director of the Policy Bureau for the Office of Illinois Attorney General Lisa Madigan. In this position, he was responsible for developing and managing the office's agenda through legislation, investigations, and outreach initiatives. Among his responsibilities, Mr. Jones served as the Attorney General's lead advisor on data security and privacy.

Previously, Mr. Jones was Deputy General Counsel and Chief Investigative Counsel to the U.S. Senate Committee on Commerce under Sen. Jay Rockefeller, where he helped create the Committee's Office of Oversight and Investigations and later served as its lead counsel on cybersecurity matters. Prior to his work in the Senate, Mr. Jones was Counsel to the House Committee on Energy & Commerce and Oversight & Government Reform, chaired by Rep. Henry Waxman. During his time in Congress, he helped direct more than 30 investigations and hearings.

Mr. Jones led and worked on a diverse range of congressional investigations related to e-commerce practices, privacy, telecommunications, transportation, energy, space policy, environmental regulations, product safety, the financial sector, health care, and government contracting. Notably, he led the Commerce Committee's investigation of abusive billing practices on the Internet and used the findings of the investigation to draft the Restore Online Shoppers' Confidence Act (ROSCA), signed into law by President Obama in 2010. While serving as counsel to the House Oversight Committee, he led the investigation that uncovered high levels of formaldehyde in trailers that the Federal Emergency Management Agency supplied to victims of Hurricane Katrina.

Mr. Jones has been especially active at the intersection of law and technology. He played a major role in congressional work on data security and technology issues, taking the lead in drafting and negotiating significant portions of the Cybersecurity Act. He led the Commerce Committee's survey of cybersecurity practices among Fortune 500 companies and helped push for the establishment of the NIST Cybersecurity Framework, the public-private partnership for developing cybersecurity standards. He also directed the first federal investigation into the privacy practices of data brokers and managed the Committee's Internet governance portfolio, which included ICANN's decision to expand top-level domain names.

While working in the Illinois AG's office, he helped develop and implement a plan to respond to the wave of data breaches affecting consumers. He was the primary staff attorney working with the AG who drafted and negotiated the first significant update to Illinois law on data security. He also directed efforts to educate Illinois businesses

BAR ADMISSIONS

Illinois

District of Columbia

EDUCATION

J.D., University of Michigan Law School, 2004

Associate Editor, *Michigan Journal of Law Reform*

B.S., *magna cum laude*, Southern Illinois University Edwardsville, 2001

MEMBERSHIPS

International Association of Privacy Professionals

American Council of Young Political Leaders

and residents on data privacy and data security issues, and participated in numerous investigations of significant data breaches affecting Fortune 500 companies. During his time with the office, Mr. Jones also initiated and led the Attorney General's inquiry into the collection of consumer medical information by websites and apps, led a statewide investigation into employers' use of payroll cards, successfully drafted and negotiated a law to regulate payroll cards, and drafted and negotiated a law aimed at patent trolls.

Mr. Jones began his career in private practice at an international law firm, where he split his time between the white-collar criminal defense practice group and the e-commerce and privacy practice group.

ACTIVITIES

- Adjunct Professor, Illinois Institute of Technology Chicago-Kent College of Law

SPEAKING ENGAGEMENTS

- December 10, 2015, A Breach Can Happen to You (or Already Has, and You Just Don't Know It Yet): How Nonprofits Can Best Manage Cybersecurity Risk
- September 29, 2015, "The Cybersecurity Threat - What You Can't See Can Hurt You" at a M&T Bank, Wilmington Trust and Venable LLP Thought Leadership Breakfast
- March - April 2015, Witness at legislative hearings on data security before the Judiciary Committees for the Illinois Senate and House of Representatives
- July 2014, Witness at a hearing, "Data Security and Identity Theft" before the Finance Committee of the Chicago City Council
- June 2014, Speaker on a panel on patent trolls at the Association of Corporate Patent Counsel's summer meeting
- April 2014, Speaker on a panel, "Challenges in Assessing Medical Apps" at Chicago-Kent College of Law's conference on Medical Apps, Privacy, and Liability
- March 2014, Witness at legislative hearings on patent trolls before the Judiciary Committees for the Illinois Senate and House of Representatives
- March 2014, Speaker on a panel, "Regulation of Data Security" at Loyola University Chicago Consumer Law Review's Symposium on Consumer Privacy and Data Collection
- September 2013, Speaker on panel, "Framing Big Data and Privacy" at a conference cohosted by the Future of Privacy Forum and the Stanford Center for Internet and Society
- March 2013, Speaker on a panel, "The Data-Driven Way of Life: Threats and Solutions" at the Direct Marketing Association's "DMA in DC 2013" Program
- February 2013, Speaker on a panel, "Cyber Warriors: What do they do and how do we get more of them?" at the TechVoice DC Fly-In hosted by CompTIA
- January 2013, Speaker in a breakout session on "Plumbing the Policy Implications of Data Analytics and Defining 'Big Data,' the Year's Most Overused Term" for the State of the Net Conference hosted by the Congressional Internet Caucus Advisory Committee
- February 2012, Speaker in a webcast for Continuing Legal Education (CLE) credit on "Congressional Investigations 2012: How to Prepare for the Investigative Agenda in the New Year"
- May 2011, Featured speaker at the Federal Trade Commission's Forum on "Examining Telephone Bill Cramming" and spoke on a panel, "Potential Solutions to the Cramming Problem"
- October 2010, Guest lecturer for the University of California's Program "Law and Lawyering in the Nation's Capital" and jointly led a lecture on "Investigations by the Federal Government: Perspectives from the Executive Branch and Congress"



Bobby N. Turnage, Jr.

Partner

*Washington, DC Office
Tysons Corner, VA Office*

T 202.344.4839 F 202.344.8300

bturnage@Venable.com

AREAS OF PRACTICE

Corporate
Privacy and Data Security
Advertising and Marketing
Intellectual Property
Technology Transactions and Outsourcing
Domain Names and Cyber Protection
Franchise and Distribution
Insurance
Mergers and Acquisitions

INDUSTRIES

Cybersecurity
New Media, Media and Entertainment
Government Contractors
Consumer Products and Services
Emerging Companies: Venable Venture Services
Life Sciences
Nonprofit Organizations and Associations

BAR ADMISSIONS

District of Columbia
Virginia

Bobby Turnage is a partner with Venable's Corporate Practice Group, and has a background in the Internet and high-tech industries. He primarily represents and advises clients concerning:

- Technology and IP transactions;
- Licensing, distribution and outsourcing contracts;
- Strategic partnering and co-branding contracts;
- Data security and privacy matters; and
- General legal counseling.

Mr. Turnage has an in-depth understanding of the inner workings of successful business operations, and is experienced in working collaboratively with client executive teams to accomplish stated objectives in a manner that works best for the client.

Prior to joining Venable, Mr. Turnage served as Senior Vice President, General Counsel and Secretary for Network Solutions, LLC, a leading Web-presence services company. Having worked as both an executive and a lawyer embedded in a business, Mr. Turnage brings valuable experience that enables him to provide practical, business-focused legal advice on matters faced by businesses in their daily operations.

Mr. Turnage's prior legal experience includes work as a litigation associate in private practice, as well as serving as Associate General Counsel for VeriSign, Inc. (a high-tech Internet services company), and serving as a defense attorney and prosecutor in the U.S. Army Reserve JAG Corps.

HONORS

Recognized in the 2013 edition of *Legal 500* in categories of M&A: Middle-Market (sub-\$500m) and Technology: Data Protection and Privacy

ACTIVITIES

During his time in the military, Mr. Turnage received several awards, including the Meritorious Service Medal; Army Commendation Medal (1OLC); Army Achievement Medal (1OLC); Leatherneck Dress Blues Award (USMC); and Navy League Outstanding Marine Corps Recruit Award (USMC).

EDUCATION

J.D., University of Mississippi
School of Law, 1992

Editorial Board, *Mississippi Law Journal*

Moot Court Board

Who's Who Among Students in
American Universities and
Colleges

B.S., Business, Virginia
Commonwealth University, 1989

Omicron Delta Kappa National
Leadership Honor Society

MEMBERSHIPS

Past Chair, General Counsel
Committee of the Northern
Virginia Technology Council

Past Member, Association of
Corporate Counsel

Past Board Member, Home Care
Delivered, Inc.

PUBLICATIONS

- March 17, 2014, Cybersecurity Assessments – Using the Tool Well, Cybersecurity Alert

SPEAKING ENGAGEMENTS

- December 10, 2015, A Breach Can Happen to You (or Already Has, and You Just Don't Know It Yet): How Nonprofits Can Best Manage Cybersecurity Risk
- November 12, 2015, "Nonprofit Privacy and Cybersecurity Risks: Not Just for Home Depot Anymore" at the Third Annual Nonprofit Executive Summit: Bringing Nonprofit Leaders Together to Discuss Legal, Finance, Tax, and Operational Issues Impacting the Sector
- November 6, 2015, "An Anatomy of a Cyber-Security Crisis" for The Conference Board
- October 21, 2015, "Cyber Security: The Risk to Associations" at the Finance & Administration Roundtable (FAR) October Luncheon
- April 22, 2015, "Cyber Security - Know the Risks and Protect Your Company" at the AHT Cyber Security Summit
- February 27, 2015, "Cybersecurity: Safely Doing Business in the Digital World" at the Wharton Executive MBA Entrepreneurial Gala at the University of Pennsylvania Wharton School
- October 30, 2014, "Valuing, Mitigating & Insuring Your Cybersecurity Risk" at CyberMaryland 2014
- September 22, 2014, "Big Data & Analytics: Opportunities and Challenges" at LEAD Virginia's Conversations with Leaders Conference
- September 24, 2013, "Emerging Cyber Threats and Breach Response from the Boardroom to the Data Room" for ACG National Capital
- April 17, 2013, Government Contracts Symposium
- March 21, 2013, "Managing Cybersecurity Risks for Financial Institutions" for ALI CLE
- November 15, 2012, "Managing and Responding to Data Security Breaches: Minimizing Reputational, Business and Legal Costs" at ACI's 2nd National Summit on Industrial & National Security Compliance
- November 5, 2012, "Fundamentals of Intellectual Property" for the USDA Commercialization Assistance Training Program (CATP)
- October 18, 2012, "Getting the Most Value from Legal Counsel," Larta Institute
- October 11, 2012 - October 12, 2012, NetDiligence Cyber Risk & Privacy Liability Forum
- September 30, 2012 - October 3, 2012, Association of Corporate Counsel (ACC) 2012 Annual Meeting
- July 12, 2012, "Expanding Privacy Rights" for the Life Sciences IT Coalition
- June 20, 2012, Getting Deals Done in a Challenging Environment
- June 19, 2012, "ACC June Webcast: Understanding Cyber-Insurance and Managing Your Risk," hosted by the Association of Corporate Counsel
- June 18, 2012, Getting Deals Done in a Challenging Environment, Venable Business Division Presentation from Tysons Corner, VA
- March 29, 2012, "The True Costs of Cyber Security: Getting Past the Myths and Misconceptions" at the Center Club
- October 5, 2011, "Building Your Brand Through Social Media" at PLI Corporate Counsel Institute 2011
- April 1, 2011, "In-House Counsel in the Cross-Hairs – How to Avoid Pitfalls Presented by New and Changing Federal Laws and Regulations," NVTC General Counsel Committee



Dan Koslofsky, Esq.

Chief Privacy & Compliance Officer
AARP

Dan currently serves as the Chief Privacy & Compliance Officer at AARP where he is responsible for ensuring compliance with an array of federal, state, local and industry regulations governing data privacy & security, telemarketing, email marketing, social media advertising, mobile marketing and behavioral advertising. Dan previously served in several legal services positions including Director of the Senior Citizen Law Project at New Hampshire Legal Assistance and Senior Staff

Attorney in the Consumer Fraud and Financial Abuse Unit at Legal Counsel for the Elderly. He litigated numerous consumer protection matters involving unfair and deceptive acts and practices, predatory lending, credit reporting abuses and financial exploitation. Dan began his legal career as a staff attorney at the New Hampshire Public Defender representing clients facing misdemeanor and felony criminal charges.



Additional Information



AUTHORS

Atitaya C. Rok
Jeffrey S. Tenenbaum

RELATED PRACTICES

Tax-Exempt Organizations

RELATED INDUSTRIES

Nonprofit Organizations
and Associations
Tax and Employee Benefits
for Nonprofits

ARCHIVES

2015	2011	2007
2014	2010	2006
2013	2009	2005
2012	2008	

ARTICLES

December 2015

THE NEW IRS PROPOSAL ON SUBSTANTIATION REQUIREMENTS FOR CHARITABLE CONTRIBUTIONS: WHAT COULD IT MEAN FOR NONPROFITS?

Under a new **Internal Revenue Service (IRS) proposed rule**, tax-exempt 501(c)(3) nonprofit organizations (and other tax-exempt entities able to receive charitable contributions) would have the option of filing a new informational return with the IRS by February 28 each year to substantiate donor contributions of \$250 or more (Donee Reporting). (Note that all references to "nonprofit organizations" and "charities" in this article refer only to these particular organizations, not to all nonprofits.) Donee Reporting would require nonprofit organizations to collect donors' names, addresses and Social Security numbers, and then provide them to the IRS.

Currently, in order for donors to claim charitable income tax deductions for contributions of \$250 or more on their tax returns, they must obtain contemporaneous written acknowledgments (CWA) from the nonprofit receiving the donation that include the following information: (1) the name of the organization; (2) the amount of the cash donation or a description (but not the value) of the non-cash property donated; (3) a statement of whether the nonprofit organization provided any goods or services as a result of the contribution and, if so, a description and good faith estimate of the value of such goods or services; and (4) a statement that the only benefit received was an intangible religious benefit, if that was the case. See **IRS Publication 1771**.

Donee Reporting under the IRS proposed rule would provide nonprofits with an alternative to the CWA by creating a new process through which they report contributions of \$250 or more directly to the IRS. Donee Reporting is intended to make it easier for donors to substantiate their donations in order to claim a charitable deduction, since each contribution would be associated with a donor Social Security number. However, this would require donors to provide nonprofits with their Social Security numbers, which raises significant privacy and identity theft concerns.

Critics of the IRS proposed rule are concerned with the potential increase in the number of identity thefts as a result of Donee Reporting, noting that hackers have accessed individuals' personal information maintained by large for-profit companies and federal government agencies that presumably have the resources to combat such breaches. Requesting donors' Social Security numbers means that nonprofits will need to invest limited resources in increased data security in order to collect, store and protect donors' personal information, which could prove very costly, particularly for smaller organizations. Moreover, critics have said that the IRS proposed rule makes it easier for fraudulent actors to prey on donors. A fraudulent solicitor could simply tell a prospective donor that the charity cannot accept their contribution unless the donor provides his/her Social Security number; unfortunately, some donors will end up falling victim to these identity thieves. The apprehension about these privacy and identity theft concerns could result in reduced contributions to charities.

Critics of the IRS proposed rule also have said that donors might think twice about making donations to a charity if they are required to disclose their Social Security numbers, claiming that Donee Reporting would put donors in the untenable position of choosing between supporting charities or sharing their sensitive, personal information. The current CWA process, **according to the IRS**, "works effectively, with minimal burden on donors and donees, and the Treasury and the IRS have received few requests... to implement a donee reporting system." Critics have concluded that change seems unnecessary when the current system is working just fine, particularly if the change creates problems for both charitable organizations and donors that do not currently exist.

For further information, contact the authors at acrok@Venable.com or jstenenbaum@Venable.com.

AUTHORS

Armand J. (A.J.) Zottola
Morgan E. Brubaker
Jeffrey S. Tenenbaum

RELATED PRACTICES

Technology Transactions
and Outsourcing

RELATED INDUSTRIES

Nonprofit Organizations
and Associations

ARCHIVES

2015	2011	2007
2014	2010	2006
2013	2009	2005
2012	2008	

ARTICLES

May 15, 2015

WHAT TO DO WHEN YOUR NONPROFIT BECOMES THE TARGET OF A PHISHING SCAM

"Phishing" is a term used generally to describe various electronic attempts by a fraudulent actor to masquerade as a legitimate entity in order to acquire sensitive information from an individual, such as a user name, password, credit card number, or Social Security number. While phishing scams often target individuals, nonprofits can likewise suffer. During the first half of 2014, there were 6,271 phishing attacks that targeted the ".dot-org" Internet domain name often used by nonprofits, according to a study by the Anti-Phishing Working Group, a consortium of industry groups and international organizations. Popular trademarks or trade names of nonprofits often are used to attract individuals to donate money or provide personal information by serving as means to create a false online identity. This misuse of a trademark or trade name can damage, among other things, a nonprofit's valuable reputation and goodwill. Phishing scams also can harm donor, member, supporter, sponsor, grantor, employee, and other relationships and can cause significant economic harm to a nonprofit.

The typical nonprofit phishing scam involves the following: An individual receives an e-mail, which appears to originate from a well-known nonprofit. The message describes an urgent reason such individual should donate money or provide information to the nonprofit for charitable purposes, either by clicking on a link embedded in the message or by replying to the message with the requested information. The provided link and/or e-mail address URL appears to be associated legitimately with the well-known nonprofit, but in a "phishing" scam, the link or address is actually controlled by the fraudulent actor/scammer. The individual mistakenly gives his or her donation or surrenders his or her own data by mistakenly providing the information requested to the fraudulent actor/scammer.

To minimize the damage, there are several steps that a nonprofit should consider taking immediately after discovering that it has become involved in a phishing scam, both to protect the nonprofit's brand and to protect individuals, who can be a nonprofit's donors, members, supporters, partners, or even employees, from further damage:

Identify the Scam: Phishing scams can initially be hard to identify. The act of forgery can be very convincing and sophisticated. However, recognizing a phishing attempt can allow a nonprofit to respond more quickly and prevent further damage. Hallmarks of common phishing scams include unauthorized use of a nonprofit's name, trademark, or content (or confusingly similar versions thereof); use of an unofficial, unaffiliated, or unauthorized contact ("From") address that closely resembles the addresses of a well-known nonprofit name; an email or other communication indicating that urgent action or an urgent response is required; a generic greeting to help introduce the request for a response; and other unfamiliar details in a communication that prompts an individual to want to respond to such request.

Gather Information: If a nonprofit discovers a phishing scam that makes unauthorized use of its name, trademarks, or web content, the nonprofit should first try to determine the scope of the phishing attempt and the type of information sought by the fraudulent actor/scammer. Determining the nature of the information sought will help later with responsive communications to thwart the phishing attempt and warn individuals against the submission of donations or information. In addition, the nonprofit should try to learn the extent to which a phishing scam uses its name, trademark, or content.

Form a Response Team: Designate a team and/or point person with primary responsibility for dealing with the phishing scam and for collecting necessary information. When possible, collect and maintain records or correspondence related to the fraudulent activity. Such records or correspondence not only can assist with a possible legal response; they also can aid notification and reporting efforts regarding the incident.

Consider Providing an Email Address for Follow-up: If necessary, consider designating an email address or other contact information that affected individuals can use to contact the entangled nonprofit regarding a phishing scam involving its name, trademark, or content.

Provide Notice: Post a conspicuous notice on the nonprofit's website (or send a communication providing the notification or a link to the notification). The notification should be specific enough to alert potential victims of the fraudulent activity and include steps to help the affected individuals avoid falling victim to the scam. Depending on the type and severity of the scam, consider sending an email to alert affected individuals (if known) of the fraudulent activity. Such a communication also could remind individuals to take proactive measures to protect their identity and information, such as alerting credit bureaus and/or seeking identity protection services, especially if information was inadvertently provided to the fraudulent actor/scammer.

Report the Scam to Law Enforcement: Phishing can not only constitute a violation of proprietary rights, it also can be a crime. Report the fraudulent activity to applicable law enforcement authorities and/or to one or more state attorney general offices. Reporting procedures vary based on location and jurisdiction. Confirm instructions for reporting by reviewing the applicable state attorney(s) general website(s). The U.S. Federal Trade Commission also offers a complaint notification process through its website. With such reporting, it is important to provide as much detail as possible. It therefore may be necessary to provide copies of relevant communications and other documentation regarding the phishing scam when possible.

Notify Nonprofit Employees: When employees are affected or involved, or when employees can assist with alerting affected third parties, consider providing notice to relevant personnel of the fraudulent activity and how to avoid it. Such a communication may include steps to alert other external individuals of the phishing event or provide contact information and other relevant information if a nonprofit's own employees, donors, members, supporters, or others have fallen victim to the phishing scam.

Notify the Applicable Domain Name Registrar: Many phishing scams operate by creating a domain name that makes confusingly similar use of a well-known trade name or trademark, either to serve as a response address or to operate a fraudulent website. Reputable domain name registrars offer takedown processes to assist with shutting down a fraudulent domain. Complete a search of the fraudulent domain name through a whois.com database to identify the registrar of the domain as well as the name of the person or corporation that has registered the domain. Use this information to contact the registrar and report the fraudulent activity.

Revisit the Nonprofit's Trademark Portfolio: Many phishing scams can be prevented by maintaining a robust trademark, domain name, or account registration or prosecution practice. Consider registering important trademarks, domain names, and account identifiers that third parties might naturally associate with the nonprofit. Additionally, ensure that the nonprofit's trademarks are registered in important geographic areas, such as the United States, European Union, and other key countries where the nonprofit is or plans to be located, operate, or provide services. Moreover, maintain a robust brand protection and maintenance program in order to better protect and authenticate the nonprofit's online identity.

Involve Attorneys Early: Addressing a phishing scam requires prompt attention. It is helpful to involve attorneys early in the process to assist with protection, notification, and other remedial or enforcement efforts. Attorneys can provide guidance on the steps listed above and help a nonprofit assess whether further legal action against the fraudulent actor is advisable. Attorneys also can assist with takedown requests and administrative actions, such as actions available under the Uniform Domain-Name Dispute-Resolution Policy (UDRP) or the Anti-cybersquatting Consumer Protection Act (ACPA).

CYBERSECURITY ALERT

March 17, 2014

CYBERSECURITY ASSESSMENTS – USING THE TOOL WELL

This alert was also published by Inside Cybersecurity on March 21, 2014.

AUTHORS

Jamie Barnett, Rear
Admiral (Ret.)
David M. DeSalle
Anthony J. Rosso
Bobby N. Turnage, Jr.
Brian M. Zimmet

RELATED INDUSTRIES

Cybersecurity

ARCHIVES

2015	2011	2007
2014	2010	2006
2013	2009	2005
2012	2008	

Are you considering a cybersecurity assessment? If you heard Venable's presentation, "**New Cybersecurity Framework Released: What You Need to Know**," you might be.

The Framework places increased emphasis on organizational cybersecurity risk management. NIST states in the Framework that "organizations responsible for Critical Infrastructure need to have a consistent and iterative approach to identifying, assessing, and managing cybersecurity risk." Sectors not considered to be Critical Infrastructure are likely subject to similar expectations. For instance, the SEC has indicated that "risk oversight is a core competence" of the boards of publicly held companies, and there can be little question today that cyber risk is an elemental component of many businesses' risk portfolios.

As a result, your organization should consider whether to perform reviews and assessments of your cybersecurity programs in the context of NIST's recommended risk management methodology. You may also want to determine your readiness to "adopt" the Framework or, because of current events and a growing awareness of increasingly sophisticated and widespread cybersecurity threats, perform vulnerability assessments or other penetration tests.

Why Consider an Assessment?

These assessments not only identify areas of improvement in any given cybersecurity program, but also confirm that other program components are successfully functioning as intended. These assessments can be extremely valuable in terms of risk management and could be used in litigation or enforcement actions to show that the cybersecurity program in question was "commercially reasonable" and managed in a reasonable manner. Additionally, corporate boards, as a matter of good corporate governance practice and fulfillment of their fiduciary duties, should consider obtaining periodic updates and assessments of their data security profile in light of the potential risks of IP loss, business interruption, harm to business reputation, and other adverse consequences arising from a data breach.

What Does My Organization Need to Know?

Evaluating your security program can help you identify areas where you can better protect your organization as well as your clients and customers, and there are some important considerations to keep in mind prior to embarking on such an endeavor.

- **First, consider engaging a third-party security consultant that specializes in cyber security.**
The typical in-house IT department has many responsibilities related to the day-to-day operations of the business, whereas a third-party specialist makes it their business to know the latest and greatest threats as well as the most effective tools for defending against those threats. Bringing in a third-party specialist will both allow your IT department to continue focusing on the important work of keeping your business running and better ensure an objective analysis of organizational cyber risk.
- **Second, we urge you to consider having outside counsel retain your selected consultant, with draft reports being provided directly to the law firm.**
This provides your lawyers with the ability to review draft findings and conclusions. Your organization likely will not know in advance what these third-party assessments will reveal, and having that information protected by attorney-client privilege could become very important, depending upon what is discovered in the assessment. Additionally, allowing your outside counsel the opportunity to provide input on the findings and conclusions in such a report while it is still in draft form enables them to ensure that a report does not contain speculative or inflammatory statements or conclusions.

that are not necessary but that could be harmful if ever disclosed.

Venable's **Cybersecurity Team** has considerable experience with these types of assessments and has partnered with numerous IT consultant firms to provide both targeted and full-service cybersecurity reviews. Please feel free to contact us with any questions about protecting your organization while ensuring that its cyber risk is effectively and reasonably managed in light of the NIST Cybersecurity Framework.

AUTHORS

Jeffrey S. Tenenbaum
Armand J. (A.J.) Zottola

RELATED PRACTICES

Technology Transactions
and Outsourcing

RELATED INDUSTRIES

Nonprofit Organizations
and Associations

ARCHIVES

2015	2011	2007
2014	2010	2006
2013	2009	2005
2012	2008	

ARTICLES

October 5, 2010

THE TOP FIVE TECHNOLOGY LEGAL TRAPS FOR THE UNWARY ASSOCIATION

**This article appeared in the Dec. 2010 issue of Associations Now magazine, published by the American Society of Association Executives.*

New technology brings new opportunities for associations to leverage new communication devices, systems and networks. However, incorporating new technology into an association's operations or its external communication, membership or marketing efforts without first considering the potential legal risks can expose the unwary association to potential liability. In order to keep from falling into these legal traps, associations must first be aware of them, and then take proactive steps to avoid them. The following is a non-exhaustive list of some of the top legal traps that can snare an association using new today's new technology.

#1 - The Online/Electronic Contract Trap

Electronic contracts are generally enforceable to the same extent as paper contracts. The Uniform Electronic Transaction Act ("UETA"), which provides that an electronic signature satisfies any legal requirement for a signature on a contract, has been adopted by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands. Federal legislation, called the Electronic Signatures in Global and National Commerce Act ("ESIGN"), also endorses the use of electronic contracts in interstate commerce. However, even if electronic contracts are generally enforceable, associations that enter into contracts online still have to be mindful of contractual requirements such as showing knowledge of, and assent to, the contract by both parties. Additionally, electronic contracting requires consideration of unique issues, such as maintaining a level of security and authentication adequate to verify reasonably the identity of the parties entering the contract.

Once an association begins to use electronic contracts to make its content, resources and tools available online, the association also should consider setting forth the specific terms and conditions governing the use of such content, resources and tools. These terms and conditions should address common issues such as end-user conduct, permissible use of intellectual property, notice of proprietary rights, disclaimers, limits on liability, the association's role or responsibilities, and other relevant legal issues related to the particular conduct. With respect to posting such terms and conditions, the association should not rely solely on mere notice. Maintaining an enforceable legal document should be accomplished by providing both notice and an opportunity for the end user or other contracting party to review the applicable terms and conditions and subsequently provide some manifestation of assent to the applicable terms and conditions. Recent court decisions suggest that mere notice without a manifestation of assent is not sufficient to make the terms and conditions enforceable. An association also should implement a process by which to document and maintain a record for the online formation and "execution" of an electronic agreement in the same general manner that an association may keep records of the execution of its paper contracts, pursuant to its records and information management policy.

#2 - The Social Media Trap

Associations that operate interactive websites, listserves, blogs, or other interactive online forums, or that utilize online social networks, may encounter user postings with content that infringes or violates the rights of others. For example, with respect to copyrightable works owned by third parties, such as articles written by others, if the posting was made by an association employee, the association may be vicariously liable for copyright infringement if the posting was done without the permission of the copyright owner. If the posting was done by a third party (such as an association member), an association could become liable if it contributes to the posting of the infringing content or alters the material so as to contribute to its content, or if it knew or should have known of the infringement and did not take prompt corrective action. The safe harbor provision of the federal Digital Millennium Copyright

Act ("DMCA") may help shield an association from liability for third-party postings that contain infringing material so long as the organization itself maintains a neutral role, *i.e.*, the infringing material is transmitted at the direction of someone else, is carried out through an automatic process, is not sent to recipients specifically selected by the hosting company, and is transmitted without modification. The federal Communications Decency Act ("CDA") also provides some protection from defamation and other tort liability for postings by third parties, so long as the association does not become the "publisher" of the content. Note that the CDA does not provide protection from antitrust liability or liability for copyright or trademark infringement.

An association should post terms and conditions that govern the behavior of third-party posters as well as the association's own employees, and that clearly identify the type of acceptable content that may be posted to the website or other interactive online forum operated by the association. In addition, associations should maintain a policy governing social media use by association employees, making clear both what is encouraged and what is prohibited, restricted or otherwise subject to regulation by the association.

Social media or networking sites also make it easier for someone to masquerade as another person or entity. For example, in *LaRussa v. Twitter, Inc.*, Major League Baseball manager Tony LaRussa sued Twitter after discovering that someone both created an account using his name (www.twitter.com/TonyLaRussa) and posted negative "tweets" about him underneath his name and photo. After contacting Twitter about the account and receiving no response, LaRussa sued Twitter for trademark infringement as well as cybersquatting and misappropriation of his name. Although the suit was later voluntarily dismissed, it provided an example of both the need to monitor and enforce an association's online identity and the risk that can arise from not establishing and identifying for the public an association's official online presence. This is especially critical when an association plans to permit others, even affiliated entities such as state and local chapters, to use the association's name online. An association should declare which sites are its own and provide rules for when someone else is using the association's name or trademark outside of the association's official site(s).

#3 - The Trademark Trap

It is easy to misuse third-party trademarks in electronic environments. As a general rule, an association should only use a third party's trademark with permission. In addition, an association should remain vigilant with respect to protecting its own trademarks. Associations should monitor for impermissible use of the association's name or trademarks in or as keyword search terms, user account names, or as the primary variables in unauthorized search engine optimization efforts. To protect against trademark infringement via online advertising or online social networks, associations should consider reserving their own trademarks as user account names and/or as online search keywords with online social networks, ad networks, search engines, and other interactive communities in order to claim rights in the character string equal to an association's full or most recognizable name (s). Associations also should notify and communicate with the appropriate search engine operators or online advertisers if they believe that their trademarks are being improperly used. Associations should make it an express policy to prohibit use by third parties of its name or trademarks as an account name or avatar (*i.e.*, a user or account holder's representation of itself, or the alter ego whether in the form of an image, symbol, icon, logo, username, or text string). Associations should periodically search and enforce such a rule in order to uncover instances when an association's trademark rights are being infringed or misused.

Domain names remain another area where trademark rights can be easily trampled. Associations likely want domain names that are equivalent or similar to their organization's name. As such, associations must remain diligent in their efforts to protect their trademark rights in connection with certain domain name reservation or registration practices. Although registrars now recognize the protection and enforcement of trademark rights in their domain name registration practices, new forms of cybersquatting consistently arise in connection with the increasing number of available top-level domains for domain name registration, such as country- or business-specific domains. For example, "front runners" are domain prospectors who register names immediately after potential brand owners have filed trademark registration applications with the U.S. Patent and Trademark Office. This has the effect of requiring the potential brand owner to purchase the domain name from the domain prospector. To protect against "front-running," associations should consider simultaneously registering for a domain name(s) corresponding to the trademark that is the subject of a new application. Associations also must remain aware of cybersquatters that engage in "drop-catching." In such instances, cybersquatters wait for a registration for a domain name to expire and then "drop-catch" (immediately register the domain name). Cybersquatters profit by building traffic off of the prior registrants. This is especially

true of domains that contain trademarks. Associations can avoid “drop-catching” by being proactive in their efforts to renew their domain names.

#4 - The New Technology Trap

When a new technology gains widespread use and acceptance, it still remains important for an association that may be utilizing the technology for the first time to be aware of the related requirements and potential risks associated with the new technology. This is true even if the association is not one of the early adopters of the technology. For example, more and more associations are conducting business transactions (such as membership dues payments, conference registration fees, and publication sales) and accepting payment through their websites. Associations that utilize credit and debit cards to process payment transactions should ensure that their efforts to protect consumer account information comply with PCI Data Security Standards (“PCI DSS”). PCI DSS is a set of 12 security standards created by the credit card industry that are intended to help organizations protect customer account information from theft and misuse. The standards focus on security management, as well as policies, procedures and protective measures for safeguarding customer account data. Although there are no federal or state laws that mandate compliance with all 12 PCI standards, several states, including Minnesota, have recently enacted statutory requirements similar to PCI DSS. The Minnesota law prohibits merchants from storing sensitive authentication data after payment cards are authorized. As a consequence, associations that process payment card data should validate the association’s data security, handling and storage processes and take proactive steps to ensure their compliance with PCI DSS. On many occasions, an association may need to implement and pay for the necessary security programs and measures required to remain in compliance with PCI DSS. Although such PCI compliance may be costly, in the long run, secure payment systems will help associations to preserve member/customer loyalty and brand value.

Associations also must protect against the risks that accompany employee use of employer-issued mobile communication devices. More and more associations permit use of, or even provide their employers with, mobile devices to facilitate their work. As the capacity and sensitivity of data that mobile communication devices can hold continues to expand, employers should make every effort to protect the information managed or stored through such devices in the same manner that the association manages the information on its own internal computer network. For example, the use of third-party applications on mobile communication devices is now a prevailing norm (e.g. ringtones, games, etc.). As a result, the risk of malware for mobile devices continues to increase (e.g., there were some 300 to 500 known versions of mobile malware in 2008). Although most mobile operating system vendors require third-party applications to be tested for approval and certification, this often is not enough protection to avoid viruses or other forms of malware. Associations should therefore work to protect both their own internal computer networks and systems and their external networks and mobile devices by purchasing anti-malware programs and measures that address both kinds of networks. Additionally, employers should implement proactive processes to protect information on employee mobile devices that are lost or stolen. Beyond password features, associations should invest in remote data deletion software that would allow an association to remotely delete sensitive information on lost or stolen devices.

#5 - The Employee Use Trap

As more and more information is stored electronically and new technology makes it easier to access and disseminate information, trade secret protection becomes harder to manage and enforce. Trade secret owners therefore must take extra precautions for the use, handling and transmission of their valuable or proprietary information in digital form. Associations should implement policies directed specifically against disclosure that may occur online or through mobile communication devices. These policies should focus on restricting and controlling employee access to and disclosure of trade secrets through these newer forms of communication. For example, associations should prohibit employees from storing confidential information on unauthorized digital devices or posting confidential information on unaffiliated websites (e.g., social media sites, blogs, etc.). Additionally, associations should actively promote security compliance to their employees, and require that employees promptly report any security breaches. Finally, upon termination of employment, associations should require employees to delete any association information that has been stored on personal electronic devices.

In addition to remaining mindful of trade secrets in connection with mobile communication devices, the capabilities of remote access are increasingly expanding the traditional notion of the workplace. This expansion has ramifications on both controlling and monitoring employee conduct. According to the U.S. Supreme Court’s recent decision in *City of Ontario v. Quon*, employers can monitor employee text

messages on employer-issued mobile phones or pagers – if done in the appropriate manner. In that case, the City reviewed an employee's text messages (and those of two fellow co-workers) after the employee exceeded his texting limit. In conducting its review, the City discovered many of the employee's text messages to be personal and sexually explicit. The Court held that the search did not violate the employee's Fourth Amendment rights to reasonable search and seizure. While *Quon* involved a government employer and thus posed different legal standards than most associations face, it serves as an important reminder that associations should consider adopting policies that explicitly address the ability to monitor employee conduct outside an association's own offices (e.g., on personal computers linked to the association's network and personal mobile communication devices linked to the association's email system) – and that specifically make clear to employees that they have no reasonable expectation of privacy when using these facilities. In addition to safeguarding confidential information and maintaining productivity, monitoring can be justified as necessary to help protect associations from vicarious liability for employee conduct. Courts have regularly held employers liable for their employees' inappropriate use of employer-provided mobile communication devices. For example, in *Ellender v. Neff Rental, Inc.*, an employer was held vicariously liable for the negligence of an employee who caused an accident in his personal vehicle while conducting business on his employer-provided cell phone. Therefore, to protect themselves from potential liability, associations should establish written policies that work to monitor and deter inappropriate use of association-related facilities both in and outside of the office.

* * * * *

Jeff Tenenbaum chairs Venable's Nonprofit Organizations Practice Group. A.J. Zottola is a partner at Venable in the Business and Technology Transaction Groups and focuses his practice on intellectual property, computer, Internet, new media, and technology law. For more information, please contact jstenenbaum@venable.com or ajzottola@venable.com, or 202-344-4000.

This article is not intended to provide legal advice or opinion and should not be relied on as such. Legal advice can only be provided in response to a specific fact situation.