# Medical Apps and Devices
## The Convergence of FDA, FTC, and State and Federal Regulation

**Barry H. Boise**
**T. Stephen Jenkins**

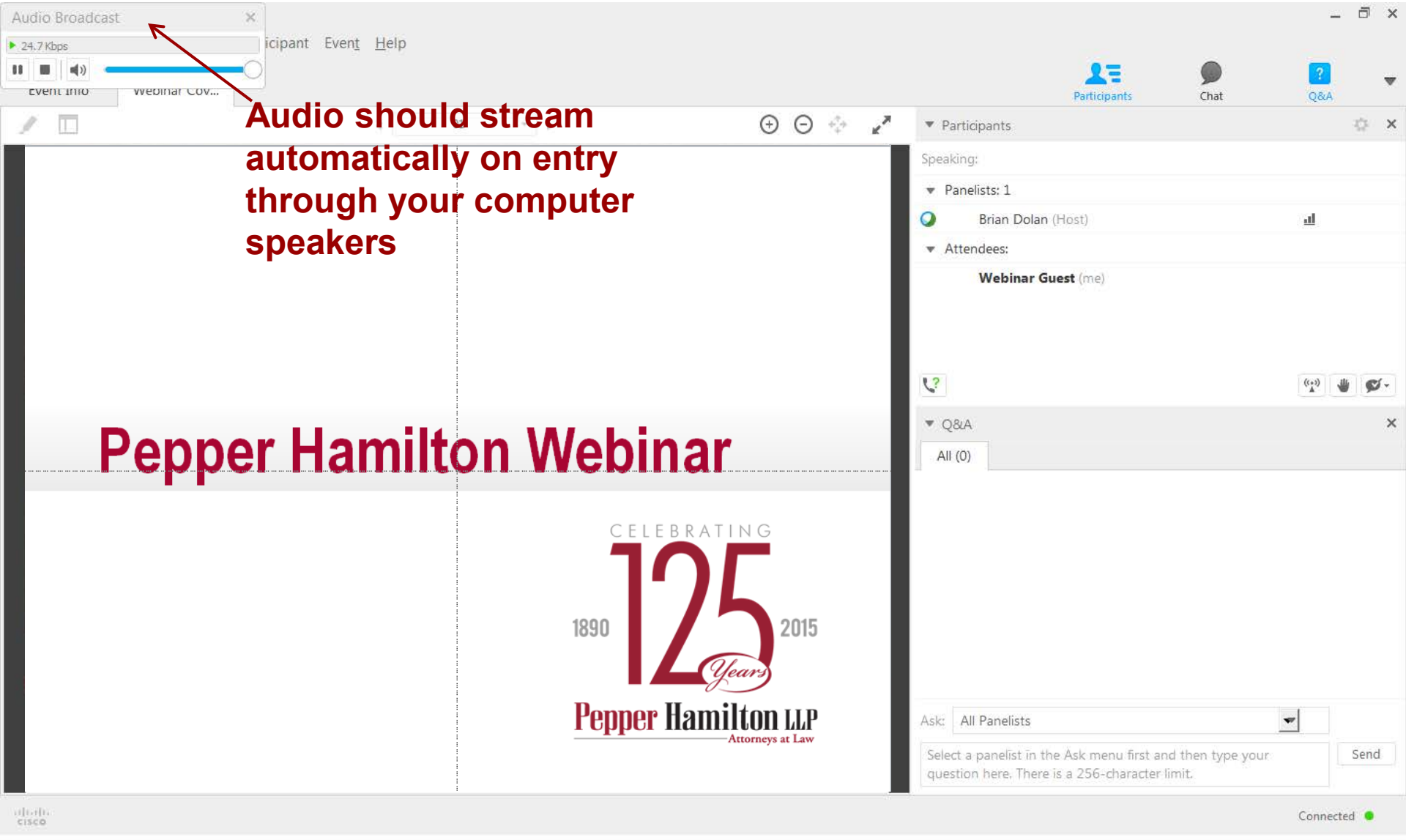
**Moderated by**
**Mark A. Kadzielski**

CELEBRATING 1890 125 Years 2015

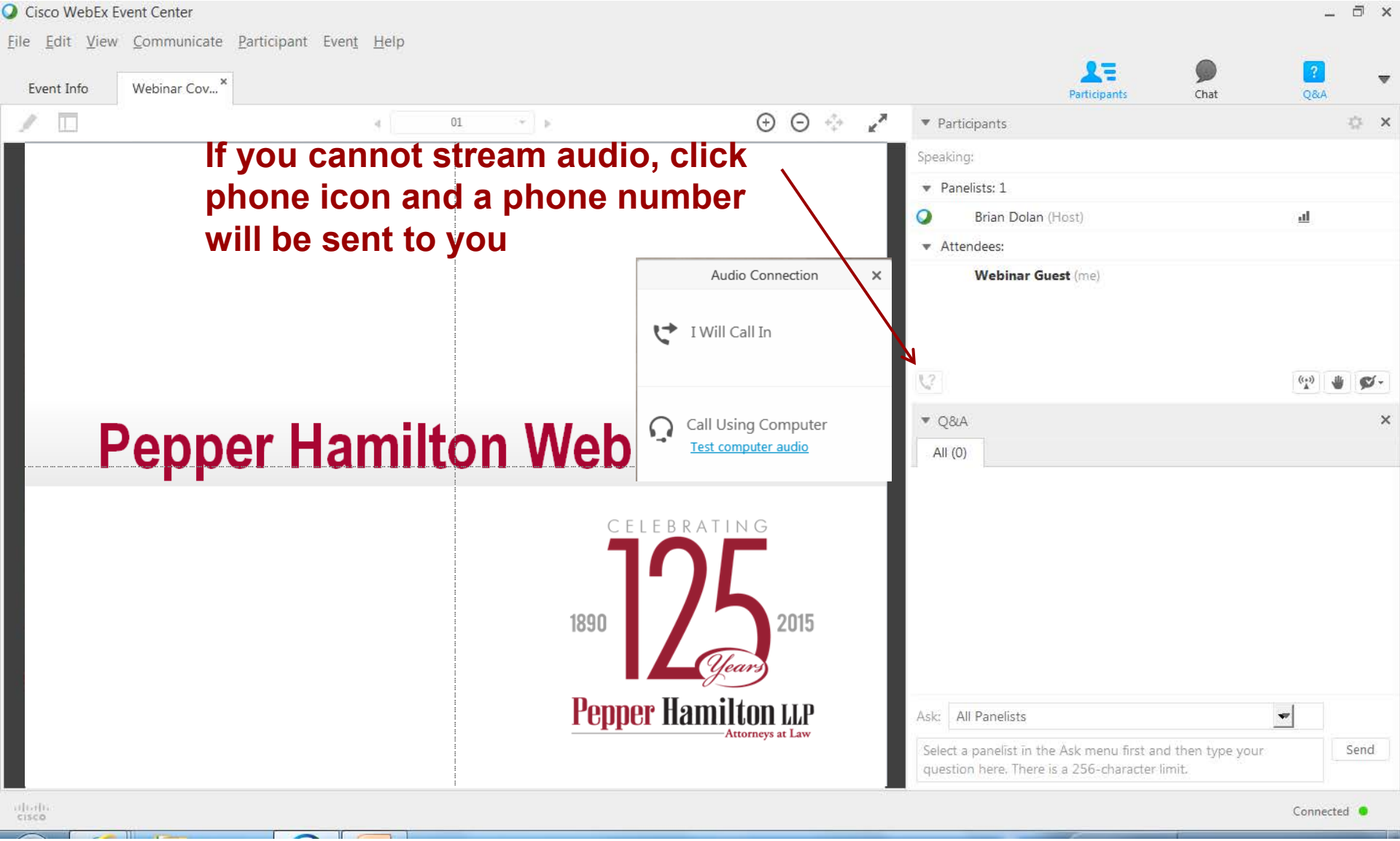
Pepper Hamilton LLP
Attorneys at Law

Health Care Services Webinar | December 17, 2015

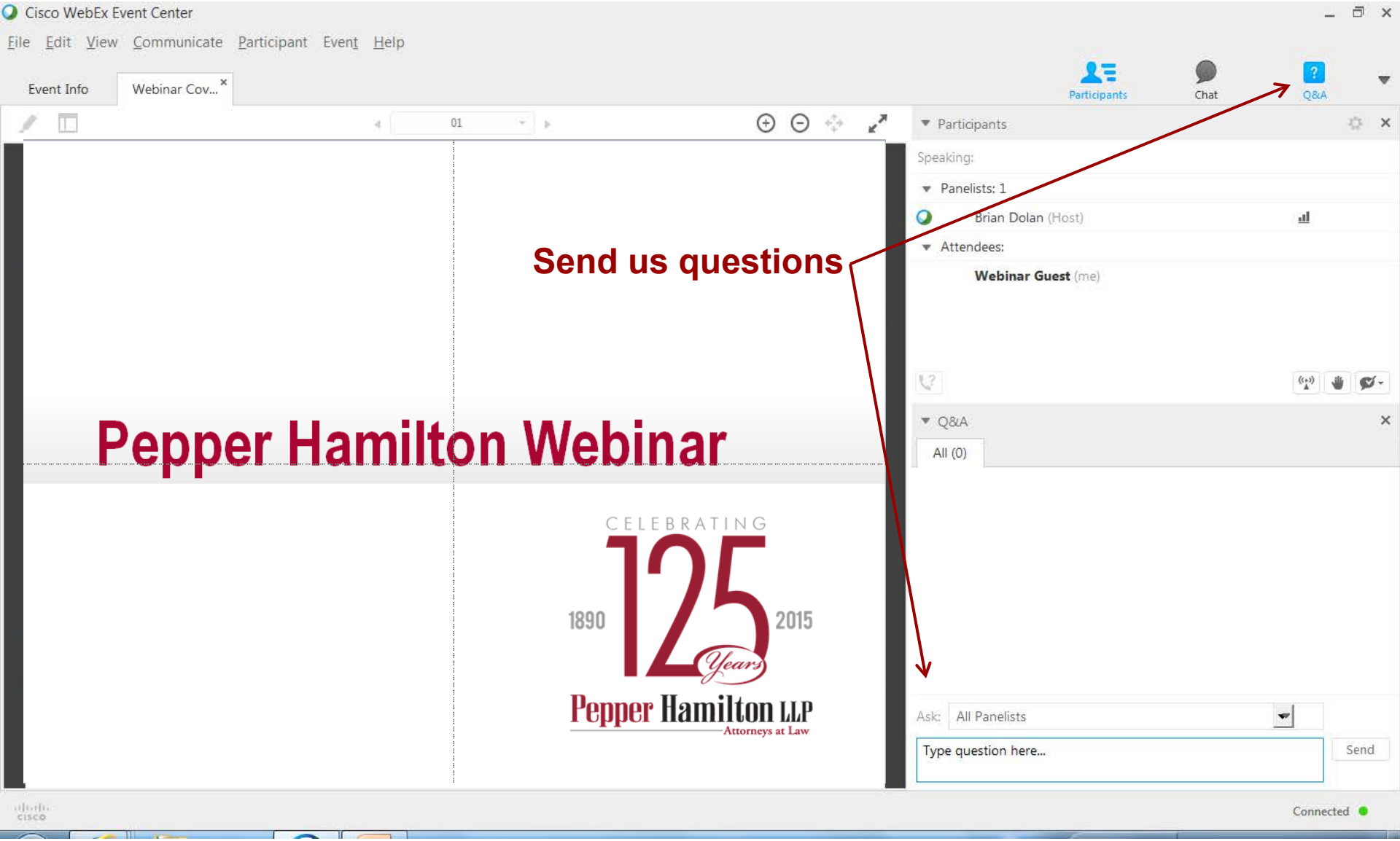
# Audio


Audio Broadcast
24.7 Kbps
Participant Event Help
Participants
Chat
Q&A
Audio should stream automatically on entry through your computer speakers
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Pepper Hamilton Webinar
CELEBRATING
1890 125 2015
Years
Pepper Hamilton LLP
Attorneys at Law
Ask: All Panelists
Select a panelist in the Ask menu first and then type your question here. There is a 256-character limit.
Send
Connected

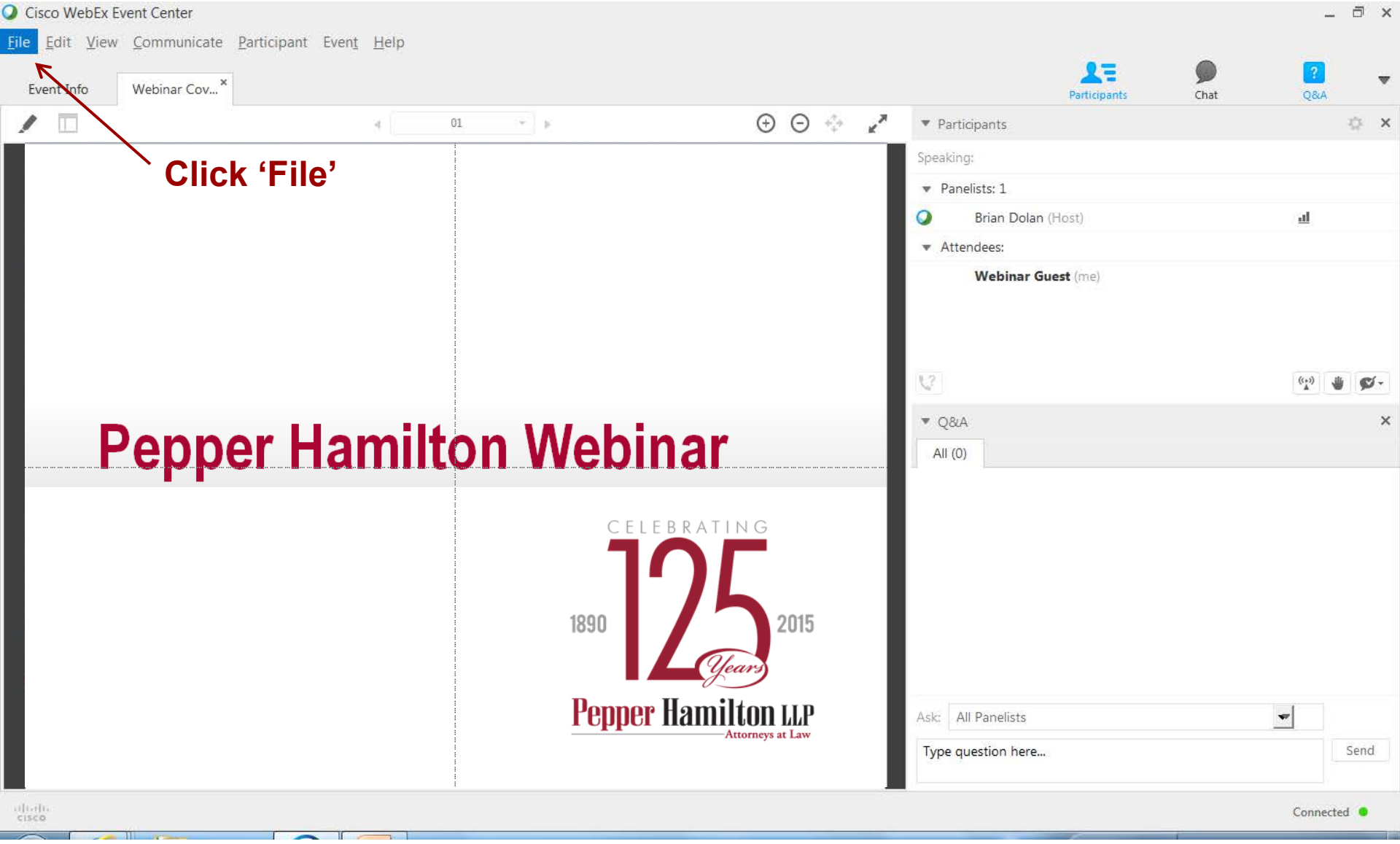
# Audio


Cisco WebEx Event Center
File Edit View Communicate Participant Event Help
Event Info
Webinar Cov...
Participants
Chat
Q&A
If you cannot stream audio, click phone icon and a phone number will be sent to you
Audio Connection
I Will Call In
Call Using Computer
Test computer audio
Pepper Hamilton Web
CELEBRATING
1890 125 2015
Years
Pepper Hamilton LLP
Attorneys at Law
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Ask: All Panelists
Select a panelist in the Ask menu first and then type your question here. There is a 256-character limit.
Send
Connected

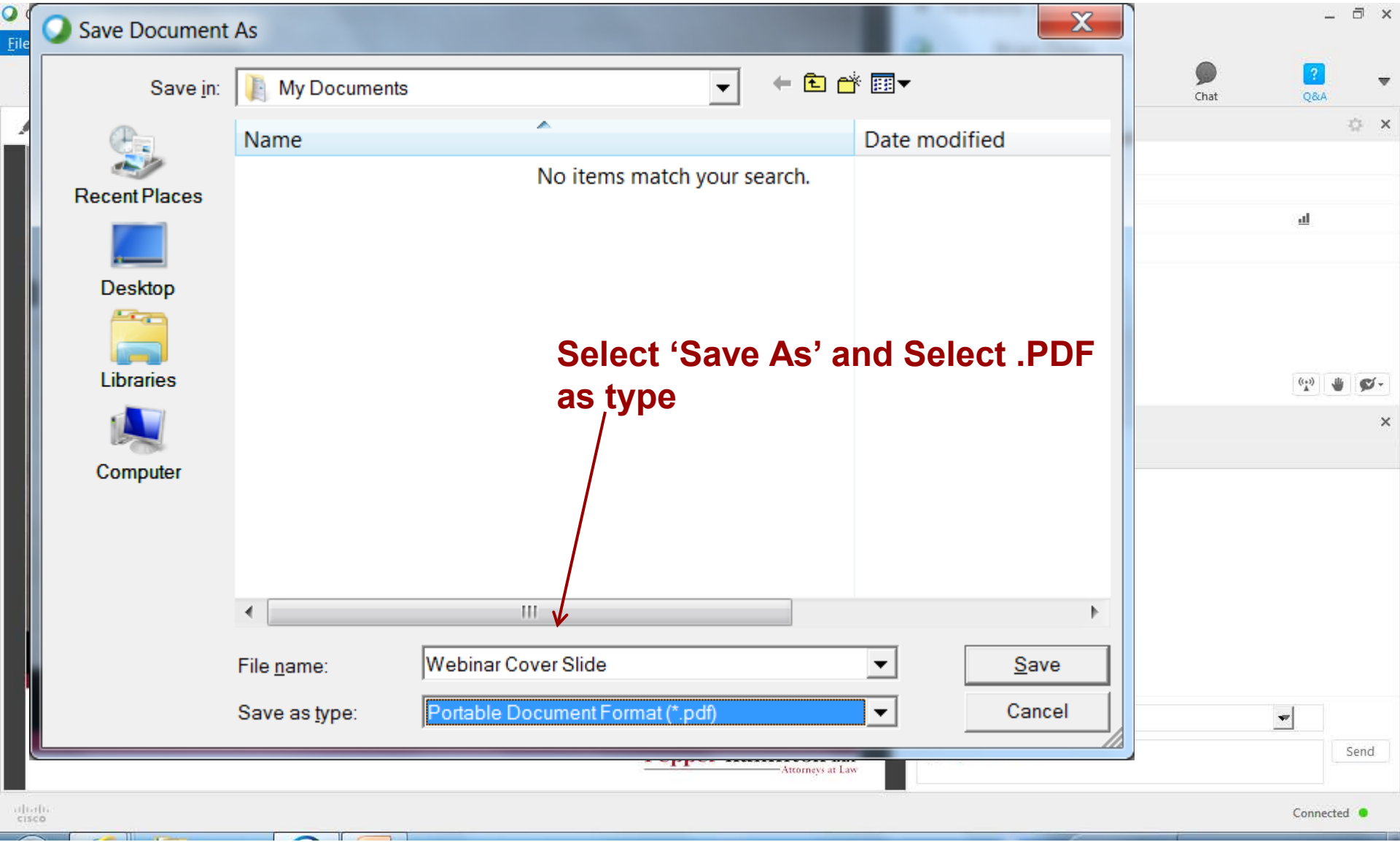
# Q&A


Cisco WebEx Event Center
File Edit View Communicate Participant Event Help
Event Info
Webinar Cov...
Participants
Chat
Q&A
Send us questions
Pepper Hamilton Webinar
CELEBRATING
1890 125 2015
Years
Pepper Hamilton LLP
Attorneys at Law
Participants
Speaking:
Panelists: 1
Brian Dolan (Host)
Attendees:
Webinar Guest (me)
Q&A
All (0)
Ask: All Panelists
Type question here...
Send
Connected

# Download PPT Slides



# Download PPT Slides



**CLE credit available in CA, NY, PA.**
**NJ CLE credit is available through reciprocity and VA CLE credit is pending.**

**Contact Brian Dolan at dolanb@pepperlaw.com for CLE form**

# Mark A. Kadzielski


## Partner and National Chair, Health Care Services

213.928.9820

kadzielskim@pepperlaw.com


- Represents hospitals, medical staffs, managed care enterprises, and institutional and individual health care providers throughout the United States
- Work includes government regulatory investigations, contracting issues, credentialing, peer review, licensing, medical staff bylaws, joint commission accreditation and Medicare certification
- Has prepared more than 200 sets of medical staff bylaws and has handled numerous peer review hearings and appeals, including litigation in many courts

# Barry H. Boise


## Partner and Vice Chair, Health Effects Litigation

215.981.4591

boiseb@pepperlaw.com

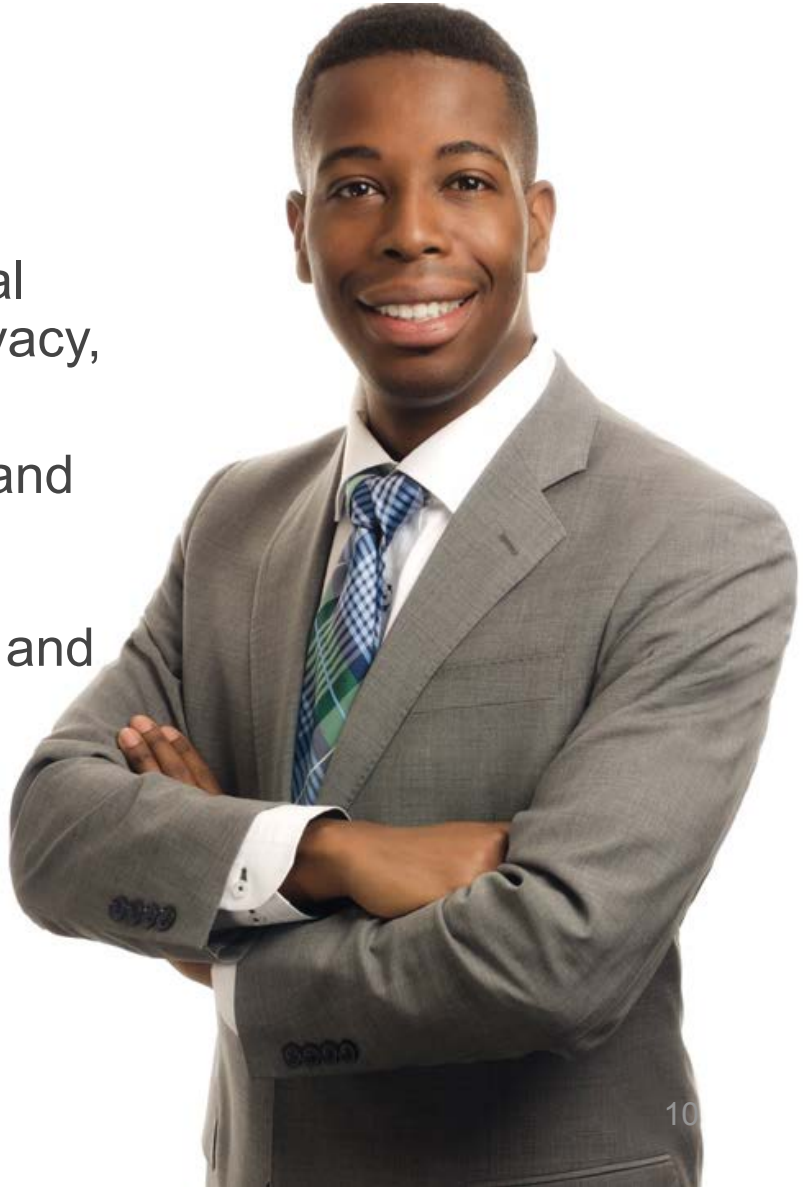

- Defends and counsels medical device, pharmaceutical, and life science companies concerning litigation and risk mitigation strategies concerning marketed products, investigational new drugs, new technologies, and payor relationships
- Represents companies in Attorney General investigations, litigation and resolution, including engagements involving multi-state consortiums and private plaintiff led litigation
- Member of Pepper's Health Care Service and Life Science Practices

# T. Stephen Jenkins

## Associate, Commercial Litigation

215.981.4743
jenkinst@pepperlaw.com

- Practice involves a range of commercial litigation and compliance, including privacy, antitrust, and unfair competition
- Member of Pepper's Privacy, Security and Data Protection practice, the Antitrust Section in the Commercial Litigation Practice Group, and the Non-Compete and Trade Secrets practices



# Mobile Medical Applications:

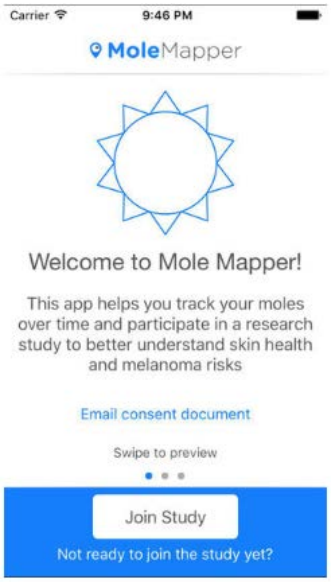
## Convergence of Privacy and Patient Safety

### Johns Hopkins researchers to use Apple Watch data to study epilepsy

EpiWatch app will help researchers better understand epilepsy, develop new methods for monitoring, managing the disorder

**Jania Matthews** / **October 15**


### Epilepsy.com Launches New iPhone App to Help People With Epilepsy Manage Seizures, Symptoms and Treatment




### Sage Bionetworks Launches Mole Mapper iPhone-app Enabled Research Study to Better Understand Melanoma

Patient-centered app-based study to quantitatively track moles and help detect early signs of malignant melanoma -- the deadliest form of skin cancer

OCTOBER 20, 2015 BY CHARLES MOORE

# Data Breach: Health Information

- The average cost of a data breach is estimated to be $3.8 million
  - Healthcare records have the highest cost per stolen record at an average of $363.
- PHI is worth up to 20 times more on black markets than financial information

# Crowded Regulatory Field




Federal Trade Commission
Protecting America's Consumers

ONC

FDA

U.S. Department of Health & Human Services
Office of Inspector General
OIG

Department of Commerce
United States of America

Department of Justice
Qui Pro Domina Justitia Sequitur

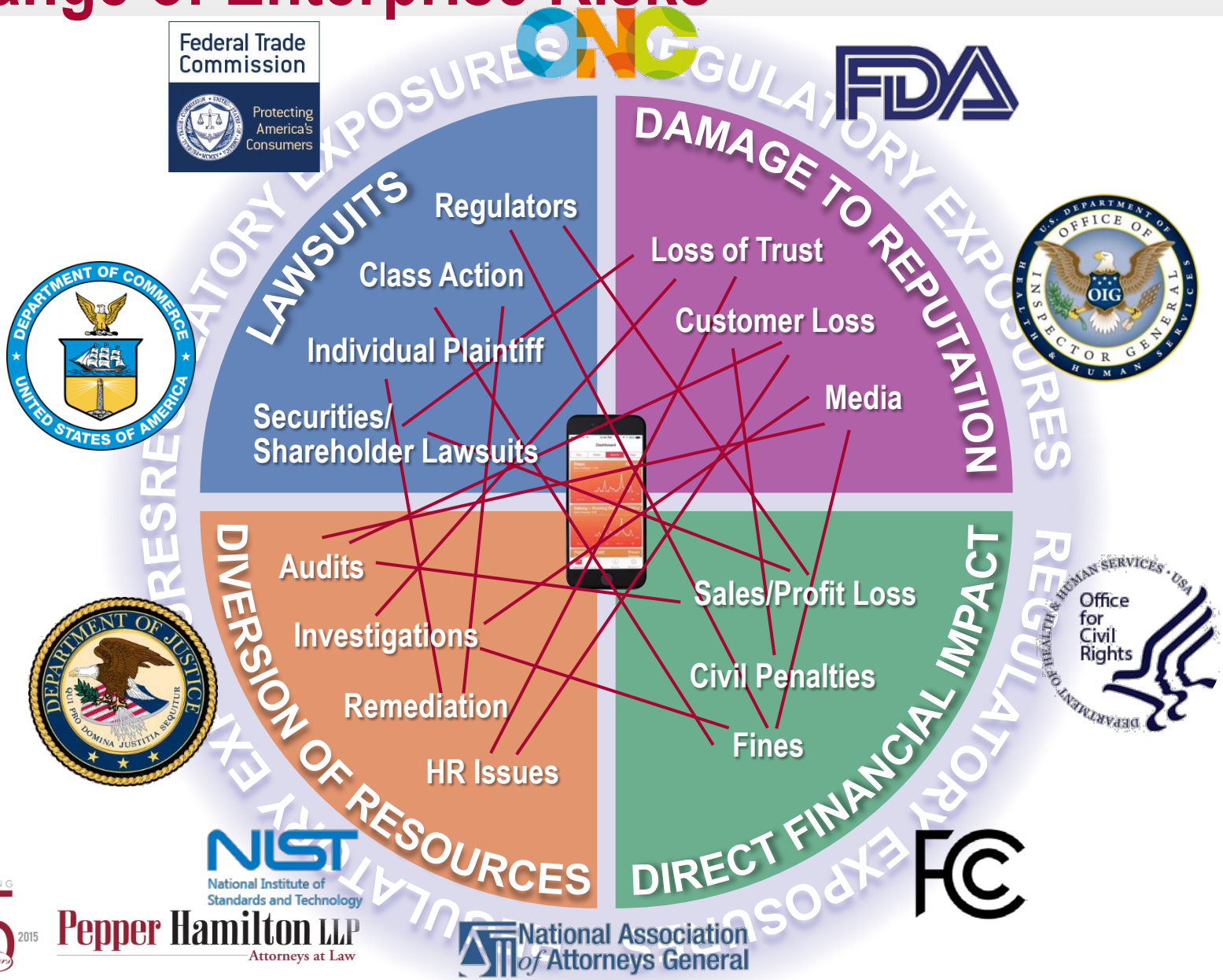
Department of Health & Human Services · USA
Office for Civil Rights

NIST
National Institute of Standards and Technology

National Association of Attorneys General

FCC

# Range of Enterprise Risks




CELEBRATING 1890 125 2015 Years

Pepper Hamilton LLP
Attorneys at Law

# Today's Presentation

## The Topics

- FDA
- FTC
- State Attorney Generals
- Consumer Class Actions
- Takeaways

# Food and Drug Administration Regulation and Enforcement

# What is a Medical Device?

A medical device is defined as:

- An instrument, apparatus, implement, machine, contrivance, or other similar or related article, including a component part or accessory, that is intended:
  - For use in the diagnosis of disease or other conditions;
  - For use in the cure, mitigation, treatment, or prevention of disease; or
  - To affect the structure or any function of the body



Source: 21 U.S.C. §321(h)

# If a Medical Device…

## FDA Regulatory Requirements include:

- Establishment Registration and Medical Device Listing
- Investigational Devices Exemption (IDE) requirements
- Labeling Requirements
- Premarket submission for approval or clearance (based on classification)
- Quality System Regulation
- Medical Device Reporting
- Correcting Problems

# If a Medical Device…

## FDA Regulatory Requirements include:

- Risk based classification based on controls necessary to provide reasonable assurances of safety and efficacy
  - Class I (low to moderate risk): general controls
  - Class II (moderate to high risk): general and Special controls
  - Class III (high risk): general controls and Premarket Approval

# February 9, 2015, FDA Guidance on Mobile Medical Applications

- What is the force of a “Guidance”?
- FDA intends to regulate mobile medical software that poses a threat to public safety
- The key regulatory factor is the **intended use** of the mobile health application
- Mobile medical Apps will be subject to the same standards FDA applies to traditional medical devices


*Glooko glucose monitoring logbook app and cable,* © 2015 Glooko, Inc.

# Intended Use Driving Classification

Will FDA regulate a **flashlight app**?

- If the app is advertised as a flashlight, FDA unlikely to regulate
- But if the app is advertised as an alternative to an ophthalmoscope (the light doctors flash in your eye), it may be subject to FDA regulation



Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

# Example of an FDA-Regulated Accessory

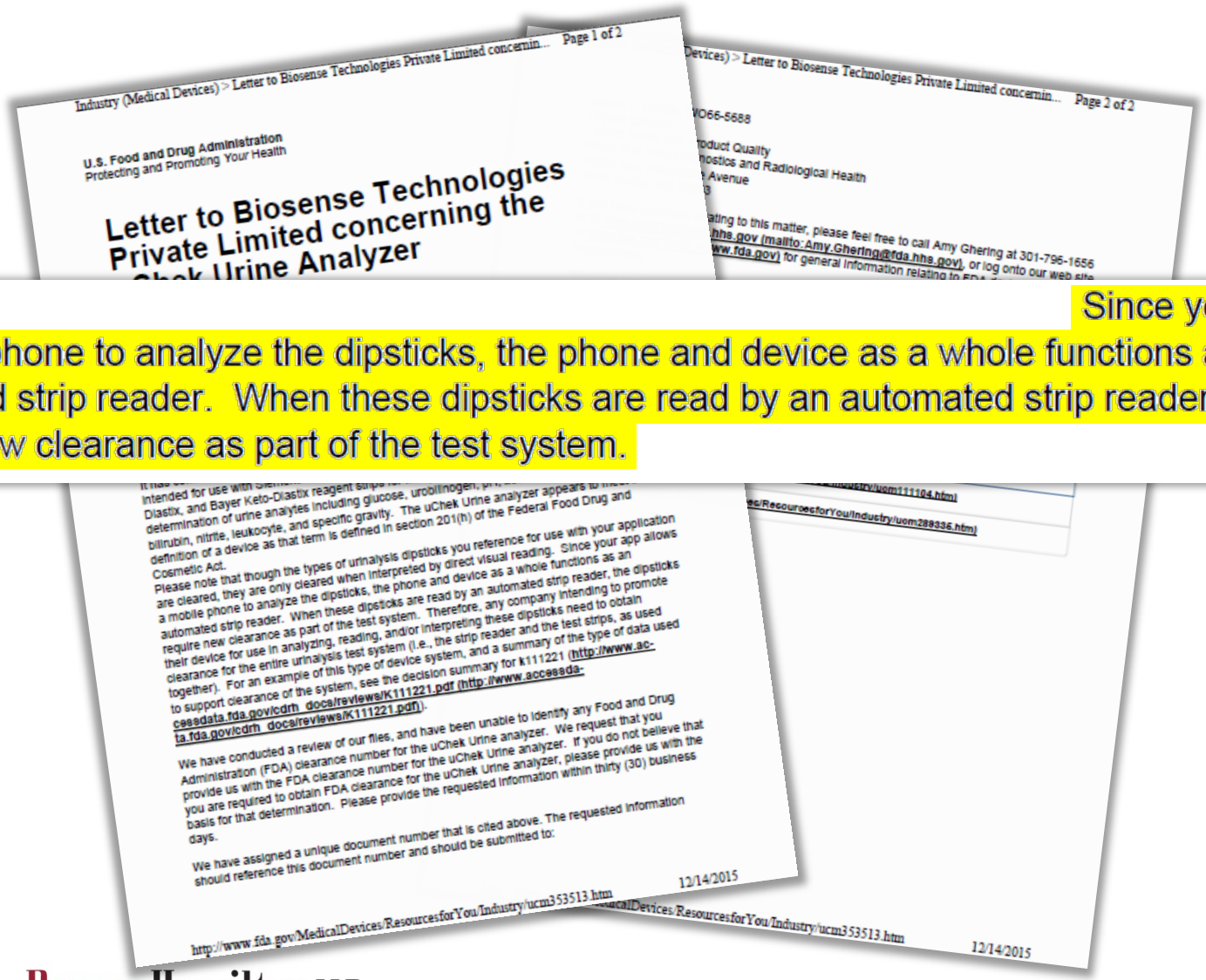
**uChek** app allowed users to analyze their urinalysis dipsticks using the camera on their mobile phone

- Dipstick is a cleared Medical Device approved only for direct visual reading
- App now enables a mobile phone to analyze the dipstick



Source: May 2013 Letter from FDA Offices of in Vitro Diagnostics and Radiological Health to Biosense

# Approved Device Analyzed by App Requires New FDA Clearance



Since your app allows a mobile phone to analyze the dipsticks, the phone and device as a whole functions as an automated strip reader. When these dipsticks are read by an automated strip reader, the dipsticks require new clearance as part of the test system.

Industry (Medical Devices) > Letter to Biosense Technologies Private Limited concernin... Page 1 of 2

U.S. Food and Drug Administration
Protecting and Promoting Your Health

**Letter to Biosense Technologies Private Limited concerning the Chek Urine Analyzer**

Devices) > Letter to Biosense Technologies Private Limited concernin... Page 2 of 2

...O66-5688

...oduct Quality
...nostics and Radiological Health
...Avenue

...ating to this matter, please feel free to call Amy Ghering at 301-796-1656
...hhs.gov (mailto:Amy.Ghering@fda.hhs.gov), or log onto our web site
...ww.fda.gov) for general information relating to FDA

Diastix, and Bayer Keto-Diastix reagent strips for the semi-quantitative or qualitative determination of urine analytes including glucose, urobilinogen, pH, protein, blood, specific gravity, bilirubin, nitrite, leukocyte, and specific gravity. The uChek Urine analyzer appears to meet the definition of a device as that term is defined in section 201(h) of the Federal Food Drug and Cosmetic Act.

Please note that though the types of urinalysis dipsticks you reference for use with your application are cleared, they are only cleared when interpreted by direct visual reading. Since your app allows a mobile phone to analyze the dipsticks, the phone and device as a whole functions as an automated strip reader. When these dipsticks are read by an automated strip reader, the dipsticks require new clearance as part of the test system. Therefore, any company intending to promote their device for use in analyzing, reading, and/or interpreting these dipsticks need to obtain clearance for the entire urinalysis test system (i.e., the strip reader and the test strips, as used together). For an example of this type of device system, and a summary of the type of data used to support clearance of the system, see the decision summary for k111221 (http://www.accessdata.fda.gov/cdrh_docs/reviews/K111221.pdf (http://www.accessdata.fda.gov/cdrh_docs/reviews/K111221.pdf)).

We have conducted a review of our files, and have been unable to identify any Food and Drug Administration (FDA) clearance number for the uChek Urine analyzer. We request that you provide us with the FDA clearance number for the uChek Urine analyzer. If you do not believe that you are required to obtain FDA clearance for the uChek Urine analyzer, please provide us with the basis for that determination. Please provide the requested information within thirty (30) business days.

We have assigned a unique document number that is cited above. The requested information should reference this document number and should be submitted to:

http://www.fda.gov/MedicalDevices/ResourcesforYou/Industry/ucm353513.htm 12/14/2015

...ResourcesforYou/Industry/ucm111104.html
...ResourcesforYou/Industry/ucm289336.html

...MedicalDevices/ResourcesforYou/Industry/ucm353513.htm 12/14/2015

Source: May 2013 Letter from FDA Offices of in Vitro Diagnostics and Radiological Health to Biosense

# FDA Will Regulate:

- Extending medical device **to control** the device for use in active patient monitoring
- Using attachments, screens, sensors to **transform** mobile platform into a medical device
- Performing **patient-specific** analysis
- Assisting with diagnosis or **patient-specific** treatment recommendations



Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

# FDA Does Not Intend to Regulate:

- Providing patients with tools to organize/track health information
- Helping patients document or communicate medical information to providers or access Medical Records
- Performing **simple** calculations used in clinical practice



Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

# FDA Does Not Intend to Regulate:

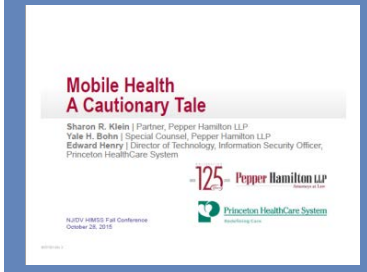
- Examples
  - Fitness Coach from iTunes
  - Apps for patients to log data they collect (*e.g.*, blood pressure) and report to provider
  - BMI calculators; delivery date estimators
  - Web portals to access own records
- Even if no FDA, other regulators (and regulations) may apply:
  - FTC
  - HIPAA/HITECH with transmission of PHI
  - State Consumer Protection Laws



Source: February 9, 2015, FDA Guidance on Mobile Medical Applications

# FDA and Cybersecurity

- FDA recently supplemented an existing guidance with additional information addressing cybersecurity vulnerabilities with networked medical devices
  - Unauthorized access into networked medical devices could impair the safety or efficacy of the device
- Continuing obligation to maintain safety and efficacy of device placed on the manufacturer, including accounting for cybersecurity




Visit http://bit.ly/1RS779b to download a PDF of a presentation from the 2015 Annual Fall Conference of the NJ/Delaware Valley Chapters of the Healthcare Information Management Systems Society (DVHIMSS) that addresses the serious security challenges resulting from the burgeoning use of mobile health care applications and the practical steps to manage such mobility risks.



Source: July 28, 2015 "Information for Healthcare Organizations about FDA's "Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software"

# 2016 OIG Work Plan

## Auditing and Enforcement

- Calls for increased scrutiny into data security capabilities of "networked medical devices" that are connected to electronic medical records (EMRs)
- Plans to examine whether FDA's oversight is sufficient to keep electronic protected health information (ePHI) contained within medical devices safe



Source: Office of Inspector General Work Plan – Fiscal Year 2016

# FDA and Cybersecurity

- July 2015 FDA Safety Alert regarding Hospira Symbiq Infusion System
  - FDA urged facilities to transition away from these devices because external hackers could control the device and change the dosage the pump delivers remotely



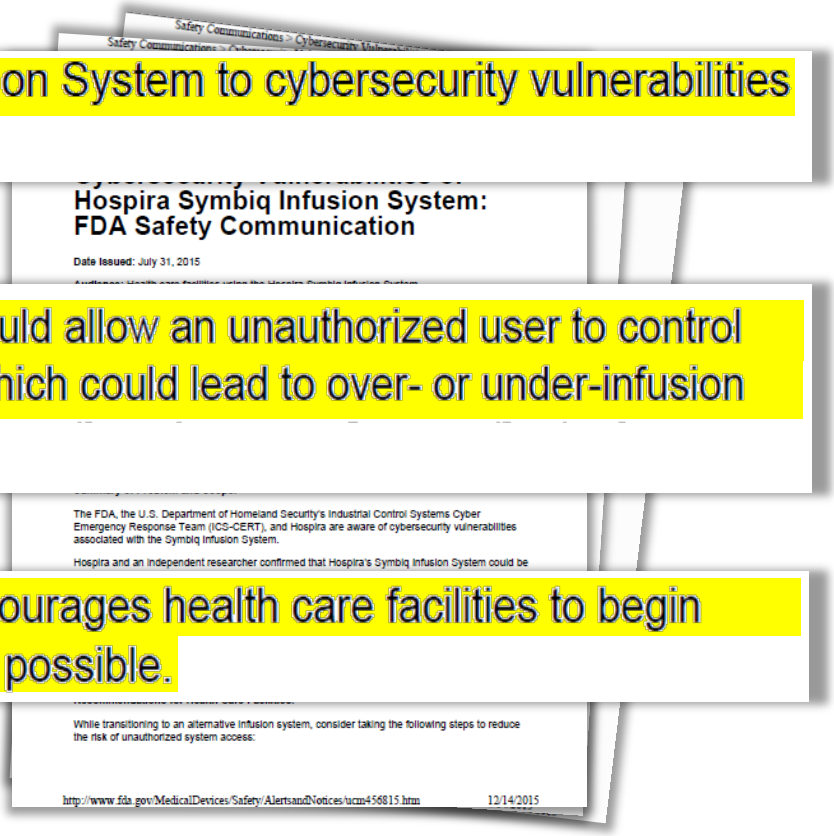

Source: July 31, 2015 FDA Letter to Hospira regarding "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication"

# FDA and Cybersecurity: FDA Safety Alert

The FDA is alerting users of the Hospira Symbiq Infusion System to cybersecurity vulnerabilities with this infusion pump.

accessed remotely through a hospital's network. This could allow an unauthorized user to control the device and change the dosage the pump delivers, which could lead to over- or under-infusion of critical patient therapies. The FDA and Hospira

the FDA strongly encourages health care facilities to begin transitioning to alternative infusion systems as soon as possible.


Safety Communications > Cybersecurity

**Hospira Symbiq Infusion System: FDA Safety Communication**

**Date Issued:** July 31, 2015

The FDA, the U.S. Department of Homeland Security's Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), and Hospira are aware of cybersecurity vulnerabilities associated with the Symbiq Infusion System.

Hospira and an independent researcher confirmed that Hospira's Symbiq Infusion System could be

While transitioning to an alternative infusion system, consider taking the following steps to reduce the risk of unauthorized system access:

http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm456815.htm 12/14/2015



Source: July 31, 2015 FDA Letter to Hospira regarding "Cybersecurity Vulnerabilities of Hospira Symbiq Infusion System: FDA Safety Communication"


# Federal Trade Commission Enforcement

# Topics

- The FTC's Interest in Mobile Medical Devices and Apps
- Select FTC Enforcement

# FTC Interest

- The FTC sees itself as the super-regulator, best equipped to protect consumers
  - Safety and advertising
  - Competition and economic impact
  - Privacy-by-design/Internet of Things
- FTC is empowered under, FTC Act § 5, which penalizes "unfair or deceptive acts or practices in or affecting commerce."



Source: 15 U.S.C. § 45

# FTC Enforcement

- Accretive Health, Inc.
- GMR Transcription Services, Inc.
- *FTC v. Wyndam*
- *FTC v. LabMD*


Visit http://bit.ly/1YhdEiK to download materials and listen to a recent Pepper/Bloomberg BNA webinar that addresses compliance and best practices under the FTC's 'Start with Security' initiative.

# Accretive Health, Inc.

## FTC Enforcement

- Accretive provides “revenue cycle” operations services to hospitals
- Accretive used actual live consumer personal information for training purposes
- An employee left a laptop containing information relating to 23,000 patients in a locked passenger compartment of a car, which was then stolen

**LESSONS LEARNED**

- Start with security
  - Don’t use personal information when it isn’t necessary
  - Protect devices that process personal information
- Secure paper, physical media, and devices
  - Keep safety standards in place when data is en route by implementing reasonable security policies

# GMR Transcription Services, Inc.

## FTC Enforcement

- GMR provided services to transcribe audio files, including for health care providers and hospitals, which included sensitive information about consumers
- GMR relied almost exclusively on third party service providers to transcribe the audio files, including medical transcription files
- FTC alleged that GMR did not adequately verify that their major service provider for medical transcription implemented reasonable security measures

**LESSONS LEARNED**

- Make sure your service providers implement reasonable security standards
  - Put it in writing when contracting with third party vendors
  - Verify compliance through audits

# FTC v. Wyndham

## FTC Enforcement

- Action arose from three (3) separate hacking incidents in 2008 and 2009
  - 619,000 customer records (names, addresses, credit cards) compromised
  - $10.6 million in losses
- FTC alleged, among other things, that Wyndham
  - failed to maintain reasonable security measures to monitor unauthorized computer access;
  - failed to conduct security investigations; and
  - failed to reasonably limit third-party access to company networks and computers.
- FTC brought an enforcement action under both the unfairness and deceptive prongs of Section 5

# FTC v. Wyndham

## FTC Enforcement

- Wyndham moved to dismiss at District Court level
  - Wyndham only challenged FTC's unfairness authority under Section 5. Wyndham claimed
    - Data security practices are not included in the definition of "unfair and deceptive" practices under Section 5
    - Section 5 violated principles of fair notice and due process because FTC fails to notify companies of rules, regulations and guidelines governing data security
- District of New Jersey denied motion to dismiss but certified the unfairness claim for appeal

# FTC v. Wyndham

## FTC Enforcement

- Third Circuit affirmed trial court and found FTC has authority to pursue enforcement action. The Court found
  - Unfairness does not require unfair conduct or unethical behavior and can occur even if company is victimized by criminal conduct
  - FTC does not have to publish rules and regulations for fair notice
  - FTC enforcement actions with other companies were sufficient to provide Wyndham with notice of acceptable cybersecurity standards
  - FTC's authority to police cyber-breaches is solidified
- Wyndham recently settled with the FTC
  - Settlement looks fairly similar but has enhanced monitoring provisions

# FTC v. LabMD

## FTC Enforcement

- LabMD is a privately held company that operated as a medical services provider, performing tests for patients at the request of doctors
- As part of its business, LabMD stored electronic billing records and medical records on an office computer
- In May 2008, a third party contacted LabMD and told LabMD that some of these files was available through LimeWire, a peer-to-peer sharing system

# FTC v. LabMD

## FTC Enforcement

- After being notified, LabMD determined that LimeWire had been installed on its billing computer, which LabMD promptly removed
- LabMD also searched and monitored LimeWire for several months for any evidence of the leaked files but found no evidence beyond the third party
- Nevertheless, the FTC brought an enforcement action against LabMD under the unfairness prong of Section 5

# Comparison of Allegations

## FTC Enforcement

### FTC v. Wyndham

- failed to maintain reasonable security measures to monitor unauthorized computer access;
- failed to conduct security investigations; and
- failed to reasonably limit third-party access to company networks and computers

### FTC v. LabMD

- did not employ readily available measures to prevent or detect unauthorized access to personal information on its computer networks; and
- did not develop, implement, or maintain a comprehensive information security program to protect consumers' personal information

# FTC v. LabMD

## FTC Enforcement

- Holding: No evidence that any consumer suffered any actual harm from alleged failure to employ “reasonable” data security
- There was no also evidence of a high likelihood of future harm

**LESSONS LEARNED**

- It matters how you react to an alleged data breach
- In the event of a data breach, use independent judgment to perform thorough investigations
- Monitor computer systems to determine if unauthorized software has been installed
- Breach does not necessarily mean liability

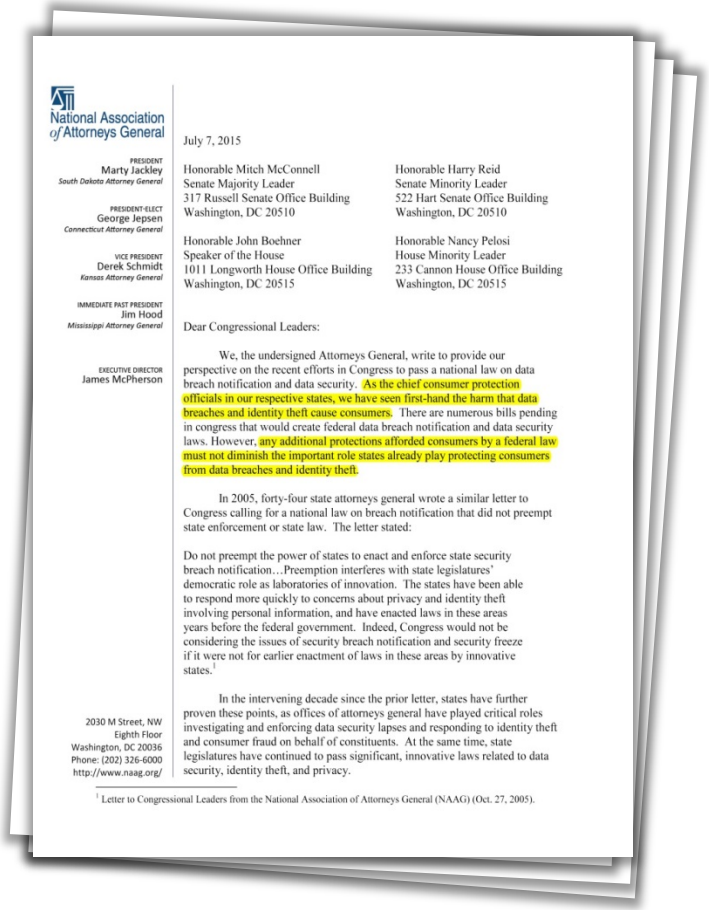
National Association of Attorneys General

# State Attorneys General Regulation and Enforcement

CELEBRATING 1890 125 Years 2015 Pepper Hamilton LLP Attorneys at Law

# State AGs: Intense Interest

## Letter to Congressional Leaders from the National Association of Attorneys General (Oct. 27, 2015)



National Association of Attorneys General

PRESIDENT
Marty Jackley
South Dakota Attorney General

PRESIDENT-ELECT
George Jepsen
Connecticut Attorney General

VICE PRESIDENT
Derek Schmidt
Kansas Attorney General

IMMEDIATE PAST PRESIDENT
Jim Hood
Mississippi Attorney General

EXECUTIVE DIRECTOR
James McPherson

July 7, 2015

Honorable Mitch McConnell
Senate Majority Leader
317 Russell Senate Office Building
Washington, DC 20510

Honorable Harry Reid
Senate Minority Leader
522 Hart Senate Office Building
Washington, DC 20510

Honorable John Boehner
Speaker of the House
1011 Longworth House Office Building
Washington, DC 20515

Honorable Nancy Pelosi
House Minority Leader
233 Cannon House Office Building
Washington, DC 20515

Dear Congressional Leaders:

We, the undersigned Attorneys General, write to provide our perspective on the recent efforts in Congress to pass a national law on data breach notification and data security. As the chief consumer protection officials in our respective states, we have seen first-hand the harm that data breaches and identity theft cause consumers. There are numerous bills pending in congress that would create federal data breach notification and data security laws. However, any additional protections afforded consumers by a federal law must not diminish the important role states already play protecting consumers from data breaches and identity theft.

In 2005, forty-four state attorneys general wrote a similar letter to Congress calling for a national law on breach notification that did not preempt state enforcement or state law. The letter stated:

Do not preempt the power of states to enact and enforce state security breach notification…Preemption interferes with state legislatures' democratic role as laboratories of innovation. The states have been able to respond more quickly to concerns about privacy and identity theft involving personal information, and have enacted laws in these areas years before the federal government. Indeed, Congress would not be considering the issues of security breach notification and security freeze if it were not for earlier enactment of laws in these areas by innovative states.[1]

In the intervening decade since the prior letter, states have further proven these points, as offices of attorneys general have played critical roles investigating and enforcing data security lapses and responding to identity theft and consumer fraud on behalf of constituents. At the same time, state legislatures have continued to pass significant, innovative laws related to data security, identity theft, and privacy.

2030 M Street, NW
Eighth Floor
Washington, DC 20036
Phone: (202) 326-6000
http://www.naag.org/

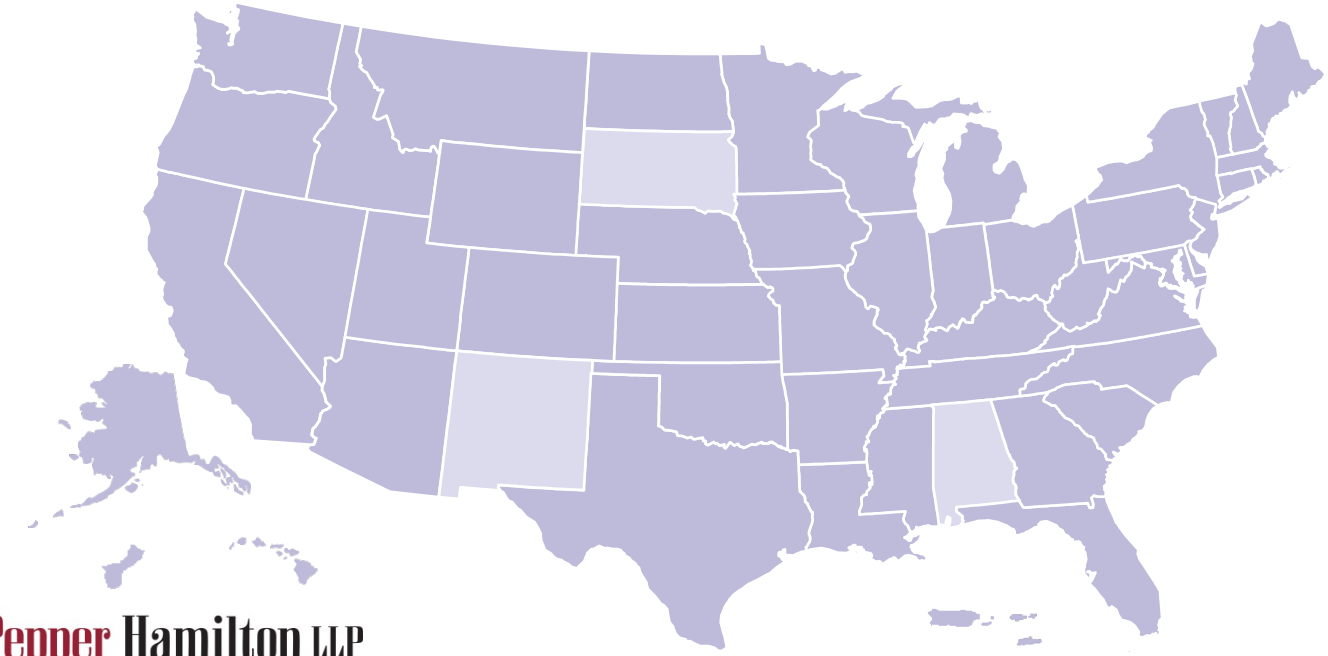
[1] Letter to Congressional Leaders from the National Association of Attorneys General (NAAG) (Oct. 27, 2005).

- **Data Breaches and Identity Theft Cause Significant Harm to Consumers**
- **States Play an Important Role Responding to Data Breaches and Identify Theft**
- **Federal Law Should Not Preempt State Law**
- **Data Security Vulnerabilities Are Too Common**

# State AGs

## Data Breach Notification Laws

- 47 states have enacted data breach notification laws
  - All require prompt notification of breach to consumers
  - Some require companies to adopt reasonable data security practices
- Provide for additional liability and impose civil penalties



# State AGs

## Enforcement Mechanisms

- What does a typical consent decree look like?
  - Penalties and fines dependent on the extent of the breach
  - Creation of new policies and procedures to ensure future compliance
  - Free identify theft protection/mitigation services
  - Mandatory audits and reporting back to State AGs
  - Creation of security based roles, including Chief Privacy Officer
  - Mandatory employee training on data security practices
  - Updates to technological infrastructure

# State AGs

## Consumer Protection

- Violating Data Breach Disclosure Laws can be a violation of Unfair Trade Practices Act
- State consumer protection laws based on Section 5 of FTC:
  - "Capable of misleading"
  - "Violates public policy"
  - "Unfair"
  - "Concealing or omitting a material fact in selling product"
  - Misrepresenting "characteristics or benefits…"
- Injunctive relief, restitution, civil penalties, disgorgement
- No proof of harm to collect civil penalties

# Consumer Class Actions

# Consumer Class Actions

- In addition to the state and federal government authorities, mobile medical app providers are also at risk for class action suits brought by private litigants
  - Sutter Health Class Action
  - Nike FuelBand Class Action

# Sutter Health

## Consumer Class Actions

- An unencrypted (but password-protected) laptop was stolen
- Plaintiffs sought statutory damages of $1000 per patient for over 4 million patients, totaling over $4 billion in nominal damages
- A purported class plaintiff claimed that Sutter Health violated California's Confidentiality of Medical Information Act (CMIA)
- The trial court denied Sutter Health's motion to dismiss, and Sutter Health appealed

# Sutter Health

## Consumer Class Actions

- The Court of Appeal vacated the decision and ordered the case dismissed because there was no evidence that patient information had been accessed or viewed by an unauthorized person

**LESSONS LEARNED**

- State statutory law has the potential to expose recipients of health information to large damages awards
- Even if ultimately successful, opposing class actions brought on state statutory grounds can be costly
- Securing physical media/devices is equally as important as securing electronic access to information

# Nike FuelBand

## Consumer Class Actions

- Purported class plaintiff brought action in California state court claiming Nike and Apple falsely advertised that the Nike Plus FuelBand electronic wristband accurately records each calorie burned by its wearer during physical activity
- Case settled for $15 check (or $25 Nike gift card) per consumer and $2.4 million in attorneys' fees all paid by Nike

**LESSONS LEARNED**

- Be careful what you advertise your product does
- When working with collaborators, hold collaborators to your standards and/or seek indemnification

# Final Thoughts and Questions

# Start with Security

The FTC provided guidance from lessons learned from 50+ data security related enforcement actions


1. Start with security
2. Control access to data sensibly
3. Require secure passwords and authentication
4. Store sensitive personal information securely and protect it during transmission
5. Segment your network and monitor who is trying to get in and out
6. Secure remote access to your network
7. Apply sound security practices when developing new products
8. Make sure your service providers implement reasonable security standards
9. Put procedures in place to keep your security current and address vulnerabilities that may arise
10. Secure paper, physical media, and devices

# Questions to Ask Yourself

- What is the function and use of the device?
- Is it a non-mobile device with the same function already regulated?
- Who are your customers?
- What PII/PHI do you absolutely need to operate?
- Which business areas/practice segments interact directly with those customers or their data?
- Who has oversight over the laws and regulations that apply to your industry and company?
- Which business areas are interact directly with these regulators?
- What standards are established and/or are developing in your industry regarding data privacy and security?

# Resources

## Regulatory Guidance

October 2014, California Department of Justice, "California Data Breach Report"

June 2015, Federal Trade Commission, "Start with Security Guidance"

NIST Guidance

October 2, 2014, Food Drug and Administration, Guidance regarding "Content of Premarket Submissions for Management of Cybersecurity in Medical Devices"

February 9, 2015, Food Drug and Administration, Guidance regarding "Mobile Medical Applications"

July 28, 2015, Food Drug and Administration, 'Information for Healthcare Organizations about FDA's Guidance for Industry: Cybersecurity for Networked Medical Devices Containing Off-The-Shelf (OTS) Software'"

# Resources

## Pepper Resources

March 24, 2015, *Federal Court Holds that Data Breach Plaintiffs Have No Standing Unless They Show Misuse*

September 11, 2015, *How to Avoid and Respond to a Cybersecurity Breach*

September 29, 2015, *Jumpstart Your Cybersecurity Program: Compliance and Best Practices Under The FTC's 'Start With Security' Initiative*

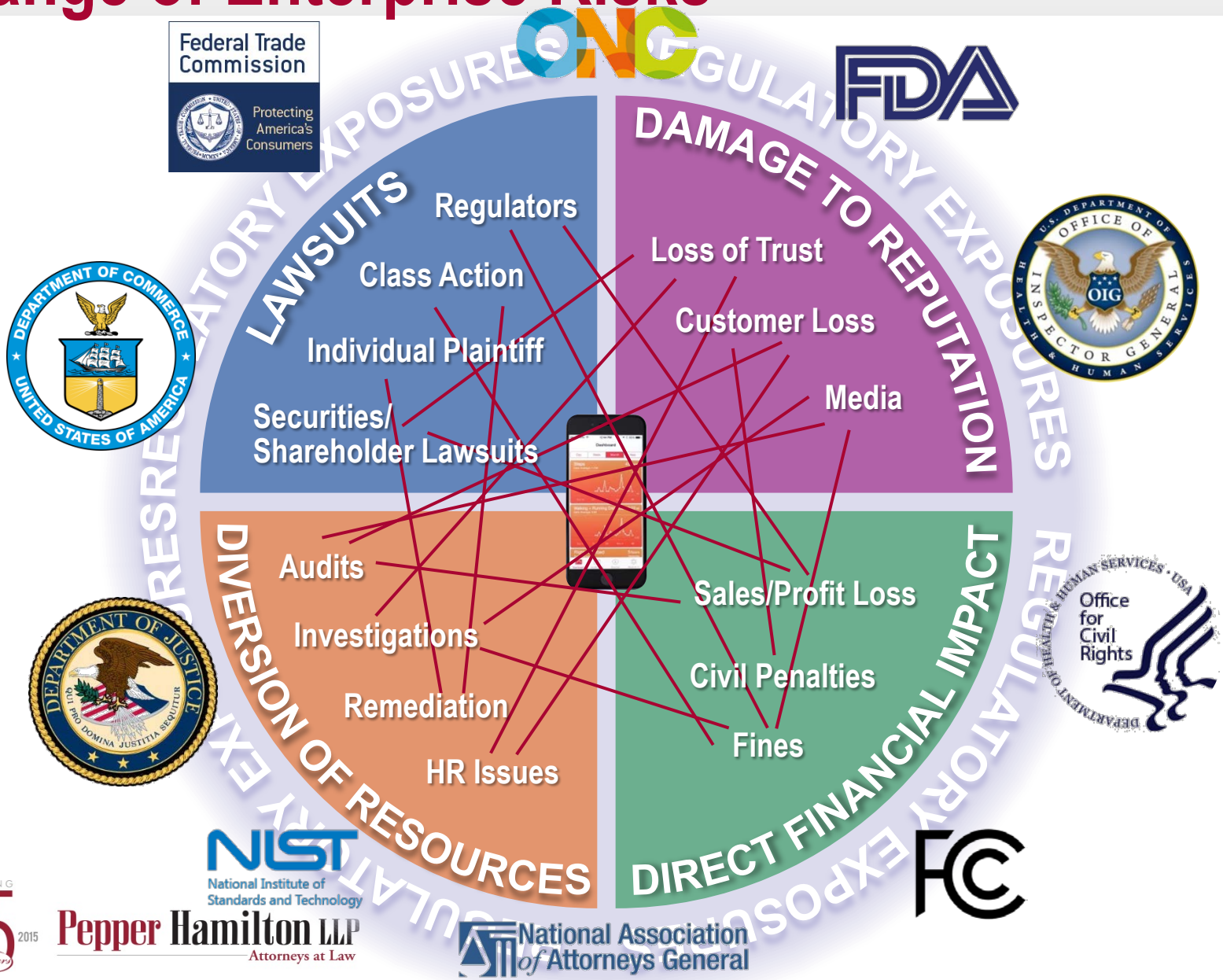
July 8, 2014, *Telemedicine and Mobile Health Innovations Amid Increasing Regulatory Oversight*

April 14, 2015, *Beyond HIPAA: Connected Health Care and the Internet of Things*

March 7, 2014, *When Is an iPad More than an iPad? When It Is an FDA Regulated Medical Device*

June 24, 2013, *Unhack My Heart: FDA Issues Guidance to Mitigate Cybersecurity Threats in Medical Devices*

# Range of Enterprise Risks



# Questions?

**Barry H. Boise**
215.981.4591
boiseb@pepperlaw.com

**T. Stephen Jenkins**
215.981.4743
jenkinst@pepperlaw.com

**Michael D. Vives**
215.981.4217
vivesm@pepperlaw.com