CLOUD SECURITY LAW

MICHAEL KEELING, PE, ESQ.

KEELING LAW OFFICES, PC

PHOENIX AND CORONADO

Presented at

Cloud Security Alliance Meeting

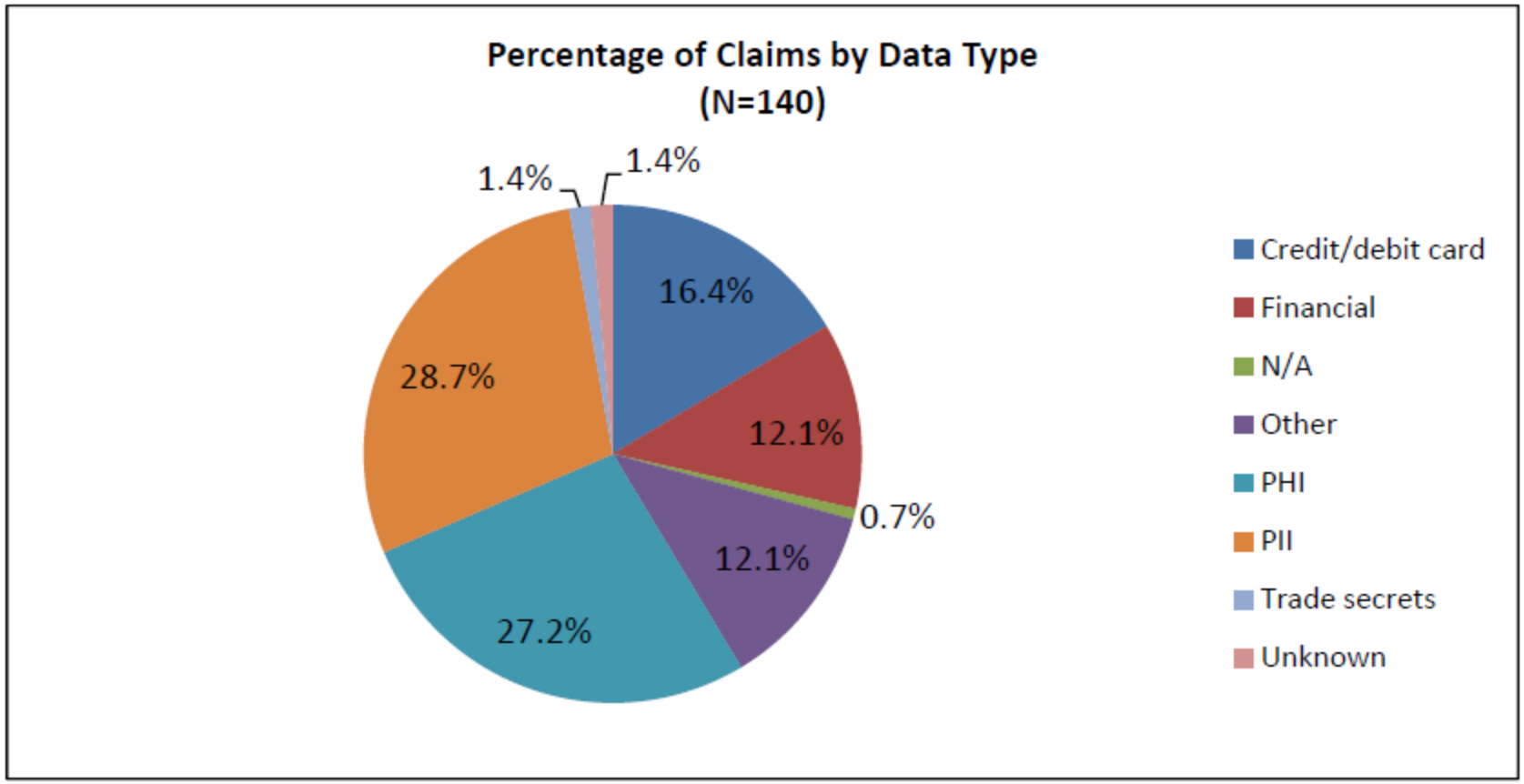
January 20, 2015

Phoenix

Cloud Perspectives

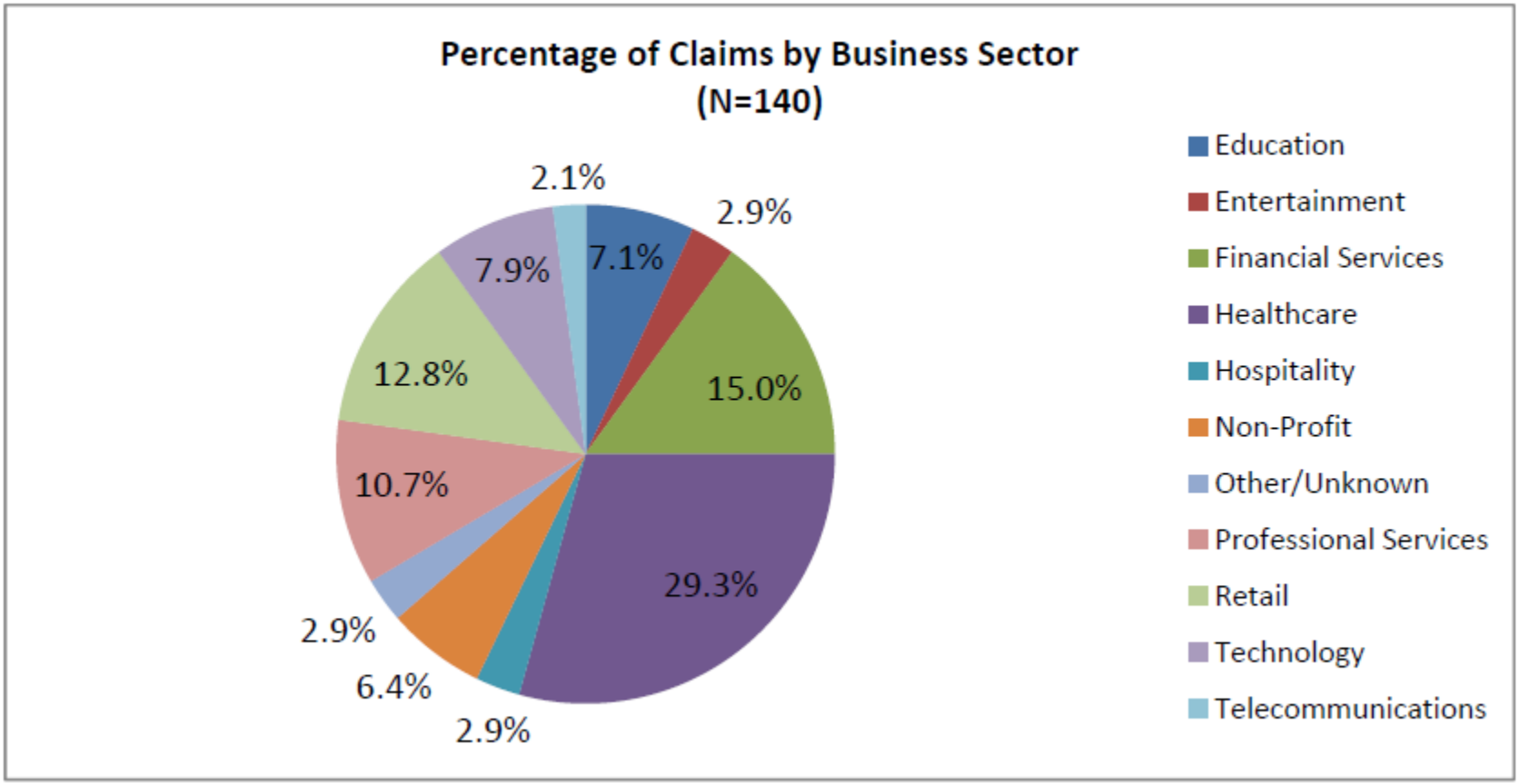
- Gartner sees
  - the cloud as a: "style of computing where scalable and elastic IT-related capabilities are provided as a service to customers using Internet technologies."
- Government sees
  - Enforcement of specific statutes
    - HIPAA
    - CAN-SPAM (Commercial messaging)
    - GLB (Financial services)
    - COPPA (Children)
  - Compliance—Federal Guidelines
    - NIST
  - State Actions
    - State patchwork of statutes
  - Federal Trade Commission
    - Primary federal enforcer.

Percentage of Claims by Data Type



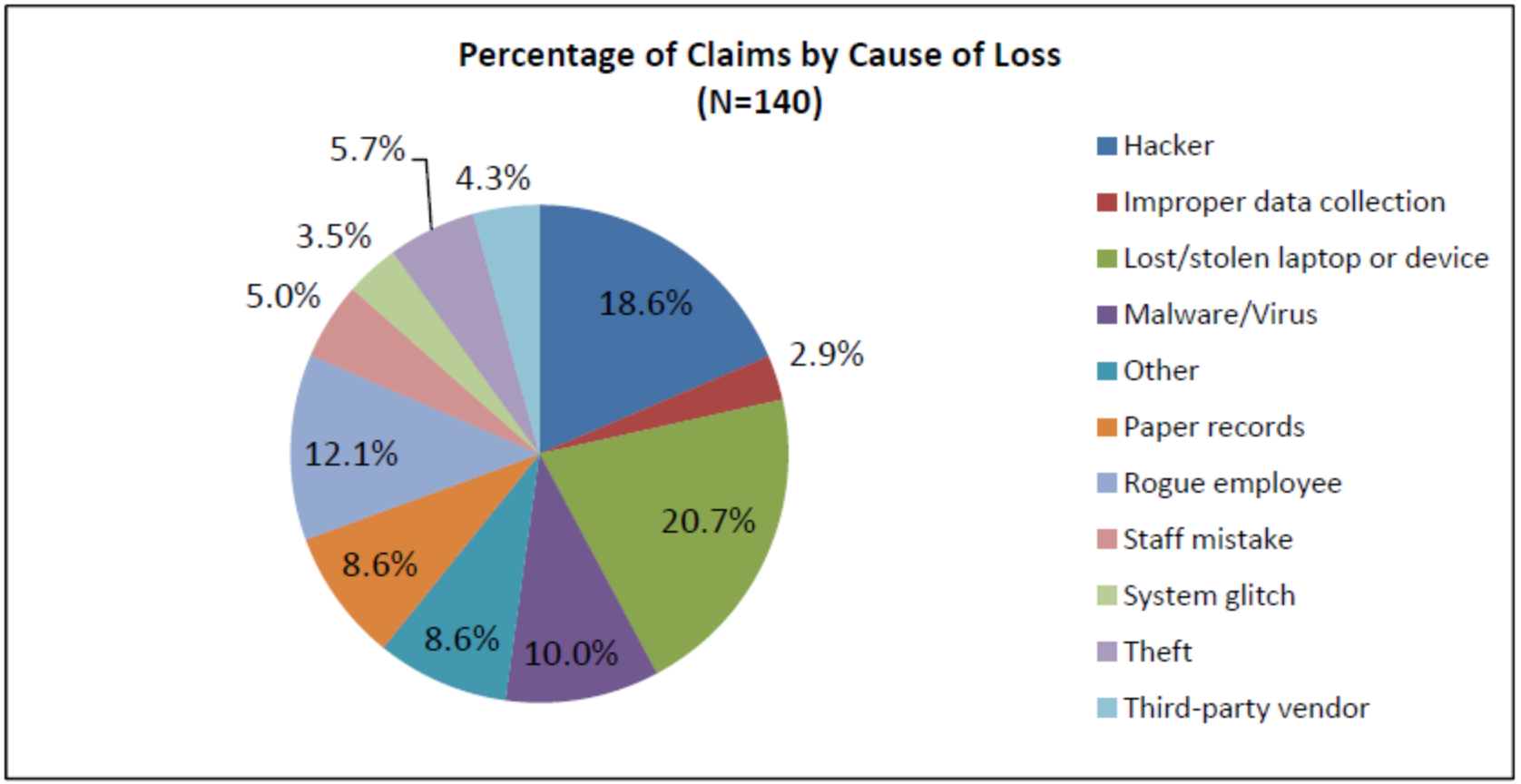
NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims

Percentage of Claims by Business Sector



NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims

Percentage of Claims by Cause of Loss



NetDiligence® 2013 Cyber Liability & Data Breach Insurance Claims

State Regulatory Exposure

- 47 States require **notice** of security breaches
  - After unauthorized access of PII/PHI
  - **If** unencrypted computerized PII/PHI
- Many States
  - **Require Notice** to state attorney general, state consumer protection agencies, and credit monitoring agencies
  - Allow **private right of action** for violations
- Encryption often a **safe harbor**
  - Data-at-rest
  - Data in transit

FTC Act

- Prohibits "**unfair or deceptive practices** in or affecting commerce."
  - **"Unfair" if** …Practice
    - Causes or is **likely to cause** substantial injury to consumers
    - **Cannot reasonably be avoided** by consumers
    - Is **not outweighed** by countervailing benefits to consumers or to competition
  - **"deceptive" if** … Practice, or Representation, or Omission
    - Misleads or is **likely to mislead** consumers
    - Based on **Consumers' interpretation** under circumstances
    - Is it **material**?
- **No intent** required (strict liability).

Liability Equals

Common Law 101

- Duty
- Breach
- Causation
- Injury/Harm
- Damages
- Defenses.

Federal Trade Commission

- No “unfair or deceptive practices in or affecting commerce.”
  - Broad dragnet
  - No *Intent* required
  - No *actual harm* required.

Court Ruled FTC Can Enforce Breaches As An Unfair Practice Under FTC Act

- FTC sued Wyndham Worldwide Corporation in 2012, alleging
  - Violated FTC Act's prohibition against unfair or deceptive acts or practices.
  - Failure to maintain reasonable and appropriate data security for consumers' sensitive personal information"
- Wyndham, moved to dismiss, arguing
  - FTC did not have authority to bring an "unfairness" claim involving data security.
- Court disagreed
  - Finding specific data security legislation passed after FTC Act merely complemented FTC's unfairness authority—but did not preclude it.
- Wyndham also argued
  - FTC had to publicize regulations to provide fair notice of its data security standards
- Court disagreed
  - Court determined taking such publication was not the only way to do so.
  - It noted **FTC Act, Section 5** provides a **three-part test**
    - Suggesting entities look to **complaints, consent agreements and public statements** to figure out FTC's standard for bringing an unfairness claim under the Act.

FTC—In Action

- Practices FTC **attacks** as "**deceptive**"
  - Violating your published privacy policies
  - Failing to verify identity of persons to whom confidential consumer information was disclosed
  - Downloading spyware/adware onto unsuspecting users' devices
- Practices FTC **attacks** as "**unfair**"
  - Failing to implement reasonable safeguards to protect privacy of consumer information
    - As compared to "developing" federal standards
      - FTC's "yardstick" is a moving target.

FTC Suit—Snapchat Misleads By Claiming Messages "Disappear Forever"

- FTC accused Snapchat of violating FTC Act, Section 5—barring deceptive business practices.
  - "if you make promises about privacy, you must honor those promises."
- FTC alleged Snapchat messages are not ephemeral as promised
  - Snapchat wrongly informed its users that their messages would vanish
    - Company's FAQ: "Is there any way to view an image after the time has expired? No, snaps disappear after the timer runs out."
    - FTC interpreted as an absolute statement. Period.
  - Snapchat deceived consumers about PII it collected and what it did with the PII.
  - Snapchat users were likely attracted by promise that their messages would disappear.
  - "Several methods exist by which a recipient can save both photo and video messages, allowing access indefinitely."
- Settlement
  - Bars Snapchat from misrepresenting its privacy policies
  - Requires Snapchat implement "a comprehensive privacy program"…monitored **20 yrs**.
  - Violations of settlement, liable for up to **$16,000 per violation per day**

FCC Expands Its Data Security Regulatory Reach

- FCC $10 million fines, October 24, 2014
  - TerraCom Inc. and YourTel America Inc.
- First time, but per FCC Enforcement Bureau Chief
  - "**it will not be the last**"
- Allegedly the 2-companies
  - collected consumer PII to demonstrate eligibility for FCC's Lifeline program
  - Stored-online unencrypted customer PII
  - with no security safeguards
- Alleged failure is
  - Violation under FCC ACT, Section 222(a), and
  - Unjust and unreasonable practice in violation of Section 201(b)
- Section 503(b)(1)
  - Empowers FCC to order forfeiture penalties for violations of the Act,
  - But does not specify a base forfeiture per violation.

Security Breach Litigation

- **Breach of Contract/Implied Contact and Negligence**
  - Anderson v. Hannaford Brothers Co., 659 F.3d 151 (1st Cir. 2011)
    - Finding **Implied contract duty** by grocery store to protect customers' data
  - Patco Construction Co. v. People's United Bank, 684 F.3d 197 (1st Cir. 2012)
    - Holding defendant's security procedures not commercially reasonable
- **Standing in Class Action Cases**
  - Lambert v. Hartman, 517 F.3d 433 (6th Cir. 2008)
    - Finding **standing** where P's information posted on municipal website, taken by identity thief, causing actual financial loss traceable to D's conduct
  - Resnick v. AvMed, Inc., 693 F.3d 1317 (11th Cir. 2012)
    - Finding **standing** where plaintiffs were **identity-theft victims**
  - Pisciotta v. Old National Bancorp., 499 F.3d 629 (7th Cir. 2007)
    - Finding **standing** based on **threat of future harm**
  - Krottner v. Starbucks Corp., 628 F.3d 1139 (9th Cir. 2010)
    - Finding **standing** where plaintiffs **unencrypted PII** stored on a stolen laptop
  - Reilly v. Ceridian Corp., 664 F.3d 38 (3d Cir. 2011)
    - Finding **no standing** in employee risk-of-identity theft suit alleging negligence and breach of contract against a payroll processing firm.

Court Allows HIPAA “Standard of Care" Negligence Claim

- **Connecticut Supreme Court** rules plaintiffs can sue for negligence if a healthcare provider violates HIPAA privacy regulations
  - *Emily Byrne vs. Avery Center for Obstetrics and Gynecology* (2014)
- HIPAA does not provide for the “private right of action”
- In data-breach cases, plaintiffs argue
  - healthcare provider, insurer or other covered entity (Business Associates) did not meet the “standard of care” under HIPAA security or privacy rule in protecting records
  - and that failure to meet that standard of care was negligent.
- BUT—in negligence lawsuits, plaintiffs must show damages.

Defenses Shrinking

- *Krottner v. Starbucks Corp.*
  - **Increased risk of identity theft** constitutes an **injury-in-fact**
- *Anderson v. Hannaford*
  - **Alleged fraud in population** and **money spent** in mitigation efforts sufficient (instead of time/effort)
- *ITERA* (Identity Theft Enforcement and Restitution Act)
  - Pay an amount equal to **Victims' value of time** reasonably spent
- *In re Hannaford Bros. Data Security Breach Litigation*
  - **Time equals money—if fraud; credit monitoring damages**
- *ChoicePoint Data Breach Settlement*
  - **"Time they [victims] may have spent monitoring their credit or taking other steps in response"**

Director Liability Arising From Data Breach

Palkon v. Holmes, No. 14-cv-01234 (D.N.J.), Wyndham SHs sued D&O's, claiming their failure to implement adequate information-security policies allowed 3 data breaches

- Shareholder derivative actions
  - Plaintiff is not required to prove damages resulting from theft of PII.
- Directors owe Duties Of Care (BJR) and Loyalty—including Duty of Oversight (No BJR)
  - Did not implement reporting or information system or controls; *or*
  - Implemented controls, BUT "consciously failed to monitor or oversee its operations." *Stone*.
- After a data breach, claims against board probably will be
  - Breach of Duty of Care and
  - Breach of Duty Loyalty/Oversight
    - Court "look[s] for evidence of whether a board has acted in a deliberate and knowledgeable way identifying and exploring alternatives." *Citron v. Fairchild Camera*
    - Directors may rely on reports prepared by others, BUT MUST TAKE an active and direct role
    - Board that fails to manage and monitor cybersecurity probably breaches its duties of care and oversight
- Protect Against Liability
  - Board must become well-informed
  - Board should appoint a committee responsible for privacy and security
  - Recruit and hire at least one tech-savvy member
  - Follow best industry practices
- Indemnification and Insurance
  - Articles of incorporation—provision eliminating director personal-liability for monetary damages for breach of the Duty of Care/Loyalty.
  - D & O Policy—WITHOUT exclusions to liability resulting from a privacy breach
  - **Example Problem Exclusion**: Insurer shall not be liable for Loss relating to a Claim made against an Insured:
    - "for emotional distress of any person,
    - or for injury from libel, slander, defamation or disparagement,
    - or for injury from a violation of a person's right of privacy."

Strategies to Minimize Exposure

- Review privacy/security policies and practices
  - Are you waking the talk?
  - If not—change it—ensure your policies never out-pace your practices
- Make privacy/security policy a binding contract
- Use arbitration provision in consumer contracts
- Review third party contracts that collect/store/transport PII/PHI
- Add **indemnification** provisions in agreements
  - Does your indemnifying contracting-party have adequate resources?
- Review/add **insurance**
- Evaluate credit card practices under state laws
- Technology solutions—tied to policy elements

Audit Your Cloud

- **Service Provider Responsibilities**
  - Service Level Agreements (SLAs)
  - Risk assessments
    - Performance and frequency
    - Where is the data?
- **Compliance**
  - Right to Audit
  - Third-party Reviews
  - ISO 27001, etc.
- **Incident Response, Notification and Remediation**
  - Legal and regulatory compliance
  - Exercising of response plans
- **Data Security**
  - Encryption
- **Identity and Access Management**
  - Who am I/What do I know/What do I have?

Prevent/Mitigate Litigation

End-User Measures:

- Encrypt data before sending to Cloud
- Industry-specific restrictive rules—on data storage/transport
- Notify customer/client HOW data is stored as part of contract governing basic relationship
  - E.g., FINRA/securities and HIPAA/medical providers
- Sophisticated/often-changed pass-phrases

- Address Cloud storage issues
  - Leak response plan
  - Compliance

Post-Leak Litigation Prevention

- Immediate internal investigation
  - Retain counsel – privilege/work product issues
  - Interview key personnel
  - Document actions taken
- Immediately and fully notify customers
  - No cover up, minimization, or delayed reporting
  - Include plan/potential compensation offer
  - Establish customer hotline

QUESTIONS

Cloud Security Law

Michael Keeling, PE, Esq.
Keeling Law Offices, PC
Phoenix and Coronado, CA
www.keelinglawoffices.com