Litigation Forum: When You Face Your First CID—Key Steps to Take When the FTC Investigates Your Company’s Privacy Practices

Presented by Anthony T. Pierce, Catherine E. Creely, Jacqueline K. Connor and Laura E. Jehl

March 10, 2015
12:30 p.m. – 2:00 p.m.
Anthony T. Pierce is a litigator who has handled a variety of complex disputes in state and federal courts, including commercial litigation, intellectual property, employment matters and internal investigations. He is the partner in charge of the firm’s Washington, D.C. office and a member of the firm’s management committee.

Mr. Pierce’s litigation and trial experience covers a diverse group of industries, including technology and telecommunications, health care, energy, entertainment and media, financial services and government contracting. As an outgrowth of his service as an investigator for the U.S. Government Accountability Office during law school, Mr. Pierce also has significant experience in internal investigations. He has conducted internal investigations to determine possible civil and criminal liability for clients for accounting fraud, employee misconduct and theft of intellectual property. Both his litigation and investigative experience have involved representing numerous clients before a plethora of federal and state regulatory and investigative agencies, including the FDA, FTC, FCC and state attorneys general.

Mr. Pierce received his J.D. in 1987 from the Georgetown University Law Center where he served as the case and notes editor of the *Georgetown Immigration Law Journal*.

Mr. Pierce is a frequent speaker on legal issues ranging from how to conduct internal investigations to the unique aspects of litigating in the “rocket docket.” In his management capacity, Mr. Pierce has also been a frequent speaker on diversity issues facing the legal community. He takes an active role in addressing legal and business issues facing the greater Washington, D.C. community. Most recently, he serves as the Chairman of the Greater Washington Board of Trade.
Catherine E. Creely’s practice focuses on a variety of litigation matters, including white collar criminal defense, government investigations and complex civil litigation.

Ms. Creely has represented corporate and individual clients in state and federal court as well as in connection with investigations by the U.S. Congress, the Department of Justice, and other federal and state regulatory bodies, including the Federal Trade Commission and the International Trade Commission. She has participated in a variety of litigation matters involving patent infringement, securities fraud, antitrust issues, breaches of contract and civil and criminal forfeitures. Ms. Creely also represents clients in the energy sector, including a major international oil company, in matters arising in federal and state courts. Ms. Creely maintains an active pro bono practice with a particular focus on individuals facing the death penalty.

Ms. Creely was an associate editor of *The Catholic University Law Review*. While attending law school, Ms. Creely represented clients as a student attorney in Catholic’s Advocacy for the Elderly Clinic and competed in moot court competitions at the national level.
Jacqueline Connor is an attorney in the Division of Privacy and Identity Protection at the Federal Trade Commission in Washington, D.C. She investigates and litigates violations of U.S. laws enforced by the Commission that govern the privacy and security of consumer information. Ms. Connor is currently serving as a staff attorney on the FTC v. Wyndham Worldwide litigation, as well as other non public investigations and consent negotiations. She has investigated and resolved matters involving data security, privacy, the Child Online Privacy Protection Act, the Gramm-Leach-Bliley Act and the Fair Credit Reporting Act. Ms. Connor is a graduate of Boston University School of Law.
Ms. Jehl is general counsel and chief privacy and security officer at Resolution Health, Inc (“RHI”), a wholly owned subsidiary of Anthem, Inc., which uses healthcare data analytics and personalized communication to improve health outcomes. In addition to her role at RHI, Ms. Jehl has responsibility for privacy issues across the Anthem corporate enterprise, and for legal issues presented by the development of innovative healthcare technologies.

Before joining Resolution Health, Ms. Jehl was chief litigation counsel at AOL, where she played a critical role in the development of Internet law, most notably involving the ISP immunity provisions of Section 230 of the Communications Decency Act, the legal battle against junk email and in achieving, on behalf of Netscape, a significant settlement of its antitrust lawsuit against Microsoft. Ms. Jehl later served in a business role as chief of staff to AOL’s vice-chairman. Early in her career, she was a lawyer in private practice at Covington & Burling in Washington, DC.

Ms. Jehl received her B.A. with highest honors in Political Science from the University of California, Berkeley, and her J.D. cum laude from Harvard Law School.
Facing an FTC Civil Investigative Demand: Topics Covered

- Introduction
- Background: The Federal Trade Commission
- Data Privacy and Security
- Trending at the FTC: Data Privacy and Security
- Enforcement and Investigation
- Best Practices
Background: The Federal Trade Commission

- The views expressed in this presentation are mine and are not necessarily those of the Commission or any individual Commissioner.
- The FTC is an independent law enforcement agency.
- The FTC’s mission is to protect consumers and promote competition.
- Section 5 of the FTC Act prohibits “unfair or deceptive acts or practices in or affecting commerce.”
  - Deception: material misrepresentations, omissions or practices that are likely to mislead consumers acting reasonably under the circumstances.
  - Unfairness: practices that cause, or are likely to cause, substantial injury to consumers that is not reasonably avoidable and is not outweighed by benefits to consumers or competition.
- The Commission also has enforcement or administrative responsibilities under more than 70 other laws.
Background: The Federal Trade Commission

**Commission investigations may originate from:**

- Presidential requests
- Congressional requests
- Government agency requests
- Attorney General requests
- Referrals by the courts
- Complaints by members of the public
- The Commission upon its own initiative
Data Privacy and Security – Definitions

- **Personal Information (PI)** – information that can be used to determine the identity of a person.

- **Privacy** – how you collect, use, access, share, manage and retain PI. Privacy also concerns what notice and choice you give to consumers about the use of PI (e.g. email opt-outs).

- **Security** – how you protect information from unauthorized access.
Data Privacy and Security in the News

- **Sony Data Breach**
  - On November 24, 2014, Sony Pictures Entertainment suffered a massive, debilitating cyber attack that compromised its business data, unreleased movies, confidential correspondence and the personally identifiable information of its current and former employees.

- **Anthem Data Breach**
  - On January 29, 2015, Anthem, Inc., the second largest U.S. health insurance company, discovered that cyber attackers had gained unauthorized access to Anthem’s IT system and obtained personal information relating to as many as 80 million consumers.

- **Costs of These Data Breaches**
  - Direct costs of investigating and remediating the breach, like credit monitoring.
  - Intangible costs like loss of reputation or unstructured data (e.g. emails being leaked).
  - Responding to government requests and investigations, such as those initiated by the U.S. House Committee on Oversight following the Sony breach.
  - Legal costs, like the class action lawsuits that have been filed by former employees who claim their personal information was not adequately secured by Sony.
  - According to a widely cited Ponemon Institute study, the **average cost of a data breach is between $188 and $277 per individual record compromised.**
Snapchat Settles FTC Charges That Promises of Disappearing Messages Were False (May 8, 2014)

- According to the FTC’s complaint, Snapchat made multiple misrepresentations to consumers about its product that stood in stark contrast to how the app actually worked.

- “If a company markets privacy and security as key selling points in pitching its service to consumers, it is critical that it keep those promises,” said FTC Chairwoman Edith Ramirez. “Any company that makes misrepresentations to consumers about its privacy and security practices risks FTC action.”

- Snapchat must implement a comprehensive privacy program that will be monitored by an independent privacy professional for the next 20 years.
Trending at the FTC: Data Privacy and Security

- FTC Files Complaint against Wyndham Hotels for Failure to Protect Consumers’ Personal Information (June 26, 2012)

  ● The FTC alleges that Wyndham Hotels’ privacy policy misrepresented the security measures that the company took to protect consumers’ personal information, and that these failures led to three data breaches, thousands of fraudulent charges on consumers’ accounts, millions of dollars in fraud loss and the export of hundreds of thousands of consumers’ payment card account information to an internet domain address registered in Russia.

  ● The case against Wyndham is part of the FTC’s ongoing efforts to make sure that companies live up to the promises they make about privacy and data security.

- This case is in ongoing litigation in federal court that began in June of 2012.
Trending at the FTC: Data Privacy and Security

**CVS** (February 2009)

- HHS and FTC announced a settlement with CVS under which the retail pharmacy chain would pay **$2.25 million** and take corrective action to protect patient privacy.
- The settlement resulted from a joint OCR/FTC investigation based on media reports that CVS pharmacies were disposing of pill bottles and other items containing PHI in unsecured industrial trash containers outside some stores.

**Reviews by OCR and FTC concluded that:**

- CVS failed to implement adequate policies and procedures to appropriately safeguard PHI during the disposal process.
- CVS failed to adequately train employees on how to dispose of patient information properly.

In addition to the payment of $2.25 million and a corrective action plan, CVS also signed a separate consent order with the FTC requiring **monitoring by an independent third party for a period of 20 years.**
Trending at the FTC: Data Privacy & Security

- **FTC Urged to Probe Verizon ‘Supercookies’ for Possible Violations**
  - Senate Democrats urged the FTC to investigate recent reports that “supercookies” developed by Verizon Wireless have been used to track the habits of cellphone users (Feb. 6, 2015).

- **National Data Security Legislation is Likely**
  - Following massive security breaches at companies like Target, Home Depot and Sony, an FTC official told Congress that the need has never been greater for data security legislation.
  - “While we have tools and we’re using them to address data security failures by companies, it would be extremely helpful to have a federal law requiring data security, not just notification, with civil penalties,” Jessica Rich, director of the FTC’s bureau of consumer protection, told the Senate Banking Committee’s national security subpanel. Stephanie Condon, *FTC asks Congress for stronger tools to fight data breaches*, CBS News (Feb. 3, 2014).
Trending at the FTC: Data Privacy & Security

President Obama Announced a New Cybersecurity Legislative Proposal on January 13, 2015, that includes:

- Modernizing law enforcement authority to combat cyber crime
- Adopting a national data breach reporting standard

Consumer Privacy Bill of Rights

- “Discussion draft” released by the White House on February 27, 2015
- Potential corporate obligations include:
  - Establishing a contact for privacy concerns
  - Deleting user information upon user withdrawal of consent for data collection, and after it has been used for its intended purpose
  - Considering whether data algorithms are potentially discriminatory.
- The proposed bill currently has no congressional sponsors.
Enforcement & Investigation: Overview

Following an investigation, the Commission may initiate an enforcement action by issuing a complaint if it has “reason to believe” that the law is being or has been violated.

Administrative Enforcement

- **Consent Agreements.** The parties may enter into a consent agreement (without admitting liability), which includes consent to entry of a final order, and waives all rights to judicial review.

- **Adjudication before an Administrative Law Judge (ALJ).** Complaints may be adjudicated before an ALJ. The ALJ’s decision is appealable to the FTC Commissioners. Final administrative decisions are appealable to the U.S. Court of Appeals. FTCA § 5.

Judicial Enforcement

- FTC can seek preliminary and permanent injunctions in federal court. FTCA § 13(b).

- Even where the Commission determines through adjudication that a practice is unfair or deceptive, the Commission must still seek the aid of a court to obtain civil penalties, consumer redress or civil penalties for violations of its orders to cease and desist.
Scope and Authority—Overview of the FTC’s Investigative and Law Enforcement Authority

- The Commission may “prosecute any inquiry necessary to its duties in any part of the United States,” FTCA § 3, and may “gather and compile information concerning, and to investigate from time to time the organization, business, conduct, practices, and management of any person, partnership, or corporation engaged in or whose business affects commerce, excepting [certain financial institutions] and common carriers . . . .” FTCA § 6(a).

- Note that pre-complaint investigations are generally non-public.
Enforcement & Investigation: The Civil Investigative Demand

- **Scope and Authority—FTC Investigations and Compulsory Process:**
  - While the FTC has the power to issue either subpoenas or civil investigative demands (“CIDs”), **the FTC must issue CIDs in consumer protection investigations** challenging unfair or deceptive acts or practices. 16 C.F.R. § 2.7.
  - Under Section 20 of the FTCA and 16 C.F.R. § 2.7, the FTC may send CIDs to third parties who are not targets. Those CIDs can include investigational hearings.
  - The FTC is not required to provide notice to targets that investigational hearings are occurring.

- **Scope of CID Broader than Subpoena**
  - Both subpoenas and CIDs may be used to obtain existing documents or oral testimony. FTCA §§ 20.
  - In addition, CIDs may also require that the recipient “file written reports or answers to questions.” FTCA § 20.
  - CIDs may require the production of tangible things. FTCA § 20.
  - CIDs may be served upon entities not found within the territorial jurisdiction of any court of the United States. FTCA § 20.
Enforcement & Investigation: The Civil Investigative Demand

- Before instituting a proceeding against a company, the Commission may issue in writing a CID “[w]henever the Commission has reason to believe that any person may be in possession, custody, or control of any documentary material or tangible things, or may have any information, relevant to unfair or deceptive acts or practices in or affecting commerce . . . .” FTCA § 20.

- A CID may require “such person to produce such documentary material for inspection and copying or reproduction, to submit such tangible things, to file written reports or answers to questions, to give oral testimony concerning documentary material or other information, or to furnish any combination of such material, answers, or testimony.” FTCA § 20.

- “Each civil investigative demand shall state the nature of the conduct constituting the alleged violation which is under investigation and the provision of law applicable to such violation.” FTCA § 20.

- The CID must allow a reasonable amount of time to produce the documents, things, reports or answers requested. 16 C.F.R. § 2.6.
Enforcement & Investigation: The Civil Investigative Demand—Responses/Objections

- **Open a Dialogue with the FTC**—Many CIDs can be successfully resolved to both parties’ satisfaction through open discussion and negotiation directly with the FTC.

- **Petitions to Limit or Quash**—“Any petition to limit or quash any . . . civil investigative demand shall be filed with the Secretary of the Commission [by the return date, or else] within twenty (20) days after service of the . . . civil investigative demand . . . . Such petition shall set forth all assertions of privilege or other factual and legal objections to the subpoena or civil investigative demand, including all appropriate arguments, affidavits and other supporting documentation.” 16 C.F.R. § 2.7.

A petition to limit or quash will be resolved by the full Commission. 16 C.F.R. § 2.10.

- *Note that while most CID-stage investigations are non-public, the Petition to Quash is a publicly available record.*

- If a party fails to comply with a CID, the Commission may file a petition in a U.S. District Court of appropriate jurisdiction for an order to enforce the CID. FTCA § 20.
Enforcement & Investigation: Penalties

- **Civil Penalties.**
  - If a respondent violates a final order, it is liable for a civil penalty of up to $16,000 for each violation. The penalty is assessed by a district court in a suit brought to enforce the Commission’s order. FTCA § 5(1).
  - Further, a court may grant such relief as it finds necessary to redress injury to consumers resulting from an unfair or deceptive practice or violation of an FTC rule, including but not limited to rescission or reformation of contracts, the refund of money or return of property, the payment of damages (except punitive damages), and public notification of the unfair or deceptive act or practice. FTCA § 19(b).

- **Preliminary and Permanent Injunctions.** The Commission may seek preliminary and permanent injunctions to remedy a violation of “any provision of law enforced by the Federal Trade Commission.” FTCA § 13(b).
  - The FTC has broadly construed its authority to obtain an order not only permanently barring deceptive practices, but also imposing various kinds of monetary equitable relief (i.e., restitution and rescission of contracts) to remedy past violations. See, e.g., *FTC v. World Travel Vacation Brokers, Inc.*, 861 F.2d 1020 (7th Cir. 1988).

- **Criminal Penalties.** The FTC may refer cases to the U.S. Department of Justice for criminal enforcement. FTCA § 16(b).
Best Practices: Litigation/Legal Holds

- **A duty to preserve arises upon receipt of a CID.**
  - *In re Napster, Inc. Copyright Litig.*, 462 F.Supp. 2d 1060, 1068 (N.D. Cal. 2006) (‘‘…duty to preserve attaches when a party should have known that the evidence may be relevant to future litigation.’’).

- **Duty may arise earlier if:**
  - You are on notice of a potential violation and have a reasonable basis to believe your materials would be relevant.

- **Preservation considerations:**
  - The legal hold applies to ‘‘evidence which [the litigant] knows or reasonably should know is relevant to the action.’’ *In re Napster*, 462 F.Supp. 2d 1060, 1067.
  - The legal hold should last as long as litigation is ‘‘probable’’ and the company has documents or other information relevant to the probable litigation. See e.g., *In re Napster*, 462 F.Supp. 2d 1060, 1068.
  - Anyone in the company with potentially relevant information, whether stored electronically or in hard copy, should receive a legal hold notice.
  - A legal hold should be periodically reissued during a lengthy action or investigation to ensure continued compliance.
Best Practices: CID Purpose and Scope

- **Ascertain reasons for CID**
  - The FTC may tell you
  - You may already know
  - This will guide and limit your search and response

- **Attempt to narrow the CID using your superior knowledge of your company’s documents and information.**

- **Options for narrowing the scope of a CID may include:**
  - Privilege
  - Overall scope (avoid a “kitchen sink” approach)
  - Cost considerations
  - Time period/date limitations
  - Corporate history issues impacting reasonable availability of documents
  - Etc.
Best Practices: Coordination of Stakeholders

- **Meet with all of the relevant stakeholders early in the process**
  - Senior management
  - Legal
  - IT
  - Vendors
  - Third parties
  - Business partners
  - Competitors

- **Joint Defense/Common Interest Agreements**
  - Third parties

- **Insurance Issues**
  - Ascertain insurance coverage immediately
  - Are voluntary steps needed to ensure coverage?
Best Practices: Production

- **e-Discovery considerations**
  - The FTC has specific formatting protocols for produced documents outlined in a “production guide”
  - Consider and discuss options for delivery of requested information to the FTC

- **Production and preservation problems**
  - Inadvertent production and clawback
  - Spoliation

- **Interrogatories**
  - Consider whether certain interrogatories may be appropriately answered with documents

- **Danger: Existing litigation**
  - Could the files you are producing affect other litigation or other ongoing investigations?
Best Practices: Confidentiality Issues

- Immediate plan to preserve attorney-client privilege wherever appropriate
  - Identify individuals with potentially privileged communications
  - Establish a privilege analysis and apply it consistently across all relevant material
  - Take adequate e-discovery steps to ensure no privileged material is inadvertently produced (e.g., run a privilege screen on collected material)
  - 16 C.F.R. 2.11 governs the treatment of protected material withheld from production to the FTC

- Other confidentiality issues may arise for documents and information concerning:
  - M & A activity
  - Other investigations
  - Third party records
  - Employee records, including personal health information

- Raise confidentiality concerns with the FTC immediately

- Always mark confidential material as such
  - Clearly identify confidential business information to protect from FOIA
Long-Term Strategy & Importance of Consistent Messaging

- Depending on the focus of the CID, receipt of the CID may be the tip of the iceberg
  - Anticipate media scrutiny
  - Potential for parallel or follow-on state attorneys general investigations
  - Plan for potential follow-on class action lawsuits
- **Craft a consistent message**
  - Craft a message with a view of your endgame, and discipline yourself to stick to that message
  - Shifting messages to address the media crisis of the moment can come back to haunt you
  - Business interest in appearing cooperative, customer-friendly and treating everyone equally may conflict with positions you will need to take later with regulators, to defeat class actions, and in potential coverage disputes with insurers
- **Close cooperation with corporate communications department is crucial**
Best Practices: Wrap Up

- **Wrap Up or Closure of the CID**
  - Agency Meeting – consider offering certain employees for interviews with FTC staff to facilitate closure
  - Agency Letter – obtain written confirmation from the FTC that its investigation has concluded
  - Further Investigation
  - Consent Decree
    - Court enforced
    - Penalties
    - Public
Speaker Contact Information

Anthony T. Pierce
Akin Gump Strauss Hauer & Feld LLP
apierce@akingump.com
202.887.4411

Catherine E. Creely
Akin Gump Strauss Hauer & Feld LLP
ccreely@akingump.com
202.887.4331

Jacqueline K. Connor
Federal Trade Commission
jconnor@ftc.gov
202.326.2844

Laura E. Jehl
Resolution Health, Inc.
ljehl@resolutionhealth.com
240.295.5834