

**Consumer Data Privacy:
Contractual Risk
Management**


John Pietila
Davis Brown Law Firm



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Consumer Privacy: Why it Matters


- **White House White Paper** (February 2012)
 - Consumer Privacy Bill of Rights
- **FTC Report** (March 2012)
- **High Profile Breaches**
 - Sony Pictures (2015)
 - Home Depot (2014)
 - JP Morgan Chase (2014)
 - Target (2013)
 - Citibank (2011)
 - Sony Playstation Network (2011)



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Consumer Privacy: Quantifying Risk

- Legal risk
- Financial risk
- Reputational risk



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Consumer Privacy: Quantifying Risk


- Security breach disclosure laws
 - Notice to affected parties
 - Notice to federal, state or local agencies
 - Credit monitoring and reporting
- Numerous state and federal laws
- International laws



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Overview


- Contract Diligence
- Contract Terms
- Contract Performance
- Specific Example: CPNI



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Diligence: Initial Assessment


- Data as an asset
- Privacy/Security Laws
 - Sector-Based Federal Laws
 - HIPAA/HITECH
 - GLBA
 - COPPA
 - FERPA
 - FACTA
 - FISMA
 - Privacy Policy and Customer Agreements
 - Regulatory Certification
 - Unfair Deceptive Practices Act (FTC and State)



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Diligence: Initial Assessment


- Technical capabilities
- Vendor-specific risk assessment
 - Unintentional breach
 - Intentional breach
 - Third party attack
 - Strength/weakness of internal security policies and controls
 - Strength/weakness of technical and physical controls
 - Knowledge, awareness or compliance gaps



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Diligence: High Level Considerations


- Is the data personally identifiable, consumer information
- Is the vendor a data broker
- Enterprise approach to compliance and risk management
 - Identifying reasonable practices
 - Identifying best practices



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Diligence: High Level Considerations


- Is the data subject to privacy/security laws
- Where (and from where) will the data be stored, accessed or processed
- Will the data be disaggregated, transformed or merged in any way
- Is the vendor subject to privacy/security laws
- What security protection will be used by the vendor
- Does the vendor have written policies and procedures in place
- What did the vendor represent in the procurement process



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.


Contract Terms: Priority Terms

- Confidentiality
 - *Personal Information or Consumer Information* as a subset of *Confidential Information*
- Limitation of Liability
 - Target data specific risks
 - Exempt breach from caps or exclusions
- Indemnification
 - Third party claims
 - Defense and control


©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.


Contract Terms: Priority Terms

- Warranties
 - What should vendor warrant or certify
 - Operationally
 - Technically
 - General or specific
 - Remedies
- Termination
 - What happens to data
 - Transition assistance


©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Terms: Common Terms

- Define vendor data use and access rights and restrictions
- Assign vendor responsibilities and risks relating to data
- Identify applicable security standards and protocols
- Address subcontracting and role of vendor employees and contractors


©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Terms: Common Terms

- Assign responsibility for data breach, reacting to breach and costs of notices and remediation
- Define requirements for data return or disposal, including security and transition assistance as vendor relationship winds down
- Define scope of audit rights and certification requirements



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Terms: Common Sticking Points

- Compliance
 - Which laws are applicable?
 - Which party will monitor compliance and coordinate any required adjustments?
 - Who pays?
- Liability
 - Are consequential damages excluded or capped?
 - Which party has responsibility and control following breach?
 - Can insurance help resolve the sticking point?



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contract Performance: Post Contract Issues

- Monitor
 - Vendor performance
 - Industry, cybersecurity and data privacy developments
 - Media coverage
- Vendor Certification
 - Coordinate scope and timing
- Audits
 - Audit security measures used by vendor or its subcontractors
 - Coordinate scope and timing



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Customer Proprietary Network Information

- Communications Act
- Shifting Emphasis (2006 FCC Declaratory Ruling)
 - Competition /Pretexting/Consumer Data Privacy
- Active Enforcement
 - Federal Communications Commission
 - Verizon Forfeiture (2014) \$7.4 M



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Federal Law

47 U.S.C. § 222(c)(1)

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: CPNI Defined

47 U.S.C. § 222(h)(1)

CPNI is defined as (A) information that relates to the quantity, technical configuration, type, destination, location and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier; except that such term does not include subscriber list information



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Exemption for SLI

47 U.S.C. § 222(h)(3)

Subscriber list information is defined as any information (A) identifying the listed names of subscribers of a carrier and such subscribers' telephone numbers, addresses, or primary advertising classifications (as such classifications are assigned at the time of the establishment of such service), or any combination of such listed names, numbers, addresses, or classifications; and (B) that the carrier or an affiliate has published, caused to be published, or accepted for publication in any directory format



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Horizontal lines for notes

Example: CPNI: Federal Law (2nd Look)

47 U.S.C. § 222(c)(1)

Except as required by law or with the approval of the customer, a telecommunications carrier that receives or obtains customer proprietary network information by virtue of its provision of a telecommunications service shall only use, disclose or permit access to individually identifiable customer proprietary network information in its provision of (A) the telecommunications service from which such information is derived, or (B) services necessary to, or used in, the provision of such telecommunications service, including the publishing of directories



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Horizontal lines for notes

Example: CPNI: Carrier Responsibilities

- Notify customers of their right to approve carrier's use or disclosure of CPNI
- Use or disclose CPNI only with customer approval or in an authorized manner
- Safeguard CPNI
- Notify law enforcement agencies if customer CPNI is breached
- Self-monitor and self-certify compliance with FCC CPNI rules



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Horizontal lines for notes

Example: CPNI: Operating Safeguards

- Establish adequate operating procedures to ensure compliance with FCC CPNI rules
- Have system for determining customer's CPNI status
- Account security and customer authentication
- Train personnel about when they are or are not authorized to use or disclose CPNI
- Identify compliance officer having personal knowledge of adequacy of carrier procedures



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Marketing Safeguards

- Supervisory review and approval of marketing campaigns
- Maintain record of marketing campaigns that use CPNI including:
 - description of campaign and companies involved
 - description of CPNI used
 - date and purpose of campaign and products or services offered



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Data Breach Notice

- Notify law enforcement agencies (LEAs) of breach as soon as practical (not less than 7 business days)
- Central reporting facility for FBI and Secret Service
- Notify customer 7 business days after notice to LEAs unless safety issue (sooner) or request by LEA (later)
- Maintain record of CPNI breaches and notifications for up to 2 years



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Carrier Certification

- Filed annually (prior to March 1) in EB Docket No. 06-36 covering prior calendar year
- Must be signed by an officer of the carrier with personal knowledge of carrier's operating procedures for adequate safeguarding of CPNI
- Must be accompanied by a statement from the carrier explaining how its operating procedures are (or are not) in compliance with FCC CPNI rules



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI: Carrier Certification

- Must include an overview of any legal or other actions taken by the carrier against data brokers
- Must include a summary of all customer complaints received in the preceding calendar year concerning unauthorized use or release of CPNI
- Should include details regarding the operating and marketing safeguards carrier has implemented and followed to comply with FCC CPNI rules



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI : Sample Terms: Compliance

Vendor shall fully comply with all applicable FCC rules and regulations governing access to and storage of customer proprietary network information ("CPNI"), as defined in 47 U.S.C. Section 222(h)(1) and 47 C.F.R. Section 64.2003(c), as amended from time to time.



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI : Sample Terms: Compliance (Alt.)

Vendor shall not, and shall ensure that its employees, subcontractors and agents do not, use or disclose CPNI in any manner that would constitute a violation of the Communications Act, the FCC CPNI Rules or any other applicable state or federal law or regulation governing the use, disclosure or privacy of CPNI. Vendor shall use or disclose CPNI only (i) to perform Services, (ii) as needed for the proper management and administration of Vendor's business functions or legal responsibilities involving Services, or (iii) as required by law.



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI : Sample Terms: Breach

In the event of a misuse or misappropriation of Confidential Information involving a CPNI data breach, Vendor shall (a) immediately notify Client of such data breach, (b) indemnify and hold harmless Client from any claims, suits or proceedings arising from or in connection with any such data breach and (c) cooperate (including with Client and law enforcement) and use its best efforts to timely resolve any alleged or actual risk or harm resulting from any such data breach.



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI : Sample Terms: Breach (Alt.)

Vendor shall notify Client as soon as practicable, but no later than seven (7) days after it is known to Vendor, or, by exercising reasonable diligence would have been known to Vendor, of any event involving the unauthorized access, use, or disclosure of CPNI in violation of this Agreement or applicable law ("Breach Event"). Vendor shall be deemed to have knowledge of a Breach Event if such Breach Event is known, or by exercising reasonable diligence would have been known, to any person, other than a person involved in the Breach Event, who is an employee, subcontractor, or agent of Vendor. Vendor will fully cooperate with Client in its investigation and remediation of any Breach Event. Vendor shall notify its employees and any agents or subcontractors with access to CPNI of Vendor's obligation to immediately notify Client of a Breach Event. Vendor will mitigate, to the extent practicable, any harmful effect that is known to Vendor resulting from any Breach Event.



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Example: CPNI : Sample Terms: Indemnification

Vendor shall indemnify, defend and hold harmless Client from and against any and all liabilities, costs, claims, suits, actions, proceedings, demands and losses (including court costs and reasonable attorneys' fees), expert witness fees, and costs of breach notification, investigation, credit protection, call center fees, and any civil monetary penalties or other fines imposed by the FCC or any other state or federal governmental authority arising from or relating to the acts or omissions of Vendor or any of its employees, subcontractors or agents in connection with Vendor's responsibilities under this Agreement.



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Take Aways

- Use good procurement practices
- Coordinate technical, business and legal diligence
- Understand your data and risks to your data
- Prioritize risky contracts/relationships
- Focus on high priority terms
- Monitor performance



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.

Contact Information

John Pietila
Davis Brown Law Firm

Phone: (515) 246-7871
Email: johnpietila@davisbrownlaw.com
Mail: 215 10th Street, Ste 1300
Des Moines, IA 50309

www.davisbrownlaw.com



©2014 DAVIS BROWN KOEHN SHORS & ROBERTS P.C.
