Trade Secrets:
Why they matter and how we can protect them

Licensing Executives Society
– Washington DC

James Pooley
July 15, 2021
Agenda

- Why They Matter
- Trade Secret Law
- Managing Trade Secrets
Industry’s primary asset is data

Source: Ocean Tomo, LLC
January 1, 2015
These valuable assets are also vulnerable

- Cyberattacks make headlines, reinforcing external threats
- Open innovation, and a modern workforce, require close management
Trade Secrets: The oldest form of IP
How Lawyers see Trade Secrets

“Real” IP

©

PATENTS

TM

Trade Secrets?

Unfair Comp?

Tort?

Labor?

Contract?

Departing employees

Non-competes
How Clients see Trade Secrets

**Assets**
- Big data/ IoT
- Market analysis
- Customer info
- Strategy for $$
- IP
- R&D

**Liabilities**
- Foreign operations
- Governance
- Risk management
- Compliance
- NDAs

- Comp. intelligence
- Comp. advantage
- Acquisitions
- Licensing
- Partners

- IT
- Lawsuits
- Government
- Cyber threats
- Employees
Increasing damage awards

- Miller v. Caterpillar (E.D.III.) $74M
- CardiAQ v. Neoasc (D. Mass) $112M
- Move v. Zillow (Wash.) $130M
- Title Source v. Housecanary (Tex.) $706M
- Epic v. Tata (W.D. Wisc.) $940M
Agenda

- Why They Matter
- Trade Secret Law
- Managing Trade Secrets
<table>
<thead>
<tr>
<th>IP Type</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patent</td>
<td>Protects specific new technological solutions</td>
</tr>
<tr>
<td>Copyright</td>
<td>Protects form of expression</td>
</tr>
<tr>
<td>Trademark</td>
<td>Protects goodwill in brand</td>
</tr>
<tr>
<td>Design</td>
<td>Protects exterior appearance of product</td>
</tr>
<tr>
<td>Trade Secret</td>
<td>Protects INFORMATION</td>
</tr>
</tbody>
</table>
What qualifies as a trade secret?

• Any information that is:
  • Secret (not generally known)
  • Has competitive value
  • Is protected by “reasonable steps”

• Skill and general knowledge are not covered

• Potentially permanent, but not exclusive
Examples of protectable secrets

- Raw data, extracted analytics, AI algorithms
- Unannounced products
- R&D, including failures and dead ends
- Information about customers and suppliers
- Information entrusted to you by your customers
- Strategic, marketing, & financial plans
Agenda

- Why They Matter
- Trade Secret Law
- Managing Trade Secrets
Management of trade secret assets

Strategic objectives of management

• Prevent loss of critical advantage
• Avoid contamination
• Comply with emerging standards
• Demonstrate “reasonable steps”

“Three may keep a secret, if two of them are dead.”
- Benjamin Franklin
Three factors for “reasonable steps”

1. **Value of the information**
   - Focus on what is most important to keep from the competition
   - Almost all secrets will eventually become known
   - Many secrets, especially business data, degrade over time

2. **Risk of loss or contamination**
   - What are the threat vectors?
   - What is the likelihood that they will come to pass?

3. **Consider mitigation measures**
   - What mitigation measures might reduce risk?
   - What do they cost (money, administration and friction)?
Risk area #1: people

Recruiting and on-boarding

- Recognize the recruiter’s dilemma: the best hire might be dangerous
- Review contracts that could constrain scope of work
- Create good record of warnings not to bring information
- Beware of groups: managers may have special responsibilities

Training

- Employees are the most common source of leaks
- Training is the cheapest form of prevention
- Effective training is continuous and varied, with tests

Termination

- Lock down access to systems, consider forensics
- Conduct a thorough exit interview
Risk area #2: processes

- **Policies**
  - Clear policies around protection of your data and respect for others’
  - Reinforce through management response to any incident
  - Pay special attention to social media policies

- **Access Controls**
  - Apply the need to know principle
  - Coordinate with HR: as positions change, access changes
  - Keep record classification systems simple

- **Endpoint controls**
  - Map where data travels and is stored: who has access and how
  - Establish procedures for use of employee-owned devices
  - Deploy robust tools for intrusion detection and response
Risk area #3: management

NDA Management

- The ubiquitous NDA gets little attention & is sometimes hidden
- It’s not a form, but a contract; it deserves negotiation
- Most problems arise from lack of execution and follow-up

International Supply Chain (esp. Asia)

- Specify your expectations for security
- Get NDAs from individuals
- Carefully track ownership issues
- Provide for penalties, get U.S. jurisdiction if possible
- Exercise audit rights vigorously

Litigation Avoidance & Control

- Trade secret litigation is costly in many ways
- Emotional issues require adult supervision
Creating a plan fit for purpose

“Audit” and “inventory” are not required
- Just know the categories of data and threats faced
- Manage to the risk, not to the rules

Central authority with distributed responsibility
- Business unit leaders perform initial assessments
- Central management must assure compliance and reviews

Regular reviews
- Threat environments are dynamic; plans need adjustment
Thank you!

Additional information:

james@pooley.com
www.pooley.com
+1 650 285 8520