Presented by:
David Beck, Viavi Solutions
Adrienne Bouleris, Emtec
Leigh Ann Buziak, Blank Rome
Justin Chiarodo, Blank Rome

# **Technology and IP Forum:** Current Trends and Best Practices in Trade Secret Protection

ACC Association of Corporate Counsel
NATIONAL CAPITAL REGION

# Setting the Stage: The Perfect Storm

1. Most Data Stored Electronically
2. Increasingly Mobile Technology, Rapidly Developing
3. Increasingly Mobile and Flexible Workforce
4. Changed Views on Public v. Private Information
5. Business is More Competitive Than Ever and Threats from Abroad

BLANKROME

# Setting the Stage: Don't Take Our Word for It

- Total Revenue Lost by U.S. Companies = $300 Billion *(Commission on the Theft of American Intellectual Property)*

- "The pace of economic espionage and trade secret theft against U.S. corporations is accelerating." *(Obama Administration "Strategy to Mitigate the Theft of U.S. Trade Secrets")*

- The loss of industrial secrets through cybercrime as the "greatest transfer of wealth in history." *(Former Director, National Security Agency, General Keith Alexander)*

BLANKROME

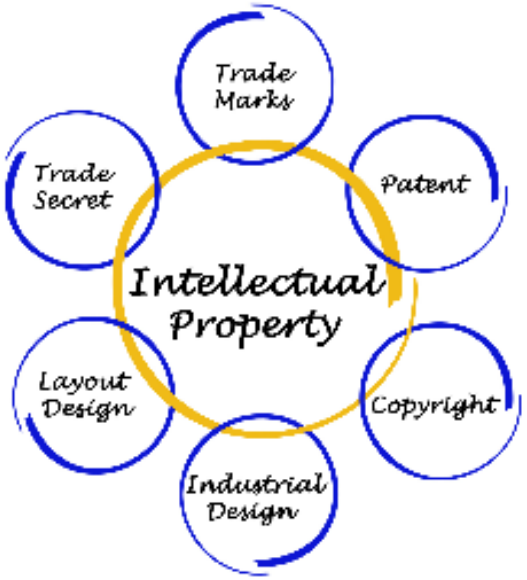
# Setting the Stage: Don't Take Our Word for It

- Former employee downloaded 14,000 files from Waymo regarding its driverless car and installed a new operating system on a computer to cover it up, taking the information to arch-competitor Uber
- Network of DuPont employees were paid off and recruited by a South Korean-based company to steal the chemical fibers that make up Kevlar
- An engineer at L-3 Communications stole thousands of electronic files regarding the design of guidance systems for missiles and rockets
- A GM employee downloaded 16,000 files pertaining to hybrid car technology, which she filtered through her and her husband's joint venture to a Chinese car company
- Three Lilly scientists were indicted for emailing information about early-stage drug development to a Chinese venture


BLANKROME

# Trade Secrets as Valuable IP

- Trade secrets may be created every day in regular business operations: R&D, marketing, strategy
- May not be protectable by other forms of IP (only 10% of innovations are patented)
- Powerful litigation tools and tactics




BLANKROME

# Trade Secrets: The Basics

# Legal Basis for Protecting Trade Secrets

- The Defend Trade Secrets Act of 2016 ("DTSA")
- Uniform Trade Secrets Act ("UTSA")
  - 48 states, MA & NY continue to follow common law or Restatement
- Residual common law torts remain (e.g., unfair competition and tortious interference with contract) where not preempted
- Criminal: Economic Espionage Act and theft statues
- Controversial: Computer Fraud and Abuse Act (Circuit split)

BLANKROME

# The Defend Trade Secrets Act of 2016

- The Defend Trade Secrets Act of 2016 ("DTSA") passed Congress with overwhelming bipartisan support and was signed by President Obama on May 11, 2016 putting the law into effect

*18 U.S.C. § 1831, et seq.*

BLANKROME

# The Basics: What are trade secrets?

- It is ***Secret***
- It is ***Valuable <u>because</u>*** it is secret
- ***Reasonable Measures*** are taken to protect it
- Technical AND business information (e.g., customer lists and marketing strategies)


BLANKROME

# The Basics: What are trade secrets?

- **Trade Secrets are <u>Broadly</u> Defined in the Statute**
- ALL Financial, business, customer, scientific, technical, economic, or engineering information
- Form: tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing
- Examples: patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes

*18 U.S.C. § 1839*


BLANKROME

# The Basics: Reasonable Measures

- Agreements (employees and third parties)
- Physical limitations on access and downloading
- Electronic limitations on access and downloading
- Mobile device management for electronic devices or ownership
- Legends and labels
- Policies and procedures
- Exit interviews and check-out procedures

- Note: failure to plead = dismissal *Raben Tire Co., LLC v. McFarland*, 2017 WL 741569 (W.D. Ky. Feb. 24, 2017); *M.C. Dean, Inc. v. City of Miami Beach, Florida*, 2016 WL 4179807 (S.D. Fla. Aug. 8, 2016)


BLANKROME

# The Basics: No Reasonable Measures

**Even if confidentiality agreements are in place, trade secret protection can be destroyed:**

- Information published to customers without agreements or warnings

  "With respect to pricing in particular, [the district court] found that "[s]ome customers which regularly place large orders may order using monthly-updated 'posted pricing,' which allows the customers to know prices on certain items in advance"; "[c]ustomer feedback reveals how competitors are pricing their products…." *Sw. Stainless, Ltd. P'ship v. Sappington*, 582 F.3d 1176, 1189-90 (10th Cir. 2009)

- Information that is widely shared internally and externally without regard to confidentiality or use outside the company

  "In practice, the contents of the Engineering Data Book were widely shared without any regard to confidentiality." *Dana Ltd. v. Am. Axle & Mfg. Holdings*, 2013 U.S. Dist. LEXIS 116899 (W.D. Mich. Aug. 19, 2013)

- Information published on the internet

  "Arkeyo made its software publicly available to individuals who owed no duty of non-disclosure to Arkeyo." *Arkeyo, LLC v. Cummins Allison Corp.*, U.S. Dist. LEXIS 100605 (E.D. Pa. June 28, 2017)

- No other limitations on employee access to the information

  "Had Arcor taken additional measures, such as limiting access to its customer information by computer password or keeping track of the hard copies of the information, we might hold otherwise. . ." *Arcor, Inc. v. Haas*, 842 N.E.2d 265, 271 (Ill. 2005)

BLANKROME

# The Basics: Reasonable Measures

- Under lock and key (perhaps literally)
- Physical vs. Electronic/Tangible vs. Intangible
  - Bad news: electronic information can be easily manipulated and taken
  - Good news: electronic information easier to track than paper because it often leaves behind an electronic fingerprint

BLANKROME

# The Basics: Options for Relief

- Injunctive relief—both preliminary and permanent
  - Early options: temporary restraining order versus preliminary injunction
  - Value of expedited discovery to securing better relief up front
- Damages—lost profits, disgorgement/constructive trust, reasonable royalties, attorneys' fees, and punitive/exemplary damages
- Referral to authorities for prosecution

BLANKROME

# The Defend Trade Secrets Act Changes Everything
## (or does it?)

# Why does the DTSA change everything? (or does it?)

- Federal Question Jurisdiction (trade secrets "related to a product or service used in, or intended for use in, interstate or foreign commerce")
- Enhanced damages (exemplary + attorneys' fees)
- State law claims where state laws provide greater trade secret protection or broader remedies that those offered by the DTSA (18 USC § 1836)

BLANKROME

# Why does the DTSA change everything? (or does it?)

- In special circumstances, companies may be able to obtain ex parte orders to seize the stolen trade secrets to avoid use and disclosure


*18 USC § 1836(b)(2)*

The seized computers installed with pirated software.

BLANKROME

# DTSA *Ex Parte* Seizure Provision

Courts will not issue if there is a belief that Rule 65 preservation orders will be effective

- ". . . the DTSA's seizure provision would only apply if seizure could not be accomplished by way of Rule 65. Obviously, in this case, Rule 65 did the trick." *Magnesia Refractories Co. v. Mishra*, 2017 U.S. Dist. LEXIS 10204 (N.D. Ind. Jan. 25, 2017)
- seizure order was "unnecessary because the Court will order that [employee] must deliver these devices to the Court at the time of the [preliminary injunction] hearing" and also ordered that the devices "may not be accessed or modified" *OOO Brunswick Rail Mgmt. v. Sultanov, 2017 U.S. Dist. LEXIS 2343 (N.D. Cal. Jan. 6, 2017)*

BLANKROME

# DTSA *Ex Parte* Seizure Provision

Courts *will* issue if there is evidence of document destruction in the past.

- "At least some of the Defendants have a high level of computer technical proficiency and there have been attempts by Defendants in the past to delete information from computers, including emails and other computer data. Further Defendants have shown a willingness to provide false and misleading information." *Axis Steel Detailing, Inc. v. Prilex Detailing Ltd. Liab. Co.*, 2017 U.S. Dist. LEXIS 221339 (D. Utah June 29, 2017)

BLANKROME

# Why does the DTSA change everything? (or does it?)

- Safe Harbor: Protects whistleblowers who disclose information in confidence to government officials or private attorneys for the purpose of reporting suspected legal violations (18 U.S.C. § 1833)
- Requires companies to "provide notice of the immunity...in any contract or agreement with an employee that governs the use of a trade secret or other confidential information" if they want the enhanced remedies under the statute (fees and exemplary damages)
- To take advantage, companies must revise confidentiality agreements to conform to the statute

BLANKROME

# Safe Harbor Sample Language

Pursuant to the Defend Trade Secrets Act of 2016, I understand that:

1. An individual may not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (a) is made (i) in confidence to a federal, state, or local government official, either directly or indirectly, or to an attorney; and (ii) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document that is filed under seal in a lawsuit or other proceeding.

2. Further, an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the employer's trade secrets to the attorney and use the trade secret information in the court proceeding if the individual: (a) files any document containing the trade secret under seal; and (b) does not disclose the trade secret, except pursuant to court order.

BLANKROME

# Safe Harbor Sample Language

**For Companies with Whistleblower Policies in Place**

I agree that, at all times during and after my employment with [EMPLOYER], I will not disclose or communicate any Confidential Information to any competitor or other third party, or use or refer to any of this information for any purpose, including but not limited to in the course of future employment for myself or any entity other than [EMPLOYER], or remove materials containing any of this information from [EMPLOYER'S] premises, except as necessary for me to properly perform services for [EMPLOYER] during my employment or as expressly authorized by and subject to the requirements of the [WHISTLEBLOWER POLICY] in [EMPLOYER'S] [POLICY DOCUMENT/HANDBOOK].

BLANKROME

# Safe Harbor Sample Language

**For Companies with NO Whistleblower Policies in Place**

I agree that, at all times during and after my employment with [EMPLOYER], I will not disclose or communicate any Confidential Information to any competitor or other third party, or use or refer to any of this information for any purpose, including but not limited to in the course of future employment for myself or any entity other than [EMPLOYER], or remove materials containing any of this information from [EMPLOYER'S] premises, except as necessary for me to properly perform services for [EMPLOYER] during my employment or as permitted by law if disclosure is made in confidence to a government official or attorney, either directly or indirectly, solely for the purpose of reporting or investigating a suspected violation of law or in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal.

BLANKROME

# Why does the DTSA change everything? (or does it?)

*Unum Grp. v. Loftus*, 2016 U.S. Dist. LEXIS 168713 (D. Mass. Dec. 6, 2016)

- Former employee attempted to seek immunity under whistleblower provision to dismiss DTSA claim at pleading stage – "My lawyer has it"
- No ruling at motion to dismiss phase where the employee had not filed suit and court was required to take allegations of complaint as true

*Christian v. Lannett Co.*, 2018 U.S. Dist. LEXIS 52793 (E.D. Pa. March 29, 2018)

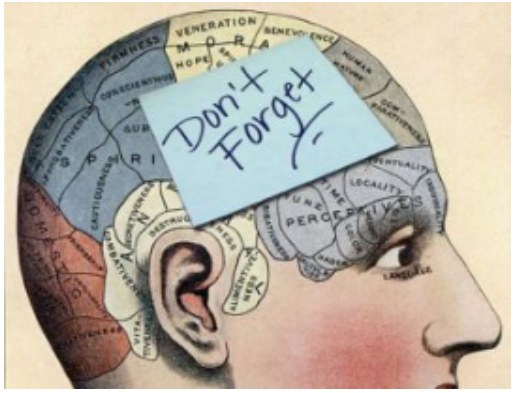
- Former employee retained 22,000 pages of documents
- Disclosing those to counsel pursuant to a discovery court order in her Title VII, ADA, FMLA suit = immunity from DTSA counterclaim

BLANKROME

# Why does the DTSA change everything? (or does it?)

- Courts cannot grant an injunction to "prevent a person from entering an employment relationship, and that conditions placed on such employment shall be based on evidence of threatened misappropriation ***and not merely on information the person knows***"

18 USC § 1836(b)(3)(A)(i)(I)




BLANKROME

# Why does the DTSA change everything? (or does it?)

- Former employee's access to "a compilation of wealthy individuals willing to consider the sorts of financial management services that FWCM provides" together with his *likely* memory of the names of clients, management fee percentage, preferences regarding risk, time horizon, how much money they invested qualified as trade secrets

- Court found that restriction on enjoining individuals for employment did not apply because "there is sufficient evidence that [employee] will use [employer's] trade secrets to develop his own business


*First Western Capital Management Co. v. Malamed*, 2016 WL 8358549 (D. Colo. Sept. 30, 2016)

BLANKROME

# Why does the DTSA change everything? (or does it?)

- First year ~200 federal court filings
- Second year ~1,134 filings
- Trend continues, 1Q, 2Q 2018 = 581


**Can you guess which state had the most original filings under the DTSA?**

BLANKROME

# Why does the DTSA change everything? (or does it?)


BLANKROME

# Why does the DTSA change everything? (or does it?)

- Who's winning? A mixed bag
  - 270 cases for Plaintiff – more than half = *consents!*
  - 334 cases for Defendants
- What are they winning? Also a mixed bag
  - Lost profits (103)
  - Punitive damages (47)
  - Royalties (7)

Lex Machina™
a LexisNexis® Company

BLANKROME

# Top Ten Things You Never Want to Hear from Your Clients (and How to Prevent Them)

"I wish we would have read his online manifesto before we hired him."

BLANKROME

# Follow a Thorough Hiring Process

- Know the basics of HR best practices
- Hire the right people for your company
- Adhere to formal hiring policies and procedures, including background check (where applicable) and thorough interview process

BLANKROME

"We forgot to mention the non-compete and non-disclosure agreements during the interview, so we just rolled the dice."

BLANKROME

# Require Restrictive Covenants

- Key evidence to show that the company has taken steps to protect its information; should be presented and enforced consistently
- Non-compete agreements
  - Enforceable through injunctive relief if reasonable in time and scope
  - Not enforceable in some states (notably, CA)
- Non-disclosure agreements
  - More common and likely more enforceable
  - Important to have third parties (vendors, contractors) sign when viewing trade secret and confidential information
  - Exhaustively define confidential information so everything is covered

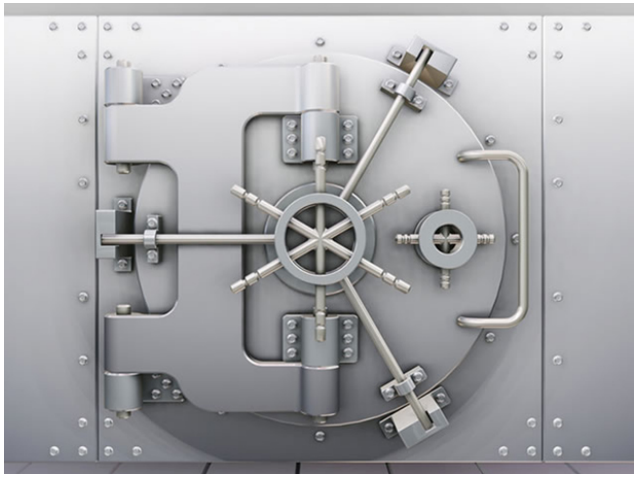
BLANKROME

"We didn't put a lock on the door to the lab because it felt. . . territorial."

BLANKROME

# Put Physical Limitations in Place

- Under lock and key, literally
- Limit physical access to areas where
- Valuable information is kept with physical security, access cards
- Signs, symbols and legends on documents



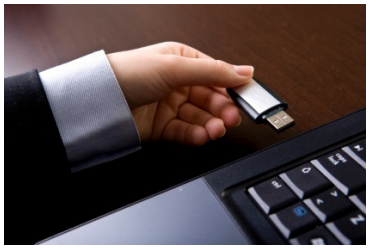

BLANKROME

“She was downloading thousands of files and I thought she was just charging her phone.”

BLANKROME

# Institute Electronic Limitations

- Most data is now kept electronically
  - Bad news: electronic information can be easily manipulated and taken
  - Good news: electronic information is easier to track than paper because it often leaves behind an electronic fingerprint
  - Electronic control of data – passwords, restrictions on use of thumb drives, mass downloading, cloud-based file sharing (Dropbox, Hightail, Google Drive), encrypted email (Hushmail)
  - Monitor and update electronic controls
  - Keystroke/mass-downloading software
  - Regular monitoring, especially in sensitive areas, and also on the Internet (Google Alerts)



BLANKROME

“He posted a link to our strategic plan on Twitter and next thing you know, all of our competitors are reading about it on Facebook and LinkedIn.”

BLANKROME

# Clearly Define Computer Use Policies

- Define confidential information, emphasize company ownership, and prohibition on outside use
  - Email policy: include that company owns email and will monitor
  - Social media/cloud storage policies: prohibit transmission of confidential information
  - Ownership of social media accounts and prohibition on use of personal accounts for official company business (i.e., require a disclaimer)
  - Internet usage policy: restricting software installation used to steal information (in addition to restricting websites prone to viruses and inappropriate material)

BLANKROME

“The iPad she used to steal all our documents wasn’t issued by the company, that was her own personal device.”

BLANKROME

# Clearly Define Mobile Device Policies

- If the company owns the issued device, the company controls the information and the device (makes life easier)
- Bring Your Own Device ("BYOD") presents other challenges and requires specific policies to secure information
  - Require passwords
  - Segregate company and personal information through use of mobile device management ("MDM") software
  - Ensure company has remote access to wipe or update company information

BLANKROME

“What do you mean exit interview? He moved to China. He’s long gone.”

BLANKROME

# Use Exit Interviews and Check-Out Procedures for Departing Employees

- Exit interviews and check-out procedures to ensure that all confidential materials are accounted for and returned upon resignation or end of engagement
- Disable electronic access immediately
- Audit data use
- Account for company devices and property
- Alert customers and vendors

BLANKROME

“None of our information is secret. You can find anything on the Internet.”

BLANKROME

# Build a Culture

- Commitment/buy-in from business people
- Treat trade secrets as trade secrets
- Publicity and marketing efforts, employee training
- Appropriate and consistent use of litigation and enforcement tools
- Protection of trade secrets integrated into company's culture and values
- Unfortunately, theft usually occurs from within—good HR policies and managers can serve as a check

BLANKROME

“Yes, we just hired her last week from our competitor. She has some great leads!”

BLANKROME

# The Golden Rule: Respect Your Competitor's Information

- Respect for competitor's IP and trade secrets
- Policies, procedures, and training
- Clear written instructions and contracts with new employees coming from competitors and with third parties who may have had access to competitors' trade secret information
- Ask about post-employment obligations during interviews and explain company's position


BLANKROME

“All of our information is valuable. If we could only find it.”

BLANKROME

# Audit Information and Policies to Ensure They Are Fully Functioning

- Work with business people to identify the information they are investing in to provide guidance on how to protect
- Work with IT to keep current with technological advances and ways employees can steal information and where and how the information is kept (information governance is the next frontier)
- Work with HR to ensure relationships are strong and lines of communication are open; ensure that policies and agreements are current and enforceable.

BLANKROME

# In Sum

- Follow a Through Hiring Process
- Require Restrictive Covenants
- Put Physical Limitations in Place
- Institute Electronic Limitations
- Clearly Define Computer Use Policies
- Clearly Define Mobile Device Policies
- Use Exit Interviews and Check-Out Procedures for Departing Employees
- Build a Culture
- Respect Your Competitor's Information
- Audit Information and Policies to Ensure They Are Fully Functioning

BLANKROME