

# Corporate Counsel

## Trade Secrets

### Civil or Criminal Enforcement of Trade Secret Misappropriation



CARLTON FIELDS  
ATTORNEYS AT LAW

Contributed by Thomas A. Dye and T. Brooks Collins,  
Carlton Fields

#### The Expanding Importance of Trade Secret Misappropriation

“The future of the nation depends in no small part on . . . the protection of intellectual property.”<sup>1</sup> It has been estimated that intellectual property in the United States is valued at nearly half of the entire economy.<sup>2</sup> The importance of trade secrets in the intellectual property arena is increasing exponentially. The number of federal trade secret cases quadrupled between 1988 and 2004, and is expected to double again within six years.<sup>3</sup> This growth is especially noticeable in the software and electronics industries that change rapidly enough to outpace the usefulness of patent protections.<sup>4</sup>

States have long provided for civil causes of action to address trade secret misappropriation. Civil enforcement alone, however, may prove insufficient at deterring trade secret theft and the far-reaching harms it causes. The costs of litigation and the difficulty of collecting on a judgment often result in the under-enforcement of trade secret theft through civil courts. Moreover, the globalization of markets has caused trade secret theft to

become a world-wide phenomenon that affects national security and nations’ economic interests—in addition to those of trade secret owners.<sup>5</sup>

The growth of technological and manufacturing industries in the United States is hindered by the mounting costs of trade secret theft. Many domestic companies rely on trade secrets to maintain their competitive advantage. These same trade secrets are also keys to creating and securing American jobs. The fact that trade secret misappropriation also undermines our national security is an even graver concern. For example, in *United States v. Cotton*,<sup>6</sup> a defendant pled guilty to stealing and attempting to deliver military trade secrets to a foreign entity. The trade secrets pertained to radar jamming, electronic countermeasures, and the ability to pin-point enemy signals during warfare. In *United States v. Chung*,<sup>7</sup> a defendant was convicted of stealing information relating to phased-array, Delta IV rockets and C-17 cargo planes.

Federal criminal prosecution supplements civil enforcement mechanisms. The expectation is that combined criminal and civil enforcement will more effectively deter trade secret misappropriation, and the far-reaching harm it causes. But the circumstances in which criminal prosecution, compared to civil action, more effectively polices trade secret misappropriation remain to be determined. This Article seeks to provide answers.

#### Discussion of Law

##### — Uniform Trade Secret Act

State-created trade secret law is relatively uniform throughout the country, as 46 states have adopted a version of the Uniform Trade Secret Act (UTSA).<sup>8</sup> Under the UTSA, a trade secret is defined as information that (1) derives independent economic value from not being generally known to, and not being readily ascertainable by proper means by, others, and (2) is subject to reasonable efforts to maintain its secrecy.<sup>9</sup> A trade secret misappropriation

Originally published by Bloomberg Finance L.P. in the Vol. 2, No. 9 edition of the Bloomberg Law Reports—Corporate Counsel. Reprinted with permission. Bloomberg Law Reports® is a registered trademark and service mark of Bloomberg Finance L.P.

This document and any discussions set forth herein are for informational purposes only, and should not be construed as legal advice, which has to be addressed to particular facts and circumstances involved in any given situation. Review or use of the document and any discussions does not create an attorney-client relationship with the author or publisher. To the extent that this document may contain suggested provisions, they will require modification to suit a particular transaction, jurisdiction or situation. Please consult with an attorney with the appropriate level of experience if you have any questions. Any tax information contained in the document or discussions is not intended to be used, and cannot be used, for purposes of avoiding penalties imposed under the United States Internal Revenue Code. Any opinions expressed are those of the author. Bloomberg Finance L.P. and its affiliated entities do not take responsibility for the content in this document or discussions and do not make any representation or warranty as to their completeness or accuracy.

claim requires: (1) the plaintiff to possess a trade secret; (2) the defendant to use or obtain the trade secret through improper means; and (3) injury to the plaintiff.<sup>10</sup>

#### – The Computer Fraud & Abuse Act

The Computer Fraud and Abuse Act (CFAA)<sup>11</sup> is aimed at deterring computer hacking-related conduct. To accomplish this goal, it imposes criminal and civil liability on persons that, without authority or exceeding authorization, access a computer and either corrupt the integrity or availability of electronic data or information, or cause an interruption of computer services.<sup>12</sup> Two subsections, 1030(a)(1) and (a)(3), apply exclusively to computers used or protected for governmental purposes.<sup>13</sup> Subsections 1030(a)(2), (a)(5), and (a)(6) are more expansive and include both private and governmental “protected computer[s].”<sup>14</sup>

In general, the CFAA applies to persons that access computers, without authorization or exceeding authorized access, and cause either harm to the accessibility or integrity of computer data, or an interruption in computer services.<sup>15</sup> Misappropriation of trade secrets, in contrast, results from the improper use of information that causes competitive injuries—not injuries to computer operations or data. Whether the CFAA can be used to ensnare trade secret misappropriators hinges on how broadly a court interprets the phrase “without authorization or exceeding authorized access.”

Some courts have found that when an authorized person uses a computer for an improper purpose—e.g., to misappropriate trade secrets—that person has exceeded his or her authorization in violation of the CFAA.<sup>16</sup> Other courts have limited the CFAA’s reach to persons who explicitly lacked authorization to access the computer in the first place, regardless of whether the actual computer use was improper.<sup>17</sup> The latter interpretation does not include trade secret misappropriation within the ambit of the CFAA unless the misappropriator harmed the computer system’s data or operations.

#### – Economic Espionage Act of 1996

The Economic Espionage Act of 1996 (EEA)<sup>18</sup> creates two distinct criminal offenses under separate sections. Both sections criminalize the knowing misappropriation or copying of a trade secret without authority, or the receipt or possession of a trade secret with knowledge that it was unlawfully obtained without authority.<sup>19</sup> The first, section 1831, requires the defendant to know that the violation would benefit a foreign governmental entity.<sup>20</sup> The second, section 1832, requires the defendant to intend to economically benefit a non-owner and to know that the misconduct will injure the owner. Under both, the misappropriated information must qualify as a trade secret under section 1839(a)(3).<sup>21</sup> The definition of a trade secret under the EEA is generally broader than the definition found in the UTSA.<sup>22</sup>

## Cost Benefit Analysis between Criminal and Civil Enforcement

### – Overarching Objectives of Trade Secret Litigation

One of the major objectives for an owner of a misappropriated trade secret is to protect the trade secret during litigation. If a trade secret is publicly disclosed during litigation, it will become less valuable and, worse, may lose its trade secret status altogether. If the security measures used to protect the trade secret and other confidential information are made available, the owner risks informing other potential misappropriators of how to circumvent the system used to protect its highly-valued information.

Another key objective in trade secret litigation is to prevent actual or threatened misuse of trade secrets. An owner must obtain a timely injunction against dissemination of the trade secret or the owner may risk loss of the trade secret’s status.

A trade secret owner must ultimately decide whether litigation will result in a net economic gain or loss. Of course, civil litigation may also provide monetary remedies. In addition, determining who will likely bear the costs of attorneys’ fees, reputational consequences, and the potential for counterclaims will help determine whether to pursue a claim through civil or criminal channels.

A trade secret owner is also interested in deterring future misappropriation. The deterrent effect on future misappropriators results primarily from the perceived probability that the wrongdoer will be discovered and held liable, and incur costs, penalties, and the stigma associated with criminal or civil liability.

Under sections 1831 and 1832 of the EEA, respectively, an individual is subject to a maximum fine of \$500,000 and a maximum sentence of 10 or 15 years, and organizations are exposed to a maximum fine of \$5 or \$10 million.<sup>23</sup> Both are exposed to potential forfeiture of property used and obtained during the violation.<sup>24</sup> Under the CFAA, criminal penalties include fines, potential imprisonment terms generally ranging from five to 20 years,<sup>25</sup> and mandated forfeiture of property used in and derived from the commission of the offense.<sup>26</sup>

For individuals and corporate entities alike, criminal penalties will likely be a harsher misappropriation deterrent. The most obvious deterrent factor is that an individual civil defendant is not subject to possible imprisonment. Civil defendants also do not risk being forced to forfeit property, and the stigma of criminal charges will assuredly be greater than that associated with an adverse civil judgment.

On the other hand, an adverse civil judgment for misappropriating highly-valued trade secrets may exceed the maximum criminal fine under the EEA or CFAA. This potential will likely be immaterial because, for all but the largest companies and wealthiest individuals, either entity will likely be rendered insolvent and unable to satisfy such a substantial judgment.

As for the probability of being identified and held liable, an owner is more likely to discover—by identifying the trade secret’s use in the owner’s marketplace—an employee’s or competing business’s misappropriation than it would be to discover misappropriation by “outsiders” or foreign entities that compete in other markets. Therefore, based on the positional and informational advantage of trade secret owners with respect to insiders and competitors, it is unlikely that criminal investigations will be better able to identify trade secret theft in these scenarios. However, as to misappropriation by “outsiders” and businesses that do not compete in an owner’s market, criminal investigations may more effectively discover acts of economic espionage. Additionally, federal investigators are uniquely capable of requiring the retention of electronic evidence held by “outsiders” within the United States and evidence held abroad by foreign entities.<sup>27</sup> This information may become a decisive factor in a trade secret trial.

#### – Cost-Benefit Analysis Factors

##### – Speed

To prevent the devaluation of a trade secret, an injunction is often needed early in civil litigation to prevent actual or threatened misappropriation. The most important showings needed to obtain both types of injunctions under Rule 65 of the Federal Rules of Civil Procedure (FRCP) are, likelihood of suffering irreparable harm in the absence of the injunction, and, likelihood of success on the merits.<sup>28</sup> These may be difficult hurdles to clear in the early stages of a civil or criminal action, especially when the exact identity and location of the expected misappropriators are unknown.<sup>29</sup>

The less expedient option, requiring notice to the party being enjoined, is to obtain a preliminary injunction under Rule 65(a).<sup>30</sup> Rule 65(b) does not require notice and allows a plaintiff to almost instantaneously obtain a temporary restraining order against misappropriation. But Rule 65(b) can only be used in limited circumstances.<sup>31</sup> The movant must show that misappropriation will cause immediate and irreparable harm before the opposing party can be heard in opposition,<sup>32</sup> and notice will only be excused where the party is unknown or cannot be contacted in time for a hearing.<sup>33</sup>

In criminal proceedings, section 1836 of the EEA empowers the Attorney General to bring civil actions to obtain “appropriate injunctive relief” in parallel with criminal prosecution<sup>34</sup>—this injunctive power is analogous to that available under Rule 65. In contrast, the CFAA provides no procedure for injunctive relief in criminal prosecutions.

##### – Protection of Trade Secrets and Security Measures During Litigation

Rule 26 of the FRCP governs civil discovery and entitles trade secret owners to protective orders prohibiting or limiting disclosure of trade secrets and other confidential information.<sup>35</sup>

Obtaining a protective order requires weighing the evidentiary need for disclosure against the harm disclosure may cause the party claiming the information’s confidential status.<sup>36</sup>

Section 1835 of the EEA is the criminal counterpart to Rule 26.<sup>37</sup> Its purpose is to encourage trade secret owners to cooperate in criminal prosecutions, and it is intended to be applied in a fashion similar to Rule 26.<sup>38</sup> The CFAA, however, does not specifically limit disclosure of confidential information during criminal prosecution. Even so, evidence of a valid trade secret is not required under the CFAA, nor is it needed to prove an attempt or conspiracy under either federal act. As such, when pursuing these claims, trade secret information will only be of limited relevance, and can often be shielded from disclosure even if not specifically protected.<sup>39</sup>

In addition to trade secret information itself, evidence describing the security measures taken to maintain the confidential information’s secrecy must be introduced to prove its status as a trade secret under the EEA and UTSA.<sup>40</sup> Disclosure of a company’s confidentiality policies and practices is unlikely to put the company’s confidential information at risk. However, evidence describing physical and electronic security measures provides wrongdoers with the blueprint needed to design ways to breach the company’s protective systems. In effect, disclosing these security measures is equivalent to disclosing the confidential information itself. Accordingly, the justifications for protecting trade secrets under Rule 26(c)(1)(g) and section 1835 apply with equal force to these types of secrecy measures, and these provisions can likely be utilized to limit public disclosure.

##### – Damages, Expenses, Potential Counterclaims, and Management Distraction

The UTSA provides for compensatory damages and, in the case of willful conduct, attorneys’ fees and punitive damages of up to twice the amount of actual damages.<sup>41</sup> The CFAA limits recovery to compensatory damages.<sup>42</sup> However, compensatory damages under the two statutes apply to different types of harm. The UTSA relates to harm caused by improperly obtaining or using information, whereas the CFAA applies to harm to the integrity of electronic data or interruptions in computer services.<sup>43</sup> Therefore, in situations where the misappropriator, without authority, accesses and harms a computer system or its data, the CFAA may allow for greater monetary recovery than the UTSA. Outside of this scenario, however, the CFAA can prove unwieldy in recovering compensation for competitive harms.<sup>44</sup>

Criminal prosecution does not allow an aggrieved owner to collect damages. Even though criminal prosecution does not displace an owner’s available civil remedies, as a practical matter, criminal fines may leave the defendant judgment-proof in subsequent civil actions. Criminal prosecutors do not allow for counterclaims to be filed against a trade secret owner. In civil suits, however, an alleged misappropriator will have available a wide range of potential counterclaims against a plaintiff. Counterclaims can be especially troublesome issues in trade secret suits between employers and employees.

Attorneys' fees contribute significantly to the costs of trade secret litigation. By shifting attorney fees onto the government, criminal prosecution allows the public interest to be vindicated regardless of whether civil litigation is economically viable for a trade secret owner.

Although both forms of enforcement consume the attention of employees and officials of corporate trade secret owners, criminal prosecution offers a far less burdensome enforcement method. As in civil suits, subpoenas to testify and requests for documents may be served on non-parties to criminal prosecution.<sup>45</sup> However, witness depositions in criminal proceedings are only allowed where justice requires that testimony be preserved for use at trial.<sup>46</sup> Thus, where discovery expenses are likely to be significant, criminal prosecution may provide an edge.

#### – *Likelihood of Success*

In predicting success rates of criminal and civil trade secret actions, the different burdens of proof loom large. Criminal conviction requires proof beyond a reasonable doubt, whereas civil liability only requires a plaintiff to prove its claim by a preponderance of the evidence.

Additionally, the mens rea required to violate the UTSA differs from the heightened requirements in the EEA and the CFAA. Both the EEA and UTSA only require that a person acquire, disclose, or derive a trade secret with knowledge or reason to know that it was improperly obtained.<sup>47</sup> But the EEA additionally requires the defendant to have, under section 1831, knowledge that the trade secret offense will benefit a foreign entity or, under section 1832, intent to economically benefit a non-owner and knowledge that the owner will be injured.<sup>48</sup> This distinction relates primarily to the result sought by the wrongdoer. The CFAA generally requires intentionally accessing or causing harm to certain computers.<sup>49</sup>

In other respects, the EEA and CFAA may make it easier to prevail. A valid trade secret is not a required element under the CFAA. Nor is it required to prove a conspiracy or attempt under the EEA or the CFAA. Along the same lines, the UTSA does not include inchoate offenses; it requires a person to have actually received, used, or possessed a trade secret knowing that it was originally obtained improperly.

#### – *Potential Reputation Issues*

Many owners fear that a reputation for aggressively pursuing employees for trade secret misappropriation will discourage future job applicants, increase employee turnover, and lead to a more hostile workplace. Generally, most employees support legal actions against employees that have willfully misappropriated trade secrets that have significant value to their employer. However, as the frequency of actions increases, and the severity of the challenged conduct decreases, employees begin to resent the hyper-litigious employer. This resentment will result from either form of enforcement because, although a non-party to a

criminal prosecution, employees will suspect that an employer is instigating or at least assisting too-frequent trade secret prosecutions.

#### – *Third-Party Factors*

Third-parties—e.g., vendors, potential customers, manufacturers—may view a company that is regularly mired in trade secret litigation as vulnerable to economic espionage. Third-parties that interact with a trade secret owner may fear that their confidential information and communications will be readily susceptible to the gauntlet of dangers posed by economic espionage.

Where misappropriation is carried out by persons outside the country or foreign entities, however, criminal prosecution is likely more appropriate. The broad powers given to federal law enforcement will likely be needed to investigate, enjoin, and prosecute this type of misconduct.

A company can avoid only some of the publicity associated with being a party to a civil trade secret suit. Likewise, the CFAA provides specific protections against the disclosure of a trade secret owner's identity. Section 1835 of the EEA, however, may allow trade secret owners to hide from adverse public exposure by using generic designations when referencing a company-owner.<sup>50</sup>

#### Conclusion

There are advantages to both civil and criminal trade secret enforcement. Civil enforcement will generally provide more litigation control and speed than criminal enforcement in trade secret cases where national interests are not implicated and international violators are not involved. This is especially true in the common litigation scenario between an owner and its employees.<sup>51</sup> If litigation costs prohibit an owner from bringing suit, criminal prosecution may likely be the only option. Criminal prosecution also provides the benefits of shifting the costs of litigation and investigation to the government, the special investigation tools of law enforcement, the threat of imprisonment, avoidance of exposure to discovery directed at owner, and counterclaims.

Where misappropriation is carried out by persons outside the country or foreign entities, however, criminal prosecution is likely more appropriate. The broad powers given to federal law

enforcement will likely be needed to investigate, enjoin, and prosecute this type of misconduct. In this scenario, criminal prosecution acts as a necessary deterrent to the misappropriation of trade secrets that provide a foundation to our nation's security and economy.

*Thomas A. Dye is a shareholder in the West Palm Beach, Florida office of Carlton Fields. Carlton Fields serves business clients through 300 lawyers in six Florida cities and Atlanta. Mr. Dye is an experienced trial lawyer handling complex commercial, intellectual property, insurance, tax, telecommunications, and consumer class action cases. Mr. Dye litigates claims related to trade secrets, covenants not to compete, trademark, copyright infringement, breach of fiduciary duty, interference with business relationships, unfair competition and related business torts.*

*T. Brooks Collins was a summer associate at the law firm of Carlton Fields.*

<sup>1</sup> Rockwell Graphic Sys., Inc. v. DEV Indus., Inc., 925 F.2d 174, 180 (7th Cir. 1991).

<sup>2</sup> David S. Almeling, et al., A Statistical Analysis of Trade Secret Litigation in Federal Courts, 45 Gonzaga L. Rev. 291, 292 (2010) (citing Robert J. Shapiro & Kevin A. Hassett, USA for Innovation, The Economic Value of Intellectual Property 3-8 (2005)).

<sup>3</sup> *Id.* at 293, 302.

<sup>4</sup> See 1 Melvin F. Jager, Trade Secrets Law § 1.1 (2008) (stating that "trade secrets have gained importance because, in many fields, the technology is changing so rapidly that it is outstripping the existing laws intended to encourage and protect inventions and innovations").

<sup>5</sup> See generally H.R. Rep. No. 104-788 at 1-2 (1996), reprinted in 1996 U.S.C.A.N. 4021, 4025 ("The ever increasing value of proprietary economic information in the global and domestic marketplaces, and the corresponding spread of technology, have combined to significantly increase both the opportunities and motives for conducting economic espionage").

<sup>6</sup> U.S. v. Cotton, Case No. CR S-08-0042-EJG (E.D. Cal. Feb. 29, 2008).

<sup>7</sup> U.S. v. Chung, Case No. SACR 08-00024-CJC (C.D. Cal. 2008).

<sup>8</sup> Uniform Trade Secrets Act § 1(1) (1985).

<sup>9</sup> See UTSA § 1(4).

<sup>10</sup> See 54A Am. Jur. 2d Monopolies and Restraints of Trade § 1071 (2011).

<sup>11</sup> The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, *et seq.* (2011).

<sup>12</sup> See Orbit One Comm'n, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385-86 (S.D.N.Y. 2010).

<sup>13</sup> See 18 U.S.C. §§ 1030(a)(1) (accessing a computer, and obtaining and transmitting information related to national defense), 1030(a)(3) (accessing and harming a computer used by or for the U.S. government).

<sup>14</sup> See 18 U.S.C. §§ 1030(a)(2), (a)(5)(C) (accessing a protected computer and, resultantly, harming or obtaining certain information from the protected computer), 1030(a)(5)(A)-(B) (transmitting a program to harm a protected computer), 1030(a)(6) (trafficking passwords to access computers used in commerce or used by or for the U.S. government); see also 18 U.S.C. § 1030(e)(2)(A)-(B) (defining "protected computer" as a computer (A) "exclusively for the use of a financial institution or the United States Government, or, . . . a computer . . . used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use"; or (B) "which is used in or affecting interstate or foreign commerce or communication").

<sup>15</sup> See Orbit One, 692 F. Supp. 2d at 385-86.

<sup>16</sup> See, e.g., International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582-84 (1st Cir. 2001); Hub Group, Inc. v. Clancy, No 05-2046, 2006 BL 11696 (E.D. Pa. Jan. 25, 2006).

<sup>17</sup> See, e.g., U.S. v. Nosal, 642 F.3d 781, 786-87 (9th Cir. 2011); Nexans Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 562-63 (2d Cir. 2006); Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 964-68 (D. Ariz. 2008); Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d 704, 709-11 (N.D. Ill. 2008); Diamond Power Intern., Inc. v. Davidson, 540 F. Supp. 2d 1322 (N.D. Ga. Oct. 1, 2007); Lockheed Martin Corp. v. Speed, 81 U.S.P.Q.2d

1699 (M.D. Fla. Aug. 1, 2006); Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A., 267 F. Supp. 2d 1268, 1324 (S.D. Fla. 2003).

<sup>18</sup> The Economic Espionage Act of 1996, 18 U.S.C. § 1831, *et seq.* (2011).

<sup>19</sup> See 18 U.S.C. §§ 1831(a)(1)-(3), 1832(a)(1)-(3).

<sup>20</sup> See 18 U.S.C. § 1831(a).

<sup>21</sup> See 18 U.S.C. § 1839(a)(3).

<sup>22</sup> See U.S. v. Hsu, 155 F.3d 189, 196 (3d Cir. 1998) ("[T]he EEA protects a wider variety of technological and intangible information than current civil law. Trade secrets are no longer restrictive to formulas, patterns, and compilations, but now include programs and codes, 'whether tangible or intangible, and whether or how stored.'") (quoting 18 U.S.C. § 1839(a)(3)).

<sup>23</sup> 18 U.S.C. §§ 1831(a), 1832(a).

<sup>24</sup> See 18 U.S.C. § 1034.

<sup>25</sup> See generally 18 U.S.C. § 1030(c)(1)-(4). But see 18 U.S.C. § 1030(c)(4)(F) (allowing life imprisonment for an offender that knowingly or recklessly cause, or attempts to cause, death from the conduct in violation of subsection (a)(5)(A)); 18 U.S.C. § 1030(c)(4)(G) (imposing a maximum one-year imprisonment an offense or attempted offense of subsection (a)(5) that does not have a specifically prescribed penalty in subsection (c)).

<sup>26</sup> 18 U.S.C. § 1030(h).

<sup>27</sup> See generally Mark L. Krotoski, Identifying and Using Electronic Evidence Early to Investigate and Prosecute Trade Secret and Economic Espionage Act Cases, 57 U.S. Attys. Bulletin 42, at 46-49 (Nov. 2009).

<sup>28</sup> Fed. R. Civ. P. 65; see also Winter v. Natural Resources Defense Council, Inc., 129 S. Ct. 365, 374 (2008) (outlining the four requirements to obtain a preliminary injunction).

<sup>29</sup> See generally Mark L. Krotoski, Common Issues and Challenges in Prosecuting Trade Secret and Economic Espionage Act Cases, 57 U.S. Attys. Bulletin 1, at 12-13 (Nov. 2009) (outlining the difficulties of reactionary investigations into trade secret theft where the defendant may be fleeing the country in a matter of hours).

<sup>30</sup> Fed. R. Civ. P. 65(a); see also Diamond Crystal Brands, Inc. v. Wallace, 531 F. Supp. 2d 1366, 1370 (N.D. Ga. 2008) ("Rule 65 of the Federal Rules of Civil Procedure . . . only requires that a party have notice of the motion and hearing; perfecting service on a defendant is not a prerequisite to the entry of a preliminary injunction order").

<sup>31</sup> Fed. R. Civ. P. 65 (b).

<sup>32</sup> Fed. R. Civ. P. 65 (b)(1)(A); see also Fed. R. Civ. P. 65 (b)(1)(B) (requiring the movant's attorney to certify in writing the efforts taken to give notice to the opposing party and the reasons explaining why notice should be excused).

<sup>33</sup> See Project Vote v. Madison Cnty. Bd. of Elecs., No. 1:08-cv-2266-JG, 2008 BL 216938 (N.D. Ohio Sept. 29, 2008) (listing these two situations as the only circumstances justifying an ex parte TRO).

<sup>34</sup> 18 U.S.C. § 1836.

<sup>35</sup> See Fed. R. Civ. P. 26(c)(1)(g).

<sup>36</sup> See Fed. Open Market Committee of the Federal Reserve Sys. v. Merrill, 443 U.S. 340, 362-63 (1979).

<sup>37</sup> 18 U.S.C. § 1835.

<sup>38</sup> See 18 U.S.C. § 1835.

<sup>39</sup> See Krotoski, *supra* note 29, at 17-18.

<sup>40</sup> See *id.* at 9-11.

<sup>41</sup> UTSA § 3(a)-(b).

<sup>42</sup> 18 U.S.C. § 1030(g).

<sup>43</sup> See *supra* notes and accompanying text.

<sup>44</sup> See Orbit One Comm'n, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385-86 (S.D.N.Y. 2010) (stating that the definition of "loss" and "damage" in the CFAA are inconsistent with damages flowing from the improper use of information).

<sup>45</sup> See Fed. R. Crim. P. 17(a),(c).

<sup>46</sup> See Fed. R. Crim. P. 15; U.S. v. Rich, 580 F.2d 929, 933-34 (9th Cir. 1978).

<sup>47</sup> See generally UTSA § 1(i)-(ii).

<sup>48</sup> See 18 U.S.C. §§ 1831(a), 1832(a).

<sup>49</sup> See generally 18 U.S.C. § 1030(a)(2)-(7).

<sup>50</sup> See Krotoski, *supra* note at 15.

<sup>51</sup> See Almeling et al., *supra* note 2, at 302 (finding that about 60 percent of trade secret suits relate to former employees and about 90 percent of suits are between employees/business partners).