

# Beyond Trade Secrets: Protecting Business Information in Arkansas

by Kevin M. Lemley



Information is often a firm's most valuable asset. Arkansas trade secret law has lost much of its strength to effectively protect this valuable information. Recent federal and state laws provide new methods for protecting information stored on computers. These new laws should cause a new dimension of thinking in how to protect business information. This article will focus on two of the most important new laws: (1) the Computer Fraud and Abuse Act ("CFAA"); and (2) Arkansas computer statutes.

## I. Development of Arkansas Trade Law

The Arkansas Trade Secret Act ("ATSA") was enacted in response to developments in federal trade secret law. No federal statute exists for trade secrets, and states developed trade secrets through the common law.<sup>1</sup> The Restatement of Torts tailored its approach to the actions of the plaintiff, adopting six factors to determine if information was a trade secret.<sup>2</sup> Applying these factors led to inconsistent results among jurisdictions.<sup>3</sup> The Uniform Trade Secret Act ("UTSA") was drafted in 1979 to unify trade secret law.<sup>4</sup> The UTSA focuses on the acts of the defendant in misappropriating information, supplanting the Restatement approach of focusing on the plaintiff's acts. After the American Bar Association approved the UTSA, nearly every state adopted all or part of the UTSA in their state law.<sup>5</sup>

The ATSA, adopted in 1981, largely mirrors the UTSA<sup>6</sup> and began life as a powerful tool for protecting business information. Information must be secret to qualify, but the ATSA definition of secrecy is not rigorous.<sup>7</sup> It protects against misappropriation from the party who wrongfully discloses the trade secret as well as the party who wrongfully acquires the trade secret.<sup>8</sup> The successful plaintiff can get attorney's fees and injunctive relief.<sup>9</sup> Trial courts are also required to enter protective orders to protect the information during the litigation.<sup>10</sup>

The Arkansas Supreme Court significantly altered trade secret law in *Saforo & Associates, Inc. v. Porocel*.<sup>11</sup> There the court turned solely to the Restatement factors to determine if a trade secret existed. By doing so, the court defeated the entire purpose of the UTSA, which Arkansas adopted through the ATSA.<sup>12</sup> The court later stated that each factor must be met for the information to qualify as a trade secret.<sup>13</sup> While other authors have scrutinized the court's approach,<sup>14</sup> the court has ignored these criticisms.



Now trade secrets are much harder to protect in Arkansas. Tyson<sup>15</sup> and Wal-Mart<sup>16</sup> both recently lost cases because the court held their business information did not meet the heightened standard to create a trade secret imposed in Arkansas. Smaller companies have incurred the same fate.<sup>17</sup> This information could have received protection under other federal and state laws.

## II. The Computer and Fraud Abuse Act

The CFAA is a powerful tool to protect business information in two significant respects. First, the CFAA applies with equal force to any information stored on a computer, whether or not the information is confidential.<sup>18</sup> Second, the CFAA does not require that the defendant use or misappropriate the information; the access of the information creates the cause of action.<sup>19</sup> Firms have failed to maximize protection available under the CFAA, largely in part because it is a complex law that developed for over a decade as an exclusively criminal statute. For much of its history, the CFAA only applied to government computers and financial institutions. The CFAA in its present form currently provides protection for any “protected computer,”<sup>20</sup> which includes any computer used in interstate commerce.<sup>21</sup> Any computer connected to the internet would qualify as a protected computer.<sup>22</sup>



*Kevin M. Lemley is an associate with the Allen Law Firm in Little Rock and an adjunct professor at the University of Arkansas at Little Rock School of Law.*

## A. Available Causes of Action Under the CFAA

The CFAA states, “Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator.”<sup>23</sup> While this civil remedy provision applies to the entire CFAA, certain subsections must be involved for the private right to accrue.<sup>24</sup> The conduct must involve one of the factors set forth in subsection (a)(5)(B).<sup>25</sup> The basic requirements under this subsection are (1) intentional access to a protected computer without authorization that (2) causes damages of at least \$5,000.<sup>26</sup> For clarification, I will refer to this as the Basic Claim.

Plaintiffs are not limited to the Basic Claim, but a violation of any other subsection must also include one of the factors in the Basic Claim.<sup>27</sup> Damages for the Basic Claim are limited to only economic damages.<sup>28</sup> However, the plaintiff could still get injunctive relief for a claim based solely on this conduct.<sup>29</sup> To achieve the full array of potential damages, the commercial plaintiff must establish one of the other enumerated causes of action provided in the CFAA:

(1) Unauthorized Access with Intent to Defraud. This claim is the most applicable to firms seeking to protect business information.<sup>30</sup> This subsection applies to one who:

knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than \$5,000 in any 1-year period.<sup>31</sup>

In this section, “defraud” means wrongdoing; the plaintiff does not have to prove the elements of common law fraud.<sup>32</sup>

(2) Unauthorized Taking of Data: accessing a computer without authorization and obtaining information from the protected computer if the conduct involved an interstate communication.<sup>33</sup> The access is improper if the defendant exceeded any authorized access in taking the information.<sup>34</sup>

(3) Trafficking in Computer Passwords: knowingly and with intent to defraud trafficking in any password or similar information through which a computer may be accessed without authorization if the trafficking affects interstate commerce.<sup>35</sup>

(4) Extortion: This subsection provides a cause of action when the defendant, with intent to extort any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer.<sup>36</sup>

## B. Application to Former Employees and Competitors

The CFAA is particularly powerful when a former employee takes information to a competitor because there is no secrecy requirement like the ATSA. The first reported case to make use of the CFAA in this context was *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*<sup>37</sup> Shurgard operated self-service storage facilities and maintained confidential marketing plans to identify and evaluate possible new locations.<sup>38</sup> Safeguard, a direct competi-

tor, offered employment to a high level manager of Shurgard who had access to the confidential marketing plans.<sup>39</sup> The manager copied this information and sent it to Safeguard while he was still employed at Shurgard.<sup>40</sup> The manager then quit Shurgard and joined Safeguard.<sup>41</sup> Shurgard brought suit against Safeguard alleging trade secret misappropriation but also asserted claims for violation of the CFAA.<sup>42</sup> Safeguard moved to dismiss the CFAA claim.<sup>43</sup>

The main issue before the court was whether the manager obtained the information through unauthorized access.<sup>44</sup> This was tricky because the manager did have authorization to access the information.<sup>45</sup> The court turned to the Restatement (Second) of Agency and found that, when the manager accessed the information to provide it to Safeguard, he ceased to be an agent of Shurgard and instead became an agent of Safeguard.<sup>46</sup>

Other courts have adopted this approach.<sup>47</sup> It is now well established that the CFAA applies to an employee taking information to a competitor, even if that employee was granted access to the information.

## C. Damages Under the CFAA

Meeting the \$5,000 damages requirement to bring a CFAA claim is not difficult. The loss may be aggregated over the course of the year; it does not have to occur at the instant of the violation.<sup>48</sup> Costs involved in investigating a possible CFAA violation also count toward this jurisdictional minimum, such as expert consultant fees to determine if a computer was inappropriately accessed.<sup>49</sup>

Once the minimal damages are established, the CFAA offers a variety of remedies. The costs of identifying a CFAA violation, including expert fees, can be recovered.<sup>50</sup> Plaintiffs can recover loss of business goodwill akin to trademark infringement or to upgrade the computer system.<sup>51</sup> Another key award is the value of the use of the information.<sup>52</sup> This is best illustrated by the concept of “restoring the data . . . to its condition prior to the offense.”<sup>53</sup>

The most applicable damage model should be trade secret misappropriation under the ATSA, which provides compensation for the actual loss caused by the misappropriation and the unjust enrichment enjoyed by the defendant.<sup>54</sup> CFAA claims involve the same misappropriation as an ATSA claim; the CFAA just protects a broader range of information. Moreover, the purpose of the CFAA is to deter unauthorized access. It makes no sense to permit the defendant to make the unauthorized access and then not provide adequate compensation. The only way to uphold the purpose is to fully compensate the plaintiff for any loss incurred and for any unjust enrichment conferred to the defendant.

The most significant drawback of the CFAA as compared to the ATSA is that the CFAA does not provide for an award of attorney’s fees.<sup>55</sup> The CFAA also has no provision for statutory or exemplary damages.

## D. Injunctive Relief Under the CFAA

The CFAA states that it allows for any injunctive relief or other equitable relief.<sup>56</sup> The question is whether the CFAA allows for an

injunction on use of information obtained through past violations of the CFAA. The Fifth Circuit was faced squarely with this issue but did not make a decision.<sup>57</sup> The CFAA should provide the same preliminary and permanent injunctive relief as the ATSA for the same reasons that the trade secret misappropriation damage model should apply to CFAA claims. It would defeat the purpose of the CFAA if the plaintiff could not prevent the defendant from using the information which was wrongfully obtained.

### E. Benefits of the CFAA Over the ATSA

The CFAA offers numerous benefits over the ATSA. First, and most significantly, the CFAA avoids the rigorous definition of “trade secret” adopted by Arkansas courts. There is no need to meet the heightened standard of secrecy to protect business information. Second, there is no requirement to show that the information was actually used or misappropriated. The cause of action accrues when the information is improperly accessed. Third, the CFAA provides federal jurisdiction for a dispute over the compromise of business information without meeting the requirements of diversity of citizenship jurisdiction. Any number of circumstances can make the state court forum unfavorable. However, at least one court has opined that a CFAA claim could be brought in state court as well.<sup>58</sup> Fourth, aside from attorney’s fees, the CFAA should provide the same monetary and injunctive relief as a successful ATSA claim.

Most importantly, the CFAA can provide a successful cause of action where a claim under the ATSA would fail. The firm can receive compensation for the compromise of its business information where once there was no remedy.

### III. Arkansas Computer Crime Statutes

Arkansas recently enacted a broad range of computer crime statutes.<sup>59</sup> Plaintiffs can bring a civil action for some of these computer crimes.<sup>60</sup> The two statutes most applicable to businesses are computer trespass and computer fraud. Computer trespass occurs when the defendant alters or damages any computer, computer system, network, program or data.<sup>61</sup> Computer fraud occurs when the defendant accesses a computer, computer system, or computer network to defraud, extort or fraudulently obtain property.<sup>62</sup>

For both computer trespass and computer fraud, the successful plaintiff can recover any damages sustained and the costs of suit.<sup>63</sup> “Damages” is defined broadly; “[w]ithout limiting the generality of the term, ‘damages’ shall include loss of profits.”<sup>64</sup> These statutes should not be preempted by the ATSA because they are not based on misappropriation of a trade secret.<sup>65</sup>

### Conclusion

At the time of this writing, the only Arkansas case involving the CFAA is an unreported opinion denying a motion to dismiss. No reported decisions exist discussing the Arkansas computer crime statutes. These laws will prove quite valuable to firms in the future against departing employees, competitors and third parties. Firms can protect their valuable business information beyond the limits imposed under Arkansas trade secret law.

### Endnotes:

1. Roger M. Milgrim, *Milgrim on Trade Secrets* § 1.01 (2007).
2. *Restatement of Torts* § 757, cmt b.
3. Note, Gina White, *Is the Arkansas Supreme Court Following Other Jurisdictions Down the Wrong Road in Analyzing Combination Trade Secrets?*, 25 U. Ark. Little Rock L. Rev. 407, 419 (2003).
4. Unif. Trade Secrets Act §§ 1 – 12, 14 U.L.A. 433-67.
5. White, *supra* note 3, at 421.
6. *Id.* at 426.
7. Ark. Code Ann. § 4-75-601(4).
8. Ark. Code Ann. § 4-75-601(2).
9. Ark. Code Ann. § 4-75-605.
10. Ark. Code Ann. §§ 4-75-606—4-75-607.
11. *Saforo & Associates, Inc. v. Porocel*, 337 Ark. 553, 991 S.W.2d 117 (1999).
12. Note, Brandon B. Cate, *The Failure of the Uniform Trade Secrets Act to Clarify the Doubtful and Confused Status of Common Law Trade Secret Principles*, 53 Ark. L. Rev. 687, 701-02 (2000).
13. *Wal-Mart Stores, Inc. v. P.O. Market, Inc.*, 347 Ark. 651, 667, 66 S.W.3d 620, 630 (2002).
14. *See generally* White, *supra* note 3 and Cate, *supra* note 12.
15. *Tyson Foods, Inc. v. ConAgra, Inc.*, 349 Ark. 469, 79 S.W.3d 326 (2002).
16. *Wal-Mart Stores, Inc. v. P.O. Market, Inc.*, 347 Ark. 651, 66 S.W.3d 620 (2002).
17. *Weigh Sys. South, Inc. v. Mark’s Scales & Equip., Inc.*, 347 Ark. 868, 68 S.W.3d 299 (2002).
18. 18 U.S.C. § 1030(a).



Endnotes continued on page 41

19. *Id.*
20. 18 U.S.C. § 1030(e)(2)(B).
21. *Id.*
22. *See id.*
23. 18 U.S.C. § 1030(g).
24. 18 U.S.C. § 1030(g).
25. 18 U.S.C. § 1030(g).
26. 18 U.S.C. § 1030(a)(5)(B).
27. *Fiber Systems Intern., Inc. v. Roebrs*, 470 F.3d 1150, 1157 (5th Cir. 2006).
28. 18 U.S.C. § 1030(g).
29. 18 U.S.C. § 1030(g); *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 511 (3rd Cir. 2005).
30. 18 U.S.C. § 1030(a)(4).
31. 18 U.S.C. § 1030(a)(4).
32. *United States v. Czubinski*, 106 F.3d 1069, 1078 (1st Cir. 1997)
33. 18 U.S.C. § 1030(a)(2).
34. 18 U.S.C. § 1030(a)(2).
35. 18 U.S.C. § 1030(a)(6).
36. 18 U.S.C. § 1030(a)(6).
37. *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F. Supp. 2d 1121 (W.D. Wash. 2000).
38. *Id.* at 1122-23.
39. *Id.* at 1123.
40. *Id.*
41. *Id.*
42. *Id.* at 1122.
43. *Id.*
44. *Id.* at 1124-25.
45. *Id.* at 1124.
46. *Id.* at 1125.
47. *E.g., P.C. Yonkers*, 428 F.3d 504.
48. *Creative Computing v. Getloaded.com*, 386 F.3d 930, 934 (9th Cir. 2004).

The advertisement features a blue background with a white circular graphic on the left. Inside the circle, the text reads: "Weekly Case Summaries" in large red font, followed by "A Member Benefit available @ www.arkbar.com & Arkansas VersusLaw" in black font. Below the text is a small image of a computer mouse. To the right of the circle, the text reads: "Weekly Case Summaries of the significant Arkansas Supreme Court and Arkansas Court of Appeals cases" in white font, followed by "Available online each week" and "Decisions from the previous week provided every Monday" in white font.

49. *EF Cultural Travel v. Explorica, Inc.*, 274 F.3d 577, 584 (1st Cir. 2001).
50. *Id.*
51. *Creative Computing*, 386 F.3d at 935.
52. *Four Seasons Hotels and Resorts B.V. v. Consorcio Barr, S.A.*, 267 F. Supp. 2d 1268, 1324 (S.D. Fla. 2003).
53. 18 U.S.C. § 1030(e)(11).
54. Ark. Code Ann. § 4-75-606.
55. 18 U.S.C. § 1030(g).
56. 18 U.S.C. § 1030(g).
57. *Fiber Sys. Int'l v. Roebrs*, 470 F.3d 1150, 1159 (5th Cir. 2006).
58. *Liebert Corp. v. Mazur*, 2004 WL 2095666 (N.D. Ill. 9/17/04) (unpublished).
59. Ark. Code Ann. §§ 5-401-101—206.
60. Ark. Code Ann. § 5-41-106.
61. Ark. Code Ann. § 5-41-104.
62. Ark. Code Ann. § 5-41-103.
63. Ark. Code Ann. § 5-41-106(a).
64. *Id.*
65. Ark. Code Ann. § 4-75-602(b).
66. *Nilfisk-Advance, Inc. v. Mitchell*, 2006 WL 827073 (W.D. Ark. 3/28/06) (unpublished). ■

[www.arkbar.com](http://www.arkbar.com)