South Carolina Law Review

Volume 63 | Issue 1 Article 6

Fall 2011

What Does CFAA Mean and Why Should I Care - A Primer on the Computer Fraud and Abuse Act for Civil Litigators

Shawn E. Tuma

"WHAT DOES CFAA MEAN AND WHY SHOULD I CARE?"—A PRIMER ON THE COMPUTER FRAUD AND ABUSE ACT FOR CIVIL LITIGATORS

Shawn E. Tuma*

"Every battle is won before it is ever fought."[1]

---

*Partner, Britton Tuma, PLLC, Plano, Texas. Website: www.brittontuma.com. B.A., Northwestern State University, *with honors*; J.D., Regent University School of Law, *magna cum laude*. The author would like to thank his wife Rachel and five children, Katherine, Seth, Andrew, Christopher, and Clara for their loving support and understanding during the preparation of this Article.

1. WALL STREET (Twentieth Century Fox Film Corp. 1987). Movie character Gordon Gekko attributes this quote to the ancient Chinese military general, strategist and philosopher, Sun Tzu in his writing, *The Art of War*. A Google search reveals that many people believe the saying is a direct quotation from Sun Tzu. The author, however, has read several translations of Sun Tzu's *The Art of War* and has been unable to find that statement in any of those translations. Moreover, one Chinese scholar, who has written a book entitled *The Art of War Applied to Wall Street*, proposes that Sun Tzu never made this statement. Y.K. Wong, *Art of War Is So Boring I Could Never Finish Reading It*, ART OF WAR ON WALLSTREET BOOK STATUS & DISCUSSION (May 19, 2010, 4:11 PM), http://www.artofwaronwallstreet.com/wordpress/?p=20.

I. INTRODUCTION

Business and warfare are one and the same.[2] That, we were told in the '80s by Gordon Gekko, and, after all, the object is the same: to win—to defeat your enemy. Borrowing from the lessons of a true warrior, he further elucidated that the key to winning was to plan ahead and think about the strategy before entering the battle, because "[e]very battle is won before it is ever fought."[3] Gekko attributed this to the lessons of Sun Tzu, who indeed taught that preparation is the key to winning:

> Now the general who wins a battle makes many calculations in his temple before the battle is fought. The general who loses a battle makes but few calculations beforehand. Thus do many calculations lead to victory, and few calculations to defeat: How much more do no calculation at all pave the way to defeat! It is by attention to this point that I can foresee who is likely to win or lose.[4]

Regardless of the source, the principle remains the same and is, almost without fail, a truism that applies equally to war, business, and litigation. Preparation is the key to winning.

In today's business environment, businesses are in a perpetual state of warfare. Competition is the essence of business.[5] Honest competition is beneficial, as it drives efficiency and innovation. Unfortunately, dishonest competition is not. Corporate espionage, corporate sabotage, and corporate theft have become part of the business landscape as well; those that cannot prevail through honorable means of competition often resort to dishonorable means to

---

2. *See* WALL STREET, *supra* note 1 (likening the business environment to "trench warfare").
3. *Id.*
4. SUN TZU, SUN TZU ON THE ART OF WAR: ARMED SERVICES EDITION 12 (Lionel Giles trans., Dover Publ'ns, Inc. 2002) (1910).
5. *See* Donald C. Dowling, Jr., *A Contract Theory for a Complex Tort: Limiting Interference with Contract Beyond the Unlawful Means Test*, 40 U. MIAMI L. REV. 487, 508 (1986).

take customers, employees, and information.[6] This has become a way of life in business and is frequently being accomplished through the use of computers to commit dishonest acts of deception, i.e., computer fraud.[7] The risks are certainly not limited to only those from corporate competitors. They also come from others engaged in computer fraud—thieves, hackers, anarchists, and inquisitive amateurs—who all pose a significant risk, and whose weapon of choice is also the computer.[8] Computer fraud is a rapidly growing threat to businesses.[9]

Accepting as true the analogy between warfare and business, if the businesses are the nation-states, who other than the litigator takes to the battle field as their commanding general? Conflict—whether waging, avoiding, or resolving—is the litigator's craft. Whether one admits it or not, on a daily basis, many businesses are engaged in a battle for their very existence. While the battlefields still remain, in large part, the courtrooms across the nation, both the nature of the war and the weapons used have evolved to incorporate computers and computer fraud at every level.[10] For litigators to be most effective, they must have a familiarity and comfort with all of the available weapons for these battles. If these businesses' litigators—their generals—are not prepared for the battle, then who is?

The purpose of this Article is to alert litigators to the need to be prepared for this new kind of battle and to provide them with sufficient information to begin this preparation. This Article first explains why litigation attorneys need to understand the growing threats their clients face from computer fraud and encourages them to recognize the need to develop an understanding of these issues by preparing for them in advance. Second, it provides a primer of the most frequently used weapon for addressing computer fraud, the Computer Fraud and Abuse Act (CFAA).[11] This will allow the litigator to be better prepared for the inevitable computer fraud battles that lie ahead, as well as to advise clients on how to avoid violating these laws, and, when necessary, use them when those clients have been victimized by the computer fraud of others or have been accused of fraud themselves.

---

6. *See* SHANE W. ROBINSON, SANS INST., CORPORATE ESPIONAGE 201 (2007), *available at* http://www.sans.org/reading_room/whitepapers/engineering/corporate-espionage-201_512.

7. *See id.*

8. *See* Marc D. Goodman & Susan W. Brenner, *The Emerging Consensus on Criminal Conduct in Cyberspace*, 10 INT'L J.L. & INFO. TECH. 139, 142 (2002).

9. Michael Edmund O'Neill, *Old Crimes in New Bottles: Sanctioning Cybercrime*, 9 GEO. MASON L. REV. 237, 238 (2000).

10. *See* Natasha Solce, *The Battlefield of Cyberspace: The Inevitable New Military Branch—The Cyber Force*, 18 ALB. L.J. SCI. & TECH. 293, 295 (2008) ("[C]yberspace is also a new global battlefield that encompasses households, corporations, universities, governments, militaries, and all categories of critical infrastructures.").

11. *See* Catherine M. Sharkey, *Trespass Torts and Self-Help for an Electronic Age*, 44 TULSA L. REV. 677, 693–95 & n.92 (2009) (noting the expansive reach of CFAA and quoting one practitioner stating that CFAA "is fast becoming one of the most expansive and potent civil statutes in a civil litigator's arsenal" (quoting Nick Akerman, *CFAA Resembles RICO*, 27 NAT'L L.J. 13, 13 (Aug. 29, 2005))).

Because the focus of this Article is on computer fraud in a civil context, its emphasis is on those aspects of the CFAA that are most likely to be at issue in civil litigation. The Article will therefore be limited to a discussion of certain relevant civil remedies under the CFAA, and some of the frequently litigated CFAA issues. There exists a significant body of scholarly work on the criminal aspects of computer fraud; this Article is not intended to overlap into that area.

II. LITIGATION ATTORNEYS MUST UNDERSTAND THE NEED TO BE PREPARED FOR THE COMPUTER FRAUD ISSUES THEIR CLIENTS WILL FACE

A. *"Everything has a computer in it nowadays."*[12]

Is that statement clear enough? "Everything has a computer in it nowadays."[13] One cannot doubt that we are now fully in the Computer Age. There is no going back.

The Computer Age was born with little notice during the first half of the twentieth century.[14] By the end of the century, however, computers had become so prevalent that many feared that a computer programming glitch would cause computers around the world to shut down or malfunction at midnight, December 31, 1999, and bring modern society to a crashing halt.[15] Fortunately, "Y2K" came and went with little impact,[16] and society has now made it past the first decade of the twenty-first century. Computers now dominate nearly every aspect of our lives.[17] This trend will likely continue until something comes along to replace the computer. If you do not accept this premise, watch the video *Did You Know?*[18] The video was prepared by Sony BMG Music Entertainment and was shown at its annual Global Management Meeting in May 2008.[19] Some say that computer technology is the wave of the future. Not even close. It is a tsunami, and there is nothing anyone can do to stop it. Preparation is the key.

---

12. United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011) (internal quotation marks omitted) ("Steve Wozniak, co-founder of Apple Computer, recently mused: 'Everything has a computer in it nowadays.'" (quoting Mark Milian, *Apple's Steve Wozniak: 'We've Lost a Lot of Control,'* CNN, (Dec. 8, 2010, 12:16 PM), http://www.cnn.com/2010/TECH/innovation/12/08/steve.wozniak.computers/index.html)).

13. *Id.* (internal quotation marks omitted).

14. *See* Irving S. Reed, *The Dawn of the Computer Age*, 69 ENGINEERING & SCI., no. 1, 2006, at 7, 7, *available at* http://calteches.library.caltech.edu/4159/1/Computer.pdf.

15. Shawn E. Tuma, *It Ain't over 'Til...A Post-Y2K Analysis of Y2K Litigation & Legislation*, 31 TEX. TECH L. REV. 1195, 1199 (2000).

16. *Id.* at 1196.

17. *See* Scott J. Shackelford, *From Nuclear War to Net War: Analogizing Cyber Attacks in International Law*, 27 BERKELEY J. INT'L L. 192, 200 (2009).

18. *Did You Know?*, YOUTUBE (May 27, 2009), http://www.youtube.com/watch?v=cL9Wu2kWwSY.

19. Karl Fisch, *Did You Know?—Music Industry Remix*, THE FISCHBOWL (Aug. 19, 2008, 8:02 PM), http://thefischbowl.blogspot.com/2008/08/did-you-know-music-industry-remix.html.

Many nations are already convinced of this and have prepared their armies for war on the cyber battlefield.[20] The world's militaries have used computers for decades, and they are an integral component of virtually all modern military systems.[21] Despite this fact, society has now taken another quantum leap forward. The close of the first decade of the New Millennium saw a formal change in the art of warfare that, for the first time in history, moved the battlefield from the physical to the cyber arena. One needs little imagination to suspect that the world's militaries have been engaged in cyber warfare for as long as computers have been in use; however, it had not become official. The year 2010 saw the first weaponized computer virus used to hamper Iran's nuclear ambitions.[22] Though people knowledgeable of cyber warfare have expected such a cyber attack for years,[23] it has finally happened: Stuxnet.[24]

The Stuxnet virus has been called "the most sophisticated cyberweapon ever deployed."[25] Stuxnet was a computer worm designed to use a variety of "previously seen individual cyber attack techniques, tactics, and procedures, automate[] them, and hide[] its presence so that the operator and the system have no reason to suspect that any malicious activity is occurring."[26] Stuxnet was so sophisticated that it was designed to eliminate all traces of its existence.[27] This is a serious weapon.

We are well over half a century into the Computer Age and we have seen the first change from the physical battlefield to the cyber battlefield.[28] This is the first time since the dawn of mankind that battles have been fought somewhere other than on an actual battlefield—now in cyberspace.[29] While no nation has claimed responsibility for the Stuxnet attack on Iran, and no one knows for

---

20. Solce, *supra* note 10, at 297 (citing John Christensen, *Bracing for Guerrilla Warfare in Cyberspace*, CNN.com (Apr. 6, 1999), http://www.thetruthseeker.co.uk/oldsite/print.asp?ID=1015).

21. *See* Solce, *supra* note 10, at 295.

22. *See* Ed Barnes, *Mystery Surrounds Cyber Missile that Crippled Iran's Nuclear Weapons Ambitions*, FOX NEWS (Nov. 26, 2010), http://www.foxnews.com/scitech/2010/11/26/secret-agent-crippled-irans-nuclear-ambitions/ (describing how the Stuxnet worm attacked Iran's nuclear program); Paul Marks, *Why the Stuxnet Worm Is Like Nothing Seen Before*, NEW SCIENTIST (Jan. 18, 2011, 2:16 PM), http://www.newscientist.com/article/dn19504-why-the-stuxnet-worm-is-like-nothing-seen-before.html (describing how the Stuxnet virus was the first of its kind).

23. *See* Marks, *supra* note 22.

24. *Id.*

25. William J. Broad et al., *Israel Tests Called Crucial on Iran Nuclear Setback*, N.Y. TIMES, Jan. 16, 2011, at A1; *see also* Barnes, *supra* note 22 (Stuxnet "is a military weapon" (stated Eric Byles, "a computer security expert").

26. Chloe Albanesius, *Stuxnet Worm Could Devastate Critical Systems, Experts Say*, PC MAG (Nov. 18, 2010, 12:27 PM), http://www.pcmag.com/article2/0,2817,2372952,00.asp (quoting Sean P. McGurk, acting director of the Homeland Security Department's Cybersecurity Center).

27. Barnes, *supra* note 22.

28. *Id.*

29. *Id.*

sure,[30] many experts believe it was a joint operation led by the United States and Israel, with help from Germany, and perhaps others.[31]

As Stuxnet has shown, over the past year, warfare has changed. There is a new weapon that has, at least on one occasion, replaced missiles, bombs, and ground troops: computers. Now, in the wake of Stuxnet, some security experts have begun to express fear that the attack has "legitimized a new form of industrial warfare, one to which the United States is also highly vulnerable."[32] Just as the United States is vulnerable, so too are businesses within the United States and around the world.[33]

Just as the computer is increasingly becoming the weapon of choice for warfare, so too has it in business warfare.[34] Computers are being used for corporate espionage (manipulating and stealing data), corporate sabotage (stealth attacks through computer viruses), or any number of other methods of attacking enemies' (competitors') strengths or exploiting their weaknesses, including old fashioned theft.[35] In one recent study, a computer security firm found that 65% of people worldwide have been the victim of some type of cyber crime.[36] This rate has increased nearly 10% from a 2003 study that found that 56% of businesses had "reported some form of unauthorized use of their computer system."[37] While many of the illicit tactics that businesses use to attack each other are often classified as crimes and punishable by criminal law,[38] in the civil

30. Marks, *supra* note 22.

31. *See, e.g.*, Barnes, *supra* note 22 (citing one commentator opining that "the most likely confederates [were] the United States, because it has the technical skills to makes the virus, Germany because reverse-engineering Siemen's product would have taken years without it, and Russia, because of its familiarity with both the Iranian nuclear plant and Siemen's systems"); Broad et al., *supra* note 25 ("[T]he operations [at the Dimona complex in Israel], as well as related efforts in the United States, are among the newest and strongest clues suggesting that the [stuxnet virus] was designed as an American-Israeli project to sabotage the Iranian program.").

32. Broad et al., *supra* note 25, at A16.

33. *See* David Gerwitz, *Digital Defense: The Coming Cyberwar*, 14 J. COUNTERTERRORISM & HOMELAND SECURITY INT'L no. 3 (Aug. 2008), *available at* http://www.computingunplugged.com/tocs/issue200808.html (discussing the vulnerability of businesses to attacks even from other "legitimate" businesses).

34. *See* ROBINSON, *supra* note 6, at 2.

35. *See generally id.* (describing various methods used to steal or sabotage electronic data).

36. SYMANTEC CORP., NORTON CYBERCRIME REPORT: THE HUMAN IMPACT 29 (2010), *available at* http://us.norton.com/content/en/us/home_homeoffice/media/pdf/cybercrime_report/Norton_USA-Human%20Impact-A4_Aug4-2.pdf.

37. Harold E. Davis & Robert L. Braun, *Computer Fraud: Analyzing Perpetrators and Methods*, THE CPA J., July 2004, at 56, *available at* http://www.nysscpa.org/cpajournal/2004/704/essentials/p56.htm.

38. *See, e.g.*, Amber L. Leaders, Note, *Gimme a Brekka!: Deciphering "Authorization" Under the CFAA and How Employers Can Protect Their Data*, 6 WASH. J. L., TECH. & ARTS 285, 288 (2011) (quoting 18 U.S.C. § 1030(a)(2) (2006)) ("The CFAA states in relevant part that whoever 'intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record of a financial institution, or of a card issuer . . . or contained in a file of a consumer reporting agency on a consumer' commits a federal crime.").

realm they are generally classified as fraud.[39] What is even more troubling is that these attacks come from inside, as well as outside, of the businesses that are attacked.[40]

B. Fraud—What Is It?

Fraud has been around since the earliest days of mankind.[41] It started in the Garden of Eden.[42] Fraud is, in its simplest form, deception.[43] *Black's Law Dictionary*'s definition of fraud encompasses both a legal definition,[44] and description of the elements,[45] as well as a generic definition that is more expansive:

> A generic term, embracing all multifarious means which human ingenuity can devise, and which are resorted to by one individual to get advantage over another by false suggestions or by suppression of truth, and includes all surprise, trick, cunning, dissembling, and any unfair way by which another is cheated. "Bad faith" and "fraud" are synonymous, and also synonyms of dishonesty, infidelity, faithlessness, perfidy, unfairness, etc.[46]

Throughout history, the primary means of accomplishing fraud has been through verbal and written communication—in person,[47] through the mail,[48] and

---

39. *See* Hanger Prosthetics & Orthotics v. Captsone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal 2008) (stating that the term "defraud," as used in 18 U.S.C. § 1030(a)(4) providing for a civil cause of action under the Computer Fraud and Abuse Act, "simply means wrongdoing").

40. *See generally* ROBINSON, *supra* note 6, at 7 (providing numerous examples of corporate espionage).

41. *See Genesis* 3:1–7 (King James).

42. *See id.*

43. *See* BLACK'S LAW DICTIONARY 660 (6th ed. 1990).

44. *Id.* (citing Delahanty v. First Pa. Bank, N.A., 464 A.2d 1243, 1251 (Pa. Super. Ct. 1983)) ("An intentional perversion of truth for the purpose of inducing another in reliance upon it to part with some valuable thing belonging to him or to surrender a legal right. A false representation of a matter of fact, whether by words or by conduct, by false or misleading allegations, or by concealment of that which should have been disclosed, which deceives and is intended to deceive another so that he shall act upon it to his legal injury. Anything calculated to deceive, whether by a single act or combination, or by suppression of truth, or suggestion of what is false, whether it be by direct falsehood or innuendo, by speech or silence, word of mouth, or look or gesture.").

45. *Id.* (citing Citizens Standard Life Ins. Co. v. Gilley, 521 S.W.2d 354, 356 (Tex. Civ. App. 1975)) ("Elements of a cause of action for 'fraud' include false representations of a present or past fact made by defendant, action in reliance thereupon by plaintiff, and damage resulting to plaintiff from such misrepresentation.").

46. *Id.* (citation omitted).

47. *See, e.g.*, Maxwell J. Mehlman, *Quackery*, 31 AM. J.L. & MED. 349, 361 (2005) (describing the "proverbial" nineteenth century snake oil salesman).

48. *See, e.g.*, John Rothchild, *Protecting the Digital Consumer: The Limits of Cyberspace Utopianism*, 74 IND L.J. 893, 904–05 (1999) (discussing the chain letter pyramid scheme).

over wires.[49] Those methods of fraud were so significant that they prompted Congress to enact laws to prevent them,[50] such as mail[51] and wire[52] fraud laws. These laws became very powerful tools for those seeking to protect against mail and wire fraud.[53] In the words of one prosecutor:

> To federal prosecutors of white collar crime, the mail fraud statute is our Stradivarius, our Colt 45, our Louisville Slugger, our Cuisinart—and our true love. We may flirt with RICO, show off with 10b-5, and call the conspiracy law "darling," but we always come home to the virtues of 18 U.S.C. § 1341, with its simplicity, adaptability, and comfortable familiarity.[54]

This statement was made decades ago.[55] Much has changed since then. Fraud knows no limits, and fraudsters will likely adapt to more efficient means of accomplishing fraud, when such means are available.[56] This adaptation has led to a whole new way of defrauding others: computer fraud—Fraud 2.0.[57] In response to this new instrument of fraud, Congress enacted the Computer Fraud and Abuse Act.[58] Just as the fraudster adapts, so too must the litigator.

C. Fraud 2.0—What Does Computer Fraud Mean?

Fraud 2.0 or computer fraud, regardless of the name, in its simplest form means deception accomplished through the use of a computer.[59] "Computer

---

49. *See, e.g.*, United States v. Aron, 328 F.3d 938, 939 (7th Cir. 2003) (describing the Defendant-Appellant's conviction of wire fraud for a fraudulent bond issuance).

50. *See* Jed S. Rakoff, *The Federal Mail Fraud Statute (Part I)*, 18 DUQ. L. REV. 771, 780 (1980).

51. 18 U.S.C. § 1341 (2006).

52. *Id.* § 1343.

53. *See* Rakoff, *supra* note 50, at 772.

54. *Id.* at 771 (footnotes omitted) (citing 18 U.S.C. §§ 1961–68, 1341; 17 C.F.R. § 240.10b-5 (2011)).

55. *Id.*

56. Brian Baxter, *Kroll Report: Fraud Will Rise as Economic Crisis Deepens*, THE AMLAW DAILY (Jan. 22, 2009, 8:30 AM), http://amlawdaily.typepad.com/amlawdaily/2009/01/kroll-report-says-fraud-to-rise-as-economic-crisis-deepens.html ("[O]nce domestic and international law enforcement agencies—including the Justice Department and SEC—turn their attention to a particular type of fraud, corporate criminals adapt quickly and devise increasingly complex schemes.").

57. I did not coin the term "Fraud 2.0," and, honestly, do not know who did coin the term, though I am going to use it freely. I found my first reference to it from an article entitled *Fraud 2.0*. DM Confidential, *Fraud 2.0*, ADOTAS (Oct. 26, 2007), http://www.adotas.com/2007/10/fraud-20/.

58. COMPUTER FRAUD AND ABUSE ACT OF 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

59. Recall that *Black's Law Dictionary* essentially defines fraud as deception or intentional misrepresentation. *See* BLACK'S, *supra* note 43, at 660. As a logical extension of this definition, computer fraud could be perceived as deception through the use of a computer.

fraud covers a variety of activity that is harmful to people [by] . . . using the computer in some way to commit dishonesty by obtaining an advantage or causing loss of something of value."[60] One commentator said that computer fraud is often "old crimes committed in new ways . . . using computers and the Internet to make the task[s] easier."[61] Indeed, computer fraud includes computer hacking, theft of data, theft of money, breach of data security and privacy, distribution of computer worms, Trojan horses, viruses, malware, and denial of service attacks that can harm businesses in any number of ways.[62]

With the Computer Age, computers have become a part of our everyday life. Now, we rely on computers to make phone calls, direct our vehicles, store and move our money, manage our business operations, and even to make our coffee and cook our food![63] Everything in our lives revolves around computers. Wozniak was right.[64] While history is replete with stories of scams involving word-of-mouth—like the snake oil salesmen of yesteryear[65] and the mail fraudster mailing out chain letter after chain letter in hopes of collecting a dollar from each[66]—because of our reliance on computers, the mouse and keyboard is the device of choice for many fraudsters today; and it is trending.[67] To make matters worse, the impact of fraud is no longer limited to being face-to-face, city-to-city, or even just state-to-state—it is now world-wide with the stroke of a key, thanks to the connectivity of the Internet.[68]

Like everything else in our lives, business is now run by computers. When someone seeks to commit a fraud against a business, it is not by face-to-face deception, mail deception, or even over the telephone, but is predominately over the Internet through the use of a computer.[69] This computer fraud can "take form in a number of ways, including program fraud, hacking, e-mail hoaxes, auction and retail sales schemes, investment schemes and people claiming to be

---

60. Ginger Kastor, *Addendum to* Megan J. Forness, *Computer Fraud*, *in* EDUCATOR'S GUIDE TO COMPUTER AND TECHNOLOGY MISUSE (2002), http://www.ed.uiue.edu/wp/crime-2002/fraud.htm (last visited Sept. 13, 2011).

61. Fahmida Y. Rashid, *Cyber-Criminals' Constantly Evolving Tactics Challenge Law Enforcement*, EWEEK.COM (Feb. 17, 2011), http://www.eweek.com/index2.php?option=content&do_pdf=1&id=66897 (quoting Adam Palmer, Norton lead cyber-security advisor at Symatec).

62. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1602–05 (2003) (commenting on various criminal forms of computer use and attending economic and non-economic harms).

63. *See* Orrin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN L. REV. 1561, 1577–78 (2010) (citing 18 U.S.C.A. § 1030(e) (West 2000 & Supp. 2009)) (observing that "protected computer" under the CFAA covers nearly everything we use in our daily lives).

64. *See supra* note 12 and accompanying text.

65. *See* Mehlman, *supra* note 47, at 361.

66. *See* Rothchild, *supra* note 48, at 904–05.

67. *See* Debra Wong Yang & Brian M. Hoffstadt, *Countering the Cyber-Crime Threat*, 43 AM. CRIM. L. REV. 201, 201 (2006).

68. *See id.* at 262.

69. *See id.*

experts on subject areas."[70] That broad description encompasses specific activity such as theft of money and information, identity theft, breaches of privacy, and countless other deceptive activities involving the use of a computer.[71] Businesses also face growing threats of distributed denial of service attacks, attacks on financial businesses and online banking, and attacks on crucial business infrastructure, to name just a few.[72] The methods are as limitless as the imaginations of the fraudsters.

This new form of fraud is deserving of its own name because of the potential it has to accomplish the objects of the fraud with such speed, efficiency, and magnitude that it surpasses all others in the blink of an eye—or stroke of a key. Welcome to the world of Fraud 2.0.

D. Fraud 2.0—It's Trending

Computer fraud is a billion dollar a year business with some estimates at $7 billion globally.[73] There is little doubt that it will continue to flourish.[74] The growth in this area of fraud is exponential and the trend is only increasing.[75] The current economic crisis facing the United States has likely contributed to this increase.[76] The problem is exacerbated by the fact that cyber criminals are now banding together to help each other accomplish their dishonest schemes.[77] The problem is certainly not limited to the United States. Computer fraud is an international issue[78] evinced by countries such as Russia having a "computer mafia"[79] that focuses its attacks on computers in America.[80]

---

70. Kastor, *supra* note 60.

71. *See generally* MICHAEL KUNZ & PATRICK WILSON, UNIV. OF MD. DEP'T OF CRIMINOLOGY & CRIMINAL JUSTICE, COMPUTER CRIME AND COMPUTER FRAUD 12–14, (2004), *available at* http://www.montgomerycountymd.gov/content/cjcc/pdf/computer_crime_study.pdf (discussing common Internet fraud crimes, including: advance fee fraud schemes, business/employment schemes, counterfeit check schemes, credit/debit card fraud, freight forwarding/reshipping, identity theft, investment fraud, non-delivery of goods/services, phony escrow services, ponzi/pyramid schemes, and spoofing/phishing).

72. GROUP-IB, STATE AND TRENDS OF THE "RUSSIAN" COMPUTER CRIME MARKET IN 2010 4 (2011), *available at* http://www.group-ib.ru/wp-content/uploads/2011/04/Group-IB_Report_Russian-cybercrime-market_2010_eng.pdf.

73. GROUP-IB, *supra* note 72, at 4.

74. *See* PONEMON INSTITUTE, SECOND ANNUAL COST OF CYBER CRIME STUDY 1 (2011), *available at* http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf.

75. *See id.*

76. PANDA SECURITY, THE CYBER-CRIME BLACK MARKET: UNCOVERED 4, *available at* http://press.pandasecurity.com/wp-content/uploads/2011/01/The-Cyber-Crime-Black-Market.pdf.

77. *See id.* at 9.

78. *See* Michael A. Sussmann, *The Critical Challenges from International High-Tech and Computer-Related Crime at the Millenium*, 9 DUKE J. COMP. & INT'L L. 451, 451 (1998) ("There is a revolution going on in criminal activity. It creates major problems for law enforcement in almost every part of the world—problems that have rarely been as system and pervasive. The revolution lies in the ways that networked computers and other technologies permit crimes to be committed

The growing trend of computer fraud is a potential threat to virtually every business, large or small, regardless of whether it is a technology savvy online company or a "mom and pop brick and mortar" cafe.[81] One survey of companies produced results showing that between 80% and 90% have experienced information security breaches.[82]

Because the objects of these crimes are often businesses—businesses that depend on litigators to prepare for and wage their battles over these issues—it is incumbent on such litigators to heed the advice of Sun Tzu and begin making their "calculations" before the battle. Moreover, because fraud targeting these businesses is trending,[83] so too is the need for capable litigators who are skilled at handling these problems. Just as the weapons of business warfare have evolved, so too have the weapons for litigators who are fighting for their clients on the legal battle front, or advising their clients on how to avoid getting into such battles in the first place.

E. Counsel's Role in Helping Clients Minimize Risks

Knowledgeable counsel also has a duty as an advisor. Based on the statistics, computer fraud will at some point be a problem for the vast majority of businesses over the coming years.[84] The magnitude of this problem is not always understood or appreciated by the businesses' decision-makers;[85] and, therefore, it is incumbent upon their attorneys to help them understand the risks, appreciate the magnitude of the risks, and prepare for dealing with them if they cannot be avoided. Many members of upper management are not yet aware of the threats that basic cyber risks pose to their businesses, and certainly do not understand all of the different types of risks that they face as they do not appreciate that information technology is a significant part of their overall

---

remotely, via the Internet and wireless communications. A criminal no longer needs to be at the scene of the crime (or within 1,000 miles, for that matter) to prey on his victim.").

79. GROUP-IB, *supra* note 72, at 1.

80. *See* Devlin Barrett, *Hackers Penetrate Nasdaq Computers*, WALL ST. J., Feb. 5–6, 2011, at A1, A4 (noting that "U.S. authorities have dealt with cyber attacks linked to computers in Russia").

81. *See* Yang & Hoffstadt, *supra* note 67, at 205.

82. Chris Costanzo, *Is Your Company Prepared for Cyber Risk?*, CORP. BD. MEMBER, First Quarter, 2011, at 42, 44, *available at* http://www.boardmember.com/MagazineArticle_Details.aspx?id=5943.

83. PONEMON INSTITUTE, *supra* note 74, at 1; *see, e.g.*, Barrett, *supra* note 80, at A1, A4 (discussing several attacks on the Nasdaq Stock Market's computer systems); Ben Rooney, *'Zeus Trojan' Zaps $3 Million from Bank Accounts*, CNN MONEY (Sept. 30, 2010, 2:47 PM), http://money.cnn.com/2010/09/30/technology/cyber_crime_charges/ (describing the work of the "cybercrime ring," which used the Zeus Trojan program to hack into bank accounts, stealing over three million dollars in the process).

84. *See* Costanzo, *supra* note 82, at 42.

85. *Id.* at 41.

business enterprise risk.[86] Moreover, few corporate boards specifically engage in key oversight activities such as annually reviewing the company's controls and policies to help protect against information technology privacy and security risks—the majority do not have executives who are dedicated solely to these types of roles.[87] This absence of management focus provides a perfect opportunity for astute legal counsel to provide added value to its relationship with the client.

The first thing counsel can do is alert and educate management. That is, simply raise the issue with management and provide a general overview of the prevalence of the risk and general types of threats that exist. Helpful information for demonstrating this risk to the client may include simply advising him that an average case of data breach for a company usually costs between $50,000 and $100,000, but some can be exponentially more depending on the level of breach and the information compromised.[88] In one case, the cost was as much as $31 million.[89] These estimated costs do not usually include legal fees for either prosecuting cases against the transgressors or defending against cases of those whose data and private information may have been compromised.[90] Counsel can then focus the discussion on how the business will need to address three aspects of this problem: prevention, loss mitigation, and loss recovery.

Prevention means the technological defenses that a business has in place to prevent computer fraud.[91] This is something that is handled by proactive information technology (IT) personnel and includes very basic things such as firewalls, anti-virus software, and data backup systems, up to more complicated defenses such as encryption and key logging.[92] Many attorneys do not have the technological knowledge to provide any more detailed advice on this issue nor should they. Computer fraud presents a rapidly changing environment with new and innovative threats literally developing each and every day.[93] Few, if any, attorneys should try to offer such technical advice.[94] Rather, it should be left up to the experts; however, proactive counsel should advise clients to seek out such expertise and implement the recommended safeguards.

---

86. *Id.*

87. *Id.*

88. *Id.* at 42.

89. *Id.*

90. *See id.*

91. *See* MARK GREISIGER, BUS. INS., CYBER RISKS: HOW TO PROTECT YOUR BUSINESS IN THE DIGITAL AGE 6 (2010), *available at* http://www.businessinsurance.com/assets/PDF/CB7208 91221.PDF.

92. *See id.*

93. *See* Hassan Mirza, *Cyber-Attacks Are the Biggest National Security Threat*, POLICYMIC, http://www.policymic.com/article/show?id=1519&response=true (last visited Sept. 6, 2011).

94. *See In re* Richmond's Case, 872 A.2d 1023, 1029, 1031 (N.H. 2005) (suspending an attorney for six months in part for practicing in an area where he lacked the necessary degree of competence).

Loss mitigation generally means having the business ensure that it has appropriate insurance coverage in place to cover the more common types of computer fraud that it will likely face.[95] Computer fraud insurance coverage is a complicated and very tricky issue. The computer fraud insuring agreements in most insurance policies are very antiquated vis-à-vis the current state of technology, which can present difficulties in getting a claim covered even when it seems apparent that coverage should be in place.[96] A thorough discussion of this issue could easily eclipse the breadth of this Article and is beyond its scope. At a minimum, however, the attorney should advise a client to carefully evaluate the types of computer fraud risks that it most likely faces, meet with the client's insurance representatives to make absolutely sure that those risks are covered by appropriate insurance coverage, and ensure that the client understands all applicable limitations and exclusions. It would be advisable to get this confirmation in writing as memories sometimes fade once a loss occurs.

The remainder of this Article will focus on the primary loss recovery tool available: the Computer Fraud and Abuse Act. This tool has been custom designed to combat the problem of computer fraud,[97] and therefore, it provides some different benefits than do traditional remedies.[98] State legislatures have crafted new laws to deal with computer fraud just as they have for the other methods of fraud.[99] The Computer Fraud and Abuse Act is the primary law that is currently used in this battle.[100]

Fraud 2.0 is here to stay and it will, over time, become more and more prevalent in business warfare. Litigation attorneys' clients are depending on their attorneys to be their general in this battle. This trust requires not only that they be good litigators, but also that they know what weapons are available and how to use them to protect their clients' most precious interests: their business lives.

---

95. *See* Russ Banham, *Inside Job: Are Your Commercial Clients Prepared for an Uptick in Fraud?*, INDEP. AGENT MAG., Nov. 2010, *available at* http://www.iamagazine.com/Magazine/2010/November/Cover_Story.aspx; John E. Black, Jr. et al., *Dangers Lurk in Cyberspace: A Primer on Risks and Insurance*, BUS. L. TODAY, July/Aug. 2002, at 41, 41.

96. *See* Mark A. Collins et al., *Recent Madoff-Related Coverage Disputes Place Crime Insurance in the Spotlight*, MCDERMOTT WILL & EMERY (Aug. 5, 2009), http://www.mwe.com/index.cfm/fuseaction/publications.nldetail/object_id/3b32b630-c698-48f9-b100-054c62b99996.cfm (describing some of the difficulties faced by computer fraud policyholders in enforcing their claims).

97. Brian S. Kabateck & Artin Gholian, *Click Here: The Computer Fraud and Abuse Act May Become the Best Tool for Fighting Advertising Click Fraud*, L.A. LAW., Apr. 2010, at 22, 24.

98. *See, e.g.*, Heather Zalar Steele, *The Computer Fraud and Abuse Act: An Overview of Potential Use in the Departing Employee Context*, FISHER & PHILLIPS LLP (June 30, 2010, 7:13 PM), http://www.noncompetenews.com/post/2010/06/30/The-Computer-Fraud-Abuse-Act-An-Overview-of-Potential-Use-in-the-Departing-Employee-Context.aspx (noting the specialized benefits provided by the CFAA in suits against departed employees).

99. Alexander Urbelis, Note, *Toward a More Equitable Prosecution of Cybercrime: Concerning Hackers, Criminals, and the National Security*, 29 VT. L. REV. 975, 982 (2005) (noting that states have crafted diverse methods to combat computer fraud).

100. *See* Sharkey, *supra* note 11, at 693–96.

III. COMPUTER FRAUD AND ABUSE ACT: A PRIMER FOR LITIGATORS

A. What Is the CFAA?

The Computer Fraud and Abuse Act is the most frequently used law for combating computer fraud.[101] In the author's experience, the frequency with which computer fraud claims are brought pursuant to the Computer Fraud and Abuse Act vis-à-vis other computer fraud related laws is overwhelming. Practically speaking, the Computer Fraud and Abuse Act is the king of all computer fraud laws. It is, therefore, important that litigation attorneys have a working knowledge of what it covers, the basics of how it is used, and the issues that generally pose the most difficulty and are the most frequently litigated.

The CFAA, as a body of law, is still in its infancy. The number of cases applying the CFAA is substantial because of the frequency with which it is used and the complexity of its statutory language.[102] Likewise, the scholarly literature addressing the CFAA is legion.[103] The CFAA is indeed a complicated piece of legislation that is highly nuanced and laden with procedural hurdles with which a practitioner must comply. This has led to conflicting interpretations and applications of various provisions of the CFAA by both judges and scholars.[104] The United States Supreme Court has yet to interpret the CFAA,[105] and there are conflicting interpretations among the various federal courts of appeal.[106] These uncertainties, as well as the sheer volume of cases and scholarly literature, cannot be thoroughly analyzed in one law review article. Thus, this Article

---

101. *See id.*

102. *See, e.g.*, Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821 (2009) (noting the confusion between the courts over the CFAA's language and providing examples of numerous cases interpreting and applying the statute).

103. *See, e.g.*, Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, 2009 U. ILL. J.L. TECH. & POL'Y 429 (2009) (examining the relationship between trade secret law and the CFAA); Kerr, *supra* note 63 (reviewing vagueness challenges to the CFAA).

104. *See* Field, *supra* note 102, at 821; Garrett D. Urban, Note, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1372 (2011).

105. Nick Akerman, *Will the Justices Rule on the Computer Fraud and Abuse Act?*, NAT'L L.J., Sept. 23, 2009, *available at* http://www.dorsey.com/files/upload/akerman_computer_fraud_july09.pdf.

106. *See, e.g.*, *id.* (discussing the conflict between the circuits regarding the interpretation of "without authorization"); John Rosenthal, *Navigating the Circuit Split on the Computer Fraud and Abuse Act*, GEORGETOWN LAW E-DISCOVERY LAW BLOG (May 3, 2010, 12:42 PM), http://www.law.georgetown.edu/cleblog/post.cfm/navigating-the-circuit-split-on-the-computer-fraud-and-abuse-act (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133–34 (9th Cir. 2009)); Int'l Airport Ctrs., LLC v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (discussing the circuit split regarding the interpretation of "authorization," especially in the employer and employee context).

merely provides a basic primer of some of the CFAA's principles and highlights those that will most often be encountered by litigators.

The Computer Fraud and Abuse Act is not even thirty years old, with its origins dating back to the early 1980s when federal law enforcement agencies were concerned that, due to the nature of emerging computer crimes, the wire and mail fraud provisions of the federal criminal code were no longer adequate tools for fighting computer related criminal activity.[107] Though many states already had their own versions of computer crime laws,[108] Congress included in the Comprehensive Crime Control Act of 1984 the first federal legislation aimed at addressing the new types of computer related criminal activity.[109] This legislation was codified at 18 U.S.C. § 1030.[110] This first statute was very narrow.[111] This statute was limited to "three specific scenarios: computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. Government computers."[112] Congress soon began to believe that there was a need for stronger federal legislation.

In 1986, Congress expanded the existing federal legislation to become what is now known as the Computer Fraud and Abuse Act (CFAA).[113] The legislative history of the CFAA indicates that Congress's intention was "to provide a clear statement of proscribed activity . . . to the law enforcement community, those who own and operate computers and those tempted to commit crimes by unauthorized access."[114] The CFAA's general purpose, originally, was to address the growing problems of computer crime and hacking directed at government interest computers.[115] Initially a federal criminal statute, the CFAA was subsequently expanded to permit the recovery of civil damages and injunctive relief for certain of its violations.[116] Courts, citing the legislative history, generally describe the CFAA as being originally designed to target computer hackers;[117] though its use has certainly expanded beyond that, both by

---

107. *See LVRC Holdings LLC*, 581 F.3d at 1130–31.

108. Greg Pollaro, Note, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. no. 12, at 2 (2010) (citing Dodd S. Griffith, Note, *The Computer Fraud and Abuse Act of 1986: A Measured Response to a Growing Problem*, 43 VAND. L. REV. 453, 459 (1990)) ("Approximately twenty-one states had enacted computer crime legislation by 1983.").

109. Kerr, *supra* note 63, at 1563–64.

110. *Id.* at 1564.

111. *Id.* at 1561.

112. *Id.* at 1564 (citing 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985)).

113. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213 (codified as amended at 18 U.S.C. § 1030).

114. S. REP. NO. 104-357, at 3 (1996).

115. Pollaro, *supra* note 108, at 11.

116. Sharkey, *supra* note 11, at 693.

117. *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1130–31 (9th Cir. 2009) (citing H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3694); A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 645 (4th Cir. 2009) (citing Charlotte Decker, Note, *Cyber Crime 2.0: An Argument to Update the United States Criminal Code to Reflect the Changing Nature of Cyber Crime*, 81 S. CAL. L. REV. 959, 980–81 (2008)).

Congressional expansion of the statutory language[118] and through application by the courts.[119] Some would say that it has now grown well beyond its purpose and is used too frequently.[120]

The CFAA has been amended frequently to enable it to keep abreast with technological advances.[121] The breadth of the CFAA was significantly expanded in three major amendments.[122] For the litigator, the most important amendment came in 1994.[123] It was then that what was originally enacted as only a criminal statute[124] was amended to add a private civil cause of action for many of its violations.[125]

B. What Constitutes a Violation of the CFAA?

"The CFAA prohibits, *inter alia*, unauthorized access to a 'protected computer' for the purpose of obtaining information, causing damage, or perpetrating fraud."[126] In its present form, the relevant provisions of the CFAA apply where someone intentionally accesses a protected computer without authorization or exceeds authorized access.[127] The term "computer" is defined by the CFAA to essentially mean any device for processing or storing data, with perhaps the only identifiable exceptions being automatic typewriters or hand held calculators.[128] A "protected computer" is either a United States government computer, a financial institution computer, or a computer used in interstate or

---

118. *See* Sharkey, *supra* note 11, at 693–94 & nn.90–91.

119. *See* Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 323–24 (2004).

120. *See* Joseph Oat Holdings, Inc. v. RCM Digesters, Inc., 409 F. App'x 498, 506 (3rd Cir. 2010) (citing Galbraith, *supra* note 119, at 324; Andrew B. Serwin, *Poised on the Precipice: A Critical Examination of Privacy Litigation*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 883, 887 (2009)).

121. Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. FED. 101 (2001).

122. *See id.* at 113.

123. *See id.* (noting that the 1994 amendments to the CFAA added the civil remedies to the Act).

124. Nick Akerman & Patricia Finnegan, *Computer Law: Civil Relief Under CFAA*, NAT'L L.J., Dec. 24–31, 2001, at A19.

125. *See* Buckman, *supra* note 121, at 113.

126. Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 774 (S.D. Tex. 2010) (footnote omitted) (citing 18 U.S.C. § 1030(a)(2)–(5) (2006)).

127. *See* § 1030(a)(1)–(7).

128. *See id.* § 1030(e)(1). The term "computer" is defined as:

> [A]n electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device[.]

Id.

foreign commerce or communication.[129] This final classification—used in interstate or foreign commerce—essentially makes a protected computer out of every computer connected to the Internet and, quite possibly, every computer.[130]

The CFAA prohibits ten general types of activity for which civil liability may be imposed. These prohibited activities include:

> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer . . . or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act;[131]
>
> . . . .
>
> (C) information from any protected computer;[132]
>
> . . . .
>
> (4) 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;[133]
>
> (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;[134]

---

129. 18 U.S.C. § 1030(e)(2) (A)-(B) (2006 & Supp. IV 2010). The term "protected computer" is defined as a computer:

> (A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
>
> (B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States[.]

Id.

130. *See Quantlab Techs. Ltd. (BVI)*, 719 F. Supp. 2d at 775–76; Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1032–33 (N.D. Ill. 2008) (citing Reno v. ACLU, 521 U.S. 844, 849–50 (1997); Paradigm Alliance, Inc. v. Celeritas Tech., LLC, 248 F.R.D. 598, 602 (D. Kan. 2008); Becker v. Toca, 2008 WL 4443050, at *5 (E.D. La. 2008); Credentials Plus, LLC v. Calderone, 230 F. Supp. 2d 890, 906 (N.D. Ind. 2002)); Kerr, *supra* note 63, at 1561, 1568 (The CFAA "potentially regulates every use of every computer in the United States and even many more millions of computers abroad.").

131. 18 U.S.C. § 1030(a)(2)(A) (2006) (citation omitted).

132. § 1030(a)(2)(C) (Supp. IV 2010).

133. § 1030(a)(4) (2006).

134. § 1030(a)(5)(A) (2006 & Supp. IV 2010).

> (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;[135] or
>
> (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[136]
>
> (6) knowingly and with intent to defraud traffics . . . in any password or similar information through which a computer may be accessed without authorization, if—
>
> (A) such trafficking affects interstate or foreign commerce;[137]
>
> . . . .
>
> (7) with intent to extort from any person any money or thing of value, transmits in interstate or foreign commerce any communication containing any—
>
> (A) threat to cause damage to a protected computer;[138]
>
> (B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access;[139]
>
> (C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion[.][140]

The CFAA also prohibits conspiracies to commit the foregoing conduct as well as attempts to commit such conduct.[141] For private civil claims, which are the primary concern for the litigator, the most useful of these are subsections (2) and (4)–(6), and, of those, subsections (2) and (4).

C. The Availability of Civil Remedies Under the CFAA

1. Authorization of Private Civil Claims

Section 1030(g) of the CFAA authorizes a civil action to seek remedies of compensatory damages and injunctive relief by one who suffers damage or loss from the CFAA violation.[142] Vis-à-vis the range of criminal violations, the civil

---

135. § 1030(a)(5)(B) (Supp. IV 2010).
136. § 1030(a)(5)(C) (Supp. IV 2010).
137. § 1030 (a)(6)(A) (2006).
138. § 1030(a)(7)(A) (Supp. IV 2010).
139. § 1030(a)(7)(B) (Supp. IV 2010).
140. § 1030(a)(7)(C) (Supp. IV 2010).
141. § 1030(b) (2006 & Supp. IV 2010).
142. § 1030(g) (2006) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

action is considerably limited and only available if the conduct involves one (or more) of five statutorily specified factors set forth in § 1030(c)(4)(A)(i).[143] Of these five factors, the most likely factor to be relevant in a business related civil matter is where the statutory violation caused (or would have caused) a loss to one or more persons in any one-year period aggregating at least $5,000.[144]

The CFAA defines the term "damage" as "any impairment to the integrity or availability of data, a program, a system, or information,"[145] and the term "loss" as:

> [A]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service [.][146]

Questions of what constitutes damage and loss are frequently litigated and, therefore, will be discussed in more detail in Section III.D.5. It is very important to note, however, that the CFAA uses both the term "damage" and "damages," and the two terms are not synonymous for purposes of the statute. Damage relates to the initial showing that must be made to satisfy the necessary conditions for bringing a civil CFAA claim.[147] The term damages, on the other hand, relates to what a plaintiff can recover for a CFAA violation.[148]

---

143. § 1030(g) (Supp. IV 2010) ("A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).") (footnote omitted). The five specified factors are as follows:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
>
> (III) physical injury to any person;
>
> (IV) a threat to public health or safety;
>
> (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security[.]

§ 1030(c)(4)(A)(i)(I)–(V) (Supp. IV 2010).

144. § 1030(c)(4)(A)(i)(I).

145. § 1030(e)(8) (2006).

146. § 1030(e)(11).

147. *See* § 1030(e)(8), (g).

148. *See, e.g.*, § 1030(g) (stating that a person who suffers "damage" as a result of a violation of this section may initiate a civil action to recover compensatory "damages").

2. *Procedural Issues Related to CFAA Claims*

The limitation period for bringing a claim for a violation of the CFAA is two years from the date of the wrongful act or the date of the discovery of the damage.[149] Therefore, "a plaintiff must file suit within two years of discovering 'any impairment to the integrity or availability of data, a program, a system, or information.'"[150] The key inquiry in determining when the limitation period accrues is when the plaintiff learns of the use of a computer in the deception, not just that there has been a deception. For example, it has been held that a plaintiff's knowledge of being deceived without having specific knowledge of the use of a computer in the deception did not commence the accrual of the limitations period until the plaintiff had knowledge of the use of the computer in the deception.[151]

A significant strategic consideration for many attorneys is choosing the court in which to try a case.[152] The CFAA is a federal statute, so a claim for its violation can be brought in federal court[153] or, in some cases, in a state court along with other claims.[154] The ability to bring this claim in a federal court can often be of great strategic benefit as state courts frequently are overburdened and lack the resources and the docket space to address the lawsuit as expeditiously as may be necessary.[155]

Federal courts do not have exclusive jurisdiction over CFAA claims. Rather, federal and state courts have concurrent jurisdiction to decide claims under the CFAA.[156] Accordingly, a CFAA claim may be brought in either the federal or state courts; however, a defendant in a state court proceeding can

---

149. *Id.*

150. Clark St. Wine & Spirits v. Emporos Sys. Corp., 754 F. Supp. 2d 474, 486 (E.D.N.Y. 2010) (quoting § 1030(e)(8)).

151. *Id.* Plaintiff's notice of "significant fraud activity" was not sufficient to constitute a discovery where plaintiff had not learned that the fraud involved the "impairment to the integrity or availability of data, a program, a system or information"; in other words, that the fraud involved access to a computer. *Id.* (quoting § 1030(e)(8)) (internal quotation marks omitted); *see* Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 775 (S.D. Tex. 2010)).

152. *See* Kimberly A. Moore & Francesco Parisi, *Rethinking Forum Shopping in Cyberspace*, 77 CHI.-KENT L. REV. 1325, 1328 (2002) ("By strategically choosing the forum, a plaintiff can maximize the expected return from litigation.").

153. *See, e.g.*, Creative Computing v. Getloaded.com LLC, 386 F.3d 930 (9th Cir. 2004) (affirming a district court verdict against the appellant for violations of the CFAA).

154. *See, e.g.*, Kellman v. Workstation Integrations, Inc., 332 S.W.3d 679, 683 (Tex. Ct. App. 2010) (plaintiff asserted several claims in state court, including claims under the CFAA, which were tried to a jury).

155. David L. Balser, *State Courts Need More Funding—Now*, 16 METRO CORP. COUNS., Feb. 2008, at 27.

156. Steven J. From & Joseph A. Martin, *Trade Secret Litigation*, 798 PRAC. L. INST. 655, 679 (2004) ("The absence of any limitations on where . . . [CFAA] civil actions may be filed leaves open the possibility that State courts will have concurrent jurisdiction with the federal courts over such claims."); *see* H & R Block Tax Servs., Inc. v. Rivera-Alicea, 570 F. Supp. 2d 255, 268 n.5 (D.P.R. 2008) ("This court does not have exclusive jurisdiction over Block's CFAA claim.").

remove the case to federal court if all other requirements for removal are satisfied.[157] Nevertheless, such removals are not always final, as federal courts are sometimes resistant to removal and remand either the case or the claim.[158] In *Liebert Corp. v. Mazur*, a federal district court did exactly that and remanded a previously removed CFAA claim back to the state court on an abstention basis.[159]

In another removal case, *Landmark Credit Union v. Doberstein*,[160] a federal district court analyzed the CFAA claim upon which the removal was premised and determined that because the CFAA claim appeared to be pretextual and not a seriously viable claim—along with the fact that the CFAA claim and the rest of the case was premised on a state law contract claim—the federal law claim was entirely derivative of state law issues, and therefore, the case did not arise under federal law.[161] Upon this rationale, the court determined that it did not have jurisdiction to hear the case and remanded it to the state court.[162] However, this case appears to be an aberration stemming from the fact that the CFAA claim was very weak on many levels, as the court averred: "[I]t can be fairly said that the claim of federal law in this case is, at best, insubstantial."[163]

In several cases, defendants have argued that Congress's enactment of the CFAA was intended to be the exclusive remedy for computer related claims and to preempt other computer related claims.[164] In each of these cases, the courts have found that the CFAA, which does not have clear preemptive language,[165] does not preclude bringing CFAA claims along with other claims.[166]

3. Asserting a Computer Fraud Claim Under the CFAA

While computer fraud is obviously an integral part of the CFAA, its reach goes far beyond computer fraud as that term is used in this Article. As previously mentioned, subsections (a)(2) and (a)(4) are the most useful CFAA

---

157. *See* 28 U.S.C. § 1441 (2006).

158. *See, e.g.*, Liebert Corp. v. Mazur, No. 05 C 2609, 2005 WL 1563202, at *3 (N.D. Ill. June 6, 2005) (remanding CFAA claims filed by plaintiff in federal court to state court).

159. *Id.*

160. 746 F. Supp. 2d 990 (E.D. Wis. 2010).

161. *Id.* at 995.

162. *Id.* at 995–96.

163. *Id.* at 995.

164. *See* United States v. Riggs, 739 F. Supp. 414, 423 (N.D. Ill. 1990); Hecht v. Components Int'l, Inc., 867 N.Y.S. 2d 889, 898 (N.Y. Sup. Ct. 2008).

165. *See* Integrated Waste Solutions, Inc. v. Goverdhanam, No. 10-2155, 2010 WL 4910176, at *15 n.10 (E.D. Pa. Nov. 30, 2010).

166. *See Riggs*, 739 F. Supp. at 423 ("[T]his court is unable to find[] anything in the legislative history of the CFAA which suggests that the statute was intended to be the exclusive law governing computer-related crimes, or that its enactment precludes the application of other criminal statutes to computer-related conduct."); *Hecht*, 867 N.Y.S.2d at 898 ("It appears that the CFAA is not intended to preempt state law claims based on unauthorized access to a computer such as trespass to chattel, conversion, or fraud.").

subsections for litigators.[167] One of the best ways to determine the validity of the claim is to review the elements necessary to prove the claim.

The elements of a civil claim for a violation of § 1030(a)(2) require the plaintiff to show that the defendant did the following:

> (1) intentionally accessed a computer, (2) without authorization or exceeding authorized access, and that he (3) thereby obtained information (4) from any protected computer (if the conduct involved an interstate or foreign communication), and that (5) there was a loss to one or more persons during any one-year period aggregating at least $5,000 in value.[168]

Subsection 1030(a)(4) of the CFAA encompasses what is generally considered to be the more traditional "fraud" violation of the CFAA:

> [Whoever] 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[.][169]

The elements of a civil claim for violation of § 1030(a)(4) require the plaintiff to show that the defendant did the following:

> (1) accessed a "protected computer," (2) without authorization or exceeding such authorization that was granted, (3) "knowingly" and with "intent to defraud," and thereby (4) "further[ed] the intended fraud and obtain[ed] anything of value," causing (5) a loss to one or more persons during any one-year period aggregating at least $5,000 in value.[170]

With an understanding of the elements of the most useful causes of action for business related claims under the CFAA, it is helpful to explore the burden by which these elements must be pleaded and proven. Despite the fact that the CFAA incorporates the word "fraud" into its title and statutory language, the pleading requirement for a CFAA claim is only that of general notice pleading of Rule 8(a),[171] and is not subject to the heightened pleading requirements of Rule

---

167. *See supra* Part III.B.
168. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009).
169. 18 U.S.C. § 1030(a)(4) (2006).
170. *LVRC Holdings LLC*, 581 F.3d. at 1132.
171. *See* FED. R. CIV. P. 8(a).

9(b)[172] of the Federal Rules of Civil Procedure that is normally required for pleading fraud.[173]

Similarly, the burden of proof for a CFAA claim is not the same as common law fraud. Rather, to defraud under the CFAA simply means wrongdoing and does not require proof of common law fraud.[174] As one court stated, "'fraud' under the CFAA only requires a showing of unlawful access; there is no need to plead the elements of common law fraud to state a claim under the Act."[175]

4. Relief Available: Economic Damages & Injunctive Relief

Subsection 1030(g) of the CFAA permits any person who has satisfied the requisite showing of damage and loss "to obtain compensatory damages and injunctive relief or other equitable relief."[176] For all practical purposes, the only compensatory damages usually recoverable in a business related case are economic damages because of the limitation contained in the statutory language.[177] In *Frees, Inc. v. McMillian*,[178] the court provided a summary of what types of damages have been found to be recoverable for a CFAA violation:

> The term "economic damages" was not statutorily defined, but courts have consistently held that this term has its ordinary meaning, i.e., simply prohibiting damages for pain and suffering, emotional distress, and other like damages. Similarly, without an express indication to the contrary, "compensatory damages" must be interpreted to have its ordinary, established meaning, thereby allowing "lost profits" as recoverable damages.
>
> Further, interpreting the statute to limit the recovery of lost revenue would lead to absurd results. The CFAA defines "damage" in terms of

---

172. FED. R. CIV. P. 9(b) ("In alleging fraud or mistake, a party must state with particularity the circumstances constituting fraud or mistake. Malice, intent, knowledge, and other conditions of a person's mind may be alleged generally.").

173. SKF USA, Inc. v. Bjerkness, 636 F. Supp. 2d 696, 719 n.13 (N.D. Ill. 2009) ("The heightened pleading standards of Rule 9(b) do not apply to the Computer Fraud and Abuse Act."); *see* Facebook, Inc. v. MaxBounty, Inc., 274 F.R.D. 279, 284 (N.D. Cal. 2011) (quoting *SKF USA, Inc.*, 636 F. Supp. 2d at 719 n.13); Enviroglas Prods., Inc. v. Enviroglas Prods., LLC, 705 F. Supp. 2d 560, 572 (N.D. Tex. 2010).

174. *See* Hanger Prosthetics & Orthotics, Inc. v. Capstone Orthopedic, Inc., 556 F. Supp. 2d 1122, 1131 (E.D. Cal. 2008) ("The term 'defraud' for purposes of § 1030(a)(4) simply means wrongdoing and does not require proof of common law fraud."); Thundervision, LLC v. Dror Int'l, LP (*In re* Thundervision, LLC), No. 09-11145, No. 09-1063 A, No. 09-1088, 2010 WL 2219352, at *12 (Bankr. E.D. La. June 1, 2010) (citing eBay, Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009)).

175. *eBay*, 608 F. Supp. 2d at 1164 (citing *Hanger Prosthetics & Orthotics, Inc.*, 556 F. Supp. 2d at 1131).

176. 18 U.S.C. § 1030(g) (2006).

177. *See* § 1030(g) (Supp. IV 2010) ("Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.").

178. No. 05-1979, 2007 WL 2264457 (W.D. La. Aug. 6, 2007).

> non-economic harm and "loss" in terms of economic harm. If the Court were to find that these terms were limitations on damages, a plaintiff would be unable to recover any monetary relief where he suffered only "damage," but no "loss." When a defendant copies unauthorized data to gain a competitive edge, it makes no sense to limit the plaintiff's recovery when the lost revenue is a direct result of defendant's misconduct.[179]

Courts have also found that loss of business and business goodwill constitutes recoverable damages under the CFAA.[180]

The CFAA does not permit recovery of exemplary damages.[181] Nor does the statutory language of the CFAA provide for the recovery of costs and attorneys' fees incurred for the prosecution or defense of a CFAA claim.[182] However, in some cases, courts have permitted the recovery of legal fees that are incurred from responding to the CFAA violation.[183]

Litigation strategy often places a higher value on the ability to obtain injunctive relief, for which the CFAA provides,[184] than on damages or attorneys' fees.[185] Strategically, injunctive relief can be the most important litigation factor, because if it is obtained, it may dispose of the case within a very short

---

179. *Id.* at *5 (citations omitted).

180. Contract Assocs. Office Interiors, Inc. v. Ruiter, No. CIV. S-07-0334 WBS EFB, 2008 WL 3286798, at *3 (E.D. Cal. Aug. 6, 2008) (citing Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935 (9th Cir. 2004)).

181. Liebert Corp. v. Mazur, No. 04 C 3737, 2004 WL 2095666, at *3 (N.D. Ill. Sept. 17, 2004). In a recent CFAA criminal case, the First Circuit ruled that restitution, though usually penal in nature, could be recovered because in the context of that case restitution was analogous to a cost of responding to a loss and, therefore, permissible. United States v. Janosko, 642 F.3d 40, 41–42 (1st Cir. 2011).

182. Thundervision, LLC v. Dror Int'l, LP (*In re* Thundervision, LLC), No. 09-11145, No. 09-1063 A, No. 09-1088, 2010 WL 2219352, at *12 (Bankr. E.D. La. June 1, 2010) ("Under the statute, the attorneys fees to assert a CFAA violation are not within the sphere of recoverable damages."); *see also Liebert Corp.*, 2004 WL 2095666, at *3 ("There is no express [CFAA] provision for . . . attorneys fees."); Tyco Int'l (US) Inc. v. John Does, No. 01 Civ. 3856(RCC)(DF), 2003 WL 23374767, at *5 (S.D.N.Y. Aug. 29, 2003) (denying claim for attorneys' fees under CFAA).

183. *See* NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1065–66 (S.D. Iowa 2009) (permitting plaintiff to recover legal fees incurred for researching how to appropriately respond to a data breach and for the response thereto, when they were considered necessary for responding to the actual CFAA violation, and, therefore, were "incurred as part of the response to a CFAA violation." (quoting A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009)) (internal quotation marks omitted)).

184. 18 U.S.C. § 1030(g) (2006).

185. *See* William Frank Carroll & Richard M. Hunt, *A Primer on Injunctive Relief in Federal and State Court*, 32 ADVOC. 34, 34 (2005) ("A suit for injunctive relief is one of the most effective tools available to a litigator, especially when a request for immediate relief is included.").

time.[186] This was exemplified in early 2011 in the matter of *Sony Computer Entertainment America LLC v. Hotz*.[187]

On January 11, 2011, Sony Computer Entertainment America (Sony) filed a lawsuit against George Hotz (Hotz) and others for "hacking" into their own Sony PlayStation®3 (PS3) gaming systems.[188] The essential accusation was that they had performed a "jailbreak" of their PS3 and were sharing information on how they did it with other people.[189] Sony sought a temporary restraining order under the CFAA as well as the Digital Millennium Copyright Act (DMCA).[190] The court granted the temporary restraining order.[191] The chronology of how this case proceeded is important, and a review of the relief granted in the temporary restraining order shows the power that injunctive relief under the CFAA can have.

On January 27, 2011, the court entered the temporary restraining order prohibiting Hotz and others from engaging in the following activities:

> 1. Offering to the public, creating, posting online, marketing, advertising, promoting, installing, distributing, providing, or otherwise trafficking in any circumvention technology, products, services, methods, codes, software tools, devices, component or part thereof, including but not limited to the Elliptic Curve Digital Signature Algorithm ("ECDSA") Keys, encryption and/or decryption keys, dePKG firmware decrypter program, Signing Tools, 3.55 Firmware Jailbreak, root keys, and/or any other technologies that enable unauthorized access to and/or copying of PS3 Systems and other copyrighted works (hereinafter, "Circumvention Devices").
>
> 2. Providing links from any web site to any other web site selling, offering for *sale, marketing, advertising, promoting, installing,*

---

186. *See* George W. Dent, Jr., *Unprofitable Mergers: Toward a Market-Based Legal Response*, 80 NW. U. L. REV. 777, 797 (1986) ("Indeed, in most cases a court should be able to decide quickly whether to grant a preliminary injunction, and as a practical matter this decision often will dispose of the entire case.").

187. Final Judgment upon Consent and Permanent Injunction, Sony Computer Entm't Am. LLC v. Hotz, No. 11-cv-000167 SI (N.D. Cal. Apr. 9, 2011) [hereinafter Permanent Injunction].

188. *Id.* at 1. The allegations were that Hotz and others were circumventing the effective technological protection measures (TPMs) employed by Sony to protect against unauthorized access to, and potential copying of, Sony's proprietary PS3 gaming systems. Complaint for Injunctive Relief and Damages Based on Violations of Digital Millennium Copyright Act; Violations of the CFAA; Contributory Copyright Infringement; Violations of the California Comprehensive Computer Data Access and Fraud Act; Breach of Contract; Tortious Interference with Contractual Relations; Common Law Misappropriation; and Trespass at 1, Sony Computer Entm't Am. LLC v. Hotz, No. 11-cv-000167 SI (N.D. Cal. Jan. 11, 2011) [hereinafter Complaint].

189. *See* Complaint, *supra* note 188, at 9–10.

190. *See id.* at 22.

191. Order Granting Plaintiff's *ex parte* Motion for Temporary Restraining Order, Order to Show Cause re: Preliminary Injunction, and Order of Impoundment at 2–3, Sony Computer Entm't Am. LLC v. Hotz, No. 11-cv-000167 SI (N.D. Cal. Jan. 27, 2011) [hereinafter Temporary Restraining Order].

> *importing, exporting, offering to the* public, distributing, providing, posting, or otherwise trafficking in any Circumvention Devices.
>
> 3. Engaging in acts of circumvention of TPMs in the PS3 System to access, obtain, remove, or traffic in copyrighted works.
>
> 4. Engaging in unauthorized access to the PS3 System or the PlayStation Network ("PSN") in order to obtain, access, or transmit any program, code, information or command therein.
>
> 5. Publishing, posting, or distributing any information, code, program, instructions, video, or other material obtained by circumventing TPMs in the PS3 System or by engaging in unauthorized access to the PS3 System or the PSN.
>
> 6. Assisting, facilitating or encouraging others to engage in the conduct set forth above in Nos. 1-5.[192]

The court further ordered, among other things, the "impoundment [of] any computers, hard drives, CD-ROMs, DVDs, USB stick[s], and any other storage devices on which any Circumvention Devices are stored in Defendant Hotz's possession, custody, or control."[193]

On February 28, 2011, United States District Judge Susan Illston granted Sony's request for a Preliminary Injunction that kept in place the prohibitions and mandates of the Temporary Restraining Order during the pendency of the case.[194] At this point, given the breadth of the temporary relief, there were few options for Hotz. In chess, this would have been checkmate.

By March 31, 2011—less than three months after the case was filed—the parties settled and agreed to a Final Judgment Upon Consent and Permanent Injunction.[195] The terms of the Permanent Injunction leave little doubt as to who won the case. The Permanent Injunction essentially prohibits the same activities that were included in the Temporary Restraining Order and Preliminary Injunction—permanently—and also provides that any violation thereof constitutes irreparable harm to Sony, entitling it to immediate relief—another temporary restraining order[196]—and stipulated liquidated damages of ten thousand dollars per violation, capped at a maximum amount of two hundred fifty thousand dollars.[197]

Had Sony not been able to obtain the Temporary Restraining Order or Preliminary Injunction, it is quite unlikely that this case would have settled on

---

192. Temporary Restraining Order, *supra* note 191, at 2–3.

193. *Id.* at 4.

194. *See* Order Granting Preliminary Injunction at 2–4, Sony Computer Entm't Am. LLC v. Hotz, No. C 11-000167 SI (N.D. Cal. Feb. 28, 2011) [hereinafter Preliminary Injunction]. While the Temporary Restraining Order was granted on the basis of Sony's CFAA and DMCA claims, *see* Temporary Restraining Order, *supra* note 191, at 2, the Preliminary Injunction was granted solely on the basis of the DMCA claim, *see* Preliminary Injunction, *supra*, at 2.

195. *See* Permanent Injunction, *supra* note 187, at 1.

196. *Id.* at 1, 3–5.

197. *Id.* at 4–5.

these terms this quickly. Successfully obtaining injunctive relief won this case, just as it wins many cases.[198] This case demonstrates the power and effectiveness of the injunctive remedies available under the CFAA. These are highly effective strategic devices that any litigators, business or otherwise, would want in their arsenal.

D. Issues Frequently Litigated Under the CFAA

Within the customary lifespan of a body of law, the CFAA is still in its infancy. The interpretation and application of its provisions are continuously evolving, and will continue to be refined through the judicial process as courts struggle with the meanings and inner workings of its key provisions. In what may seem counterintuitive, the litigation of these issues is positive for its development and refinement.[199] This is the essence of jurisprudence and will benefit the CFAA just as it has other bodies of law throughout history.[200] In the words of the eminent legal scholar Benjamin Cardozo, "In the endless process of testing and retesting, there is a constant rejection of the dross, and a constant retention of whatever is pure and sound and fine."[201]

This process is ongoing at this very moment, demonstrated by the fact that during the drafting of this Article alone, two significant circuit courts' decisions have made a substantive impact on the application of the CFAA to issues discussed in this Section. These decisions, *United States v. Kramer*[202] and *United States v. Nosal*,[203] are both criminal cases that will have a prodigious impact on CFAA business litigation cases and CFAA jurisprudence as a whole.[204]

---

198. *See* Dent, *supra* note 186, at 797 ("Indeed, in most cases a court should be able to decide quickly whether to grant a preliminary injunction, and as a practical matter this decision often will dispose of the entire case." (footnote omitted)).

199. *See* BENJAMIN N. CARDOZO, THE NATURE OF THE JUDICIAL PROCESS 35 (1921) ("[A]s a system of case law develops, the sordid controversies of litigants are the stuff out of which great and shining truths will ultimately be shaped. The accidental and the transitory will yield the essential and the permanent.").

200. *See id.* at 23–25.

> The rules and principles of case law have never been treated as final truths, but as working hypotheses, continually retested in those great laboratories of the law, the courts of justice. Every new case is an experiment; and if the accepted rule which seems applicable yields a result which is felt to be unjust, the rule is reconsidered. It may not be modified at once, for the attempt to do absolute justice in every single case would make the development and maintenance of general rules impossible; but if a rule continues to work injustice, it will eventually be reformulated. The principles themselves are continually retested; for if the rules derived from a principle do not work well, the principle itself must ultimately be re-examined.

Id. at 23 (quoting MUNROE SMITH, JURISPRUDENCE 21 (1909)) (internal quotation marks omitted).

201. *Id.* at 179.

202. 631 F.3d 900 (8th Cir. 2011).

203. 642 F.3d 781 (9th Cir. 2011).

204. *See infra* notes 210–220, 241 and accompanying text.

The United States Supreme Court has yet to interpret the CFAA, which leaves many questions unanswered.[205] Consequently, jurisdictions are in conflict about the interpretation and application of various provisions of the CFAA.[206] Further, though it may not be readily apparent given its complexity, even what may seem to be a relatively clear and straightforward reading of a provision of the CFAA may be subject to more than one interpretation. At this stage of the CFAA's development, very little can be relied on as being settled with finality.[207]

Given all of this uncertainty, attorneys must stay abreast of the prevailing developments within their jurisdiction on various issues and be methodical in asserting or defending against a CFAA claim to ensure that all of the procedural requirements are satisfied. Many of the CFAA decisions are rulings on motions to dismiss for failure to state a claim on the grounds that various procedural requirements have not been met.[208] Thus, the attorneys who brought the claim likely either did not know how to properly assert it, or, because of facts that were beyond their control, simply could not properly assert all the necessary requirements for the claim.[209] Accordingly, when considering bringing or defending a claim under the CFAA, it is important to take nothing for granted and always use the most current research.

1. What Is a Computer Under the CFAA?

One of the first questions to answer is "what is a computer under the CFAA?" A cell phone? Yes.[210] Recent case law has reinforced the proposition that virtually everything that contains a microchip (which, these days, is almost everything) is a "computer."[211] In *United States v. Kramer*, the Eighth Circuit

---

205. *See* LVRC Holdings, LLC, v. Brekka, 581 F.3d 1127 (9th Cir. 2009); United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009); Akerman, *supra* note 105.

206. *See supra* note 205.

207. *See supra* note 205.

208. *See, e.g.*, Triad Consultants, Inc. v. Wiggins, 249 F. App'x 38, 38, 40 (10th Cir. 2007) (affirming the district court's dismissal of the plaintiff's CFAA claim pursuant to Rule 12(b)(6) for failure to plead facts showing defendant obtained anything of value as required by § 1030(a)(4)); Lee v. PMSI, Inc., No. 8:10-cv-2904-T-23TBM, 2011 WL 1742028, at *2–3 (M.D. Fla. May 6, 2011) (granting plaintiff's motion to dismiss defendant's counterclaim for failing to allege unauthorized computer use).

209. One of the author's primary purposes in writing this Article is to equip the business litigator with enough information to know what procedural requirements need to be addressed, determine the appropriate standard for the relevant jurisdiction, and be able to properly assert the claim. Indeed, this is the essence of the author's second purpose as identified in Section III. The issues discussed in this Section are only a small sample of the issues that arise in litigating CFAA claims. This discussion provides only a limited overview of some of the frequently litigated issues and how those issues are often argued and addressed. It does not purport to state what the law "is" on these issues because, at this point, that is indeterminable.

210. *See* United States v. Kramer, 631 F.3d 900, 901 (8th Cir. 2011) (citing 18 U.S.C. § 1030(e)(1) (2006)).

211. *Id.* at 902 (citing § 1030(e)(1)).

analyzed this issue in a case that did not involve a CFAA violation,[212] looking to the CFAA's definition of computer for guidance.[213] The court held that a standard cell phone is a computer under the CFAA's definition.[214] It was this court that quoted the cofounder of Apple Computer, Steve Wozniak, as saying, "[e]verything has a computer in it nowadays."[215] The court's opinion certainly went a long way toward confirming that proposition insofar as computers are defined under the CFAA. The court observed that the definition of computer in the CFAA is exceedingly broad:

> If a device is "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions," it is a computer. This definition captures any device that makes use of an electronic data processor, examples of which are legion. *Accord* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1577 (2010) ("Just think of the common household items that include microchips and electronic storage devices, and thus will satisfy the statutory definition of 'computer.' That category can include coffeemakers, microwave ovens, watches, telephones, children's toys, MP3 players, refrigerators, heating and air-conditioning units, radios, alarm clocks, televisions, and DVD players, in addition to more traditional computers like laptops or desktop computers." (footnote omitted)). Additionally, each time an electronic processor performs any task—from powering on, to receiving keypad input, to displaying information—it performs logical, arithmetic, or storage functions. These functions are the essence of its operation. *See* The New Oxford American Dictionary 277 (2nd ed. 2005) (defining "central processing unit" as "the part of the computer in which operations are controlled and executed").[216]

The court acknowledged that a normal cell phone might not easily fit within the colloquial definition of computer, but that it was bound to follow the definition set forth in the CFAA.[217] It further acknowledged that, due to the sweeping nature of this definition, as technology continues to develop even more devices, although neither industry experts nor Congress foresaw their creation, these devices may nonetheless be considered a computer.[218]

---

212. *Id.* at 901–02.

213. *Id.* at 902–04.

214. *Id.* at 901.

215. *Id.* at 901 (citing Mark Milian, *Apple's Steve Wozniak: 'We've Lost a Lot of Control,'* CNN, (Dec. 8, 2010, 12:16 PM), http://www.cnn.com/2010/TECH/innovation/12/08steve.wozniak.computers/index.html).

216. *Id.* at 902–03.

217. *Id.* at 903.

218. *Id.* at 903–04 (footnotes omitted).

Finally, the court analyzed the specific operations and specifications of the cell phone at issue and determined that the phone contained a lithium ion battery, had 5 MB of memory, was capable of running software, used a graphics accelerator to run its display images, and contained a software copyright notice, all of which sufficiently demonstrated that the phone makes use of an electronic data processor.[219] Based upon the definition of computer in the CFAA, the court reasoned that the cell phone at issue was indeed a computer pursuant to the CFAA's definition.[220]

The court was correct in that most people do not think of a cell phone as a computer in a colloquial sense; however, today's cell phones may very well be more powerful computers than many of the first computers owned by the readers of this Article. This is certainly true of the author, whose first computer was a TI–99 made by Texas Instruments that had a 3.3 MHz processor and 16 KB of RAM.[221] Comparing the TI-99's specifications to a current "smart phone" would not be fair. The smart phone is an exponentially more powerful computer.[222] Perhaps a better comparison is to a popular children's toy: a Leapster game console marketed for children between the ages of four and eight years old.[223] The Leapster has a CPU running at 96 MHz, and has 128 MB of RAM.[224] By '80s standards, this child's toy is a supercomputer![225]

A video gaming system? Absolutely. Recall that the computer at issue in *Sony Computer Entertainment America LLC v. Hotz* was a Sony PlayStation3 gaming system.[226] The issue in that case was whether Hotz performed a "jailbreak" on his own PS3, and the court found that, at least for purposes of the Temporary Restraining Order and Preliminary injunction, it was a computer.[227]

---

219. *See id.* at 904.

220. *See id.* at 904–05.

221. *Texas Instruments Introduces the TI-99/4 Home Computer*, TI994.COM, http://www.ti994.com/1979/brochures/1979pamphlet.pdf (last visited Sept. 16, 2011); *Texas Instruments TI-99/4*, OLDCOMPUTERS.NET, http://oldcomputers.net/ti994.html (last visited Sept. 16, 2011).

222. *See Droid Incredible by HTC at Verizon Wireless*, HTC, http://www.htc.com/us/products/droid-incredible-verizon#tech-specs (last visited Sept. 16, 2011) (specifying a processor of 1 GHz and memory up to 8 GB).

223. *Leapster 2*, LEAPFROG, http://www.leapfrog.com/gaming/leapster2/ (last visited Sept. 16, 2011).

224. *LeapFrog LeapSter 2—handheld game console—pink*, CNET, http://shopper.cnet.com/consoles/leapfrog-leapster-2-handheld/4014-10109_9-33897286.html#info-5 (last visited Sept. 16, 2011).

225. *See* John Sheesley, *The 80's Supercomputer That's Sitting in Your Lap*, TECHREPUBLIC (Oct. 13, 2008, 3:47 PM), http://www.techrepublic.com/blog/classic-tech/the-80s-supercomputer-thats-sitting-in-your-lap/189. In the 1980s, the fastest supercomputer ran at 250 MHz, and the fastest desktop computer available had a processor that ran at 66 MHz. *Id.*

226. *See* Complaint, *supra* note 188, at 1.

227. *See* Temporary Restraining Order, *supra* note 191, at 1–2; Preliminary Injunction, *supra* note 194, at 1–2.

A website? Yes. Courts have held that websites are computers for many years,[228] but the infamous MySpace "bully-mom" case[229] recently brought a great deal of attention to the issue.[230] In that case, Lori Drew was prosecuted for violating the CFAA by creating a fake MySpace account that she then used to harass a thirteen-year-old girl to the point that the girl ultimately committed suicide.[231] The charges alleged that Drew violated MySpace's Terms of Service by intentionally accessing the MySpace website, a computer, without authorization or in excess of authorization.[232] The court recited the CFAA definition of computer, and reasoned that to access an Internet website requires one to access the server hosting the website, which is a computer.[233] The court followed the well settled standard and found that a website is a computer for purposes of the CFAA.[234] Steve Wozniak was correct: everything does indeed have a computer in it and the trend is increasing.[235]

2. *Access: Unauthorized v. Exceeding—What Is and What Isn't?*

a. *Complex and Perpetually Evolving Nature of Access*

The CFAA requires more than simply using a computer in the commission of a wrongful act. It requires the improper access of a computer.[236] Therefore, it does not apply to every fraud involving computer use.[237] The issue of access is integral to establishing a violation of the CFAA and has been one of the most complicated and highly litigated issues arising under the CFAA.[238] As with other areas of the CFAA, this issue is evolving. Much has changed, however, during the drafting of this Article. Leading up to April 28, 2011, there was what on the surface appeared to be a conflict that had two circuit courts of appeal on a

---

228. *See* LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1136 (9th Cir. 2009) ("There is no dispute that if Brekka accessed LVRC's information on the LOAD website after he left the company in September 2003, Brekka would have accessed a protected computer 'without authorization' for purposes of the CFAA."); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581–82 (1st Cir. 2001); Craigslist, Inc. v. Naturemarket, Inc., 694 F. Supp. 2d 1039, 1049, 1057 (N.D. Cal. 2010).

229. United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009).

230. *See, e.g.*, *Mom Indicted in MySpace Suicide Case*, MSNBC.COM (May 15, 2008), http://www.msnbc.msn.com/id/24652422/ns/us_news-crime_and_courts/t/mom-indicted-myspace-suicide-case/#.TmRGLY5yDvE (discussing the *Drew* case).

231. *Drew*, 259 F.R.D. at 452.

232. *Id.* (citing 18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)(ii) (2006 & Supp. III 2009)).

233. *See id.* at 456–57 (citing § 1030(e)(2)(B)).

234. *See id.* at 458.

235. *See* Milian, *supra* note 12.

236. *See supra* notes 137–146 and accompanying text.

237. *See id.*

238. *See, e.g.*, LVRC Holdings, LLC v. Brekka, 581 F.3d 1127, 1132–35 (9th Cir. 2009) (citations omitted) (interpreting "exceeds authorized access"); Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 (S.D.N.Y. 2010) (examining various interpretations of "access" by the courts).

collision course, and at least two somewhere in the middle.[239] It looked as though the CFAA was going to be examined by the United States Supreme Court.[240]

Then, the Ninth Circuit filed its opinion in *United States v. Nosal*[241] and seemed to meld together some of those conflicts in a way that could have a profound impact on the various theories of access jurisprudence, as Part III.D.4.(a) will explain. How well the other circuit courts will receive *Nosal*, including whether the Seventh Circuit will move closer to the middle,[242] is uncertain. The more immediate question, however, is what has led to all of this confusion. The statutory language is the best place to begin.

3. Generally Applicable Principles for Both Forms of Access

The CFAA prohibits intentionally or knowingly accessing a computer "without authorization" and "exceed[ing] authorized access."[243] These are two different concepts.[244] The first step of the analysis is that there must be an actual access to a computer.[245] An access can occur in any number of ways, from something as simple as logging in to a computer to view information,[246] to sending or receiving an email,[247] or to having an elaborate program using codes and proprietary information to extract data from a web site.[248] Access does not include a computer technician's misleading statements about services he performed on a computer where his failure or incompetence in performing those services may have resulted in lost data.[249] Regardless of how false or misleading the statements were, they did not constitute access to a computer—they were statements, not access.[250]

The access must be knowing or intentional.[251] A mistaken or accidental access that is neither intentional nor knowing does not constitute a violation of

---

239. *See infra* Part III.D.4.

240. *See* Akerman, *supra* note 105.

241. 642 F.3d 781 (9th Cir. 2011).

242. *See infra* text accompanying notes 279–287.

243. 18 U.S.C. § 1030(a) (2006).

244. *See* § 1030(e)(6) (defining the term "exceeds authorized access" to mean "to access a computer *with* authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter" (emphasis added)).

245. § 1030(a).

246. *See* United States v. Rodriguez, 628 F.3d 1258, 1263 (11th Cir. 2010).

247. *See* Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1273 (N.D. Iowa 2000).

248. *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 579, 581–82 (1st Cir. 2001) (citations omitted).

249. *See* Hillsboro Dental, LLC v. Hartford Cas. Ins. Co., No. 410-CV-271 (CEJ), 2010 WL 5184956, at *3 (E.D. Mo. Dec. 15, 2010) (citing § 1030(a)).

250. *See id.*

251. *See* 18 U.S.C. § 1030(a) (2006).

the CFAA.[252] However, the CFAA does recognize vicarious liability, and an employer can be responsible for its employees' wrongful access under certain circumstances.[253]

Third party issues occasionally arise under the CFAA. For example, a CFAA violator's access will be wrongful whether he uses his own computer or a third party's computer to effectuate the access.[254] The focus is on the person causing the access, not on the actual computer used to facilitate the access.[255] Insofar as it is the computer that is the object of the access, however, it is not quite so clear. One court has held that a plaintiff can only bring CFAA claims for wrongful access to its own computers, not the computers of third parties.[256] The Ninth Circuit, however, rejected a district court's dismissal for the same reason in *Theofel v. Farey-Jones*,[257] where it explained this issue as follows:

> The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to "*[a]ny person* who suffers damage or loss by reason of a violation of this section." "[T]he word 'any' has an expansive meaning, that is, 'one or some indiscriminately of whatever kind.'" Nothing in the provision's language supports the district court's restriction. Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.[258]

---

252. *See* Hunt v. Branch Banking & Trust Co., No. 4:09-cv-2151-JMC-TER, 2011 WL 1101050, at *1, *6 (D.S.C. Mar. 23, 2011) (defendant's mistaken origination of plaintiff's bank account in a manner not authorized by the plaintiff was not contemplated by the CFAA).

253. *See* Clark Street Wine & Spirits v. Emporos Sys. Corp., 754 F. Supp. 2d 474, 486 (E.D.N.Y. 2010) (In the context of the CFAA, "[a]n employer is responsible for an employee's intentional tort only when the employee was acting within the scope of his or her employment when he or she committed the tort." (quoting Girden v. Sandals Int'l, 262 F.3d 195, 205 (2d Cir. 2001) (internal quotation marks omitted))). This, however, usually raises a predominantly factual issue for the jury, but in some cases it is appropriate for determination as a matter of law. *See Girden*, 262 F.3d at 205.

254. *See* eBay Inc. v. Digital Point Solutions, Inc., 608 F. Supp. 2d 1156, 1164 (N.D. Cal. 2009) (citing Binary Semantics, Ltd. v. Minitab, Inc., No. 4:07-CV-1750, 2008 WL 763575, at *5 (M.D. Pa. Mar. 20, 2008)).

255. *See id.* (explaining that "hackers may use the computers of unknowing third parties to carry out their schemes").

256. *See* Scottrade, Inc. v. BroCo Invs., Inc., 774 F. Supp. 2d 573, 584 (S.D.N.Y. 2011). Scottrade's customers' accounts were hacked and Scottrade reimbursed its customers for their losses, and then asserted a CFAA claim against the hacker and Genesis, the investment broker through which the hacker originally purchased securities fraudulently traded to Scottrade customers. *Id.* at 575–76. The court held, "[b]ecause Scottrade does not allege that Genesis hacked into its systems, or otherwise accessed its computers without authorization, Scottrade's CFAA claim against Genesis fails and must be dismissed." *Id.* at 584.

257. 359 F.3d 1066 (9th Cir. 2004) ("The district court dismissed without leave to amend on the theory that the Act does not apply to unauthorized access of a third party's computer.").

258. *Id.* at 1078 (citations omitted) (internal quotation marks omitted).

This was also made clear by another court, which ruled that the CFAA "allows a party to seek a civil remedy if it experiences loss or damage due to information obtained from *any* protected computer."[259] As discussed, the disagreement of the courts on this issue is indicative of the overall lack of agreement among many courts in interpreting and applying various provisions of the CFAA. At least to some courts, it appears the focus is on the person harmed by the access, not necessarily on who owns the actual device that was accessed.

4. *Differentiation Between Unauthorized and Exceeding Is Not Always Clear*

As an essential requirement "for all civil claims under the CFAA, a plaintiff must show that the defendant's access to the protected computer was either 'without authorization' or that it 'exceed[ed] authorized access.'"[260] The legislative history of the CFAA shows that Congress anticipated that persons who exceed authorized access are likely to be insiders, with some rights to access the computer, whereas persons who act without authorization are likely to be outsiders, with no rights to use the computer.[261] It is important to understand this general purpose and keep it in mind to help in understanding the distinction between the two categories of computer access. The CFAA clearly differentiates between unauthorized users and those who exceed authorized access,[262] and one must assume that Congress did so for a reason.

The lines between these two, however, have become blurred by the courts, with some saying the difference is "paper thin but not quite invisible,"[263] and others not even bothering to distinguish between the two.[264] Many of the cases interpreting and applying the access issues do not clearly differentiate between the two types of access, thus creating substantial overlap and confusion between the two.[265] This appears to be an oversight on the part of the courts that has further exacerbated the confusion about the access issue. Congress clearly intended to not only create two separate and distinct categories of access, but also for the implications of each to be different.[266] This congressional intention

---

259. Sloan Fin. Grp., LLC v. Coe, No. 0:09-cv-02659-CMC, 2010 WL 4668341, at *5 n.8 (D.S.C. Nov. 18, 2010) (citing 18 U.S.C. § 1030(a)(2)(C), (g) (2006 & Supp. III 2009)).

260. Remedpar, Inc. v. Allparts Med., LLC, 683 F. Supp. 2d 605, 609 (M.D. Tenn. 2010).

261. United States v. Phillips, 477 F.3d 215, 219 (5th Cir. 2007) (citing S. REP. NO. 104-357, at 11 (1996); S. REP. NO. 99-432, at 10 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2488).

262. *Id.*

263. Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (citation omitted).

264. *See* United States. v. Drew, 259 F.R.D. 449, 461 (C.D. Cal. 2009) ("However, this Court concludes that an intentional breach of the [MySpace.com Terms of User Agreement] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute.").

265. *See id.*

266. *Phillips*, 477 F.3d at 219.

> [T]he CFAA . . . does clearly differentiate between unauthorized users and those who "exceed[] authorized access." Several subsections of the CFAA apply exclusively to

should be respected. In order to resolve this confusion in the future, courts should exercise more discipline in their analysis and follow the structure of the statutory framework by first identifying specifically which of the two categories the cases are being analyzed under, as well as upon which their rulings are based.

a. "Without Authorization"

It has been said that the meaning of access "without authorization" is elusive.[267] The elusive nature of this phrase's meaning stems from Congress not defining what it means to access without authorization for purposes of the CFAA.[268] Because it is not defined, principles of statutory construction direct that the "words will be interpreted as taking their ordinary, contemporary, common meaning."[269] The common meaning of without authorization, therefore, means accessing a computer without any permission at all.[270] The application, however, is not quite so simple.

As discussed, the expectation was that the "without authorization" category would apply to outside hackers who have no right to access a computer.[271] An example of this would be a hacker, with no rights to access a computer, secretly entering an office, locating a hidden password, and intentionally logging in by typing the password into the computer. The hacker has thus gained access by bypassing the password protection system that would have otherwise prevented him from obtaining the information stored on the computer.[272] Determining whether an outsider, with no rights to access a computer, who accesses a computer nonetheless accesses without authorization is not usually a difficult issue for the courts to decide.[273]

This issue becomes significantly more complicated, however, when it involves insiders who have been given permission to access a computer, but then

---

> users who lack access authorization altogether. In conditioning the nature of the intrusion in part on the level of authorization a computer user possesses, Congress distinguished between "insiders, who are authorized to access a computer," and "outside hackers who break into a computer."

Id. (citations omitted).

267. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001).

268. *See* United States v. Nosal, 642 F.3d 781, 785 (9th Cir. 2011); *Phillips*, 477 F.3d at 219.

269. LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009) (quoting Perrin v. United States, 444 U.S. 37, 42 (1979) (internal quotation marks omitted)).

270. *Id.* at 1133 ("[A] person who 'intentionally accesses a computer without authorization' accesses a computer without any permission at all . . . ." (citations omitted) (quoting 18 U.S.C. § 1030(a)(2) (2006))).

271. *See supra* text accompanying note 261.

272. *See, e.g.*, United States v. Ivanov, 175 F. Supp. 2d 367, 369 (D. Conn. 2001) (discussing a similar factual scenario wherein a hacker physically located in Russia broke into an American company's customer databases in the United States and was found to have acted without authorization).

273. *See, e.g.*, United States v. Phillips, 477 F.3d 215, 220 (5th Cir. 2007) (finding unauthorized access where defendant used a "brute-force" attack program to gain access to a certain website).

use that access in an improper manner. The circuit courts have generally applied three different theories in how they address these issues: the Seventh Circuit's "agency theory," set forth in *International Airport Centers, LLC v. Citrin*;[274] which appeared to be in direct conflict with the Ninth Circuit's "access means access theory," set forth in *LVRC Holdings LLC v. Brekka*;[275] and, in the middle ground between the two of them, the Fifth and Eleventh Circuits' "intended-use analysis," set forth in *United States v. John*[276] and *United States v. Rodriguez*,[277] respectively. A chronology of those four cases alone demonstrates the evolution of CFAA access jurisprudence.

In the earliest of these cases, at one end of the spectrum of theories, is the agency theory set forth by the Seventh Circuit in *Citrin*.[278] This theory is the most permissive in that it permits authorization to be terminated the easiest, with no activity required by the grantor.[279] In *Citrin*, the court addressed a case in which an employee had been given permission to access a company computer, but was determined to have had that authorization terminated at the time he breached his duty of loyalty to his employer by violating terms of his employment contract.[280] The employee was held to have accessed the computer without authorization.[281] The rationale is that, under common law agency principles, the employee's right to access the computer was premised upon his agency relationship with his employer; when he breached his duty of loyalty to his employer, it terminated the agency relationship upon which the right to access was premised, thereby terminating that right to access.[282]

The Fifth Circuit occupies the middle ground with its intended-use analysis that was first applied to the "without authorization" category of access in *United States v. Phillips*.[283] Under this rationale, an insider, once given authorization to access a computer for certain purposes, will have that authorization terminated if it is used for reasons beyond its intended purpose, therefore rendering the access without authorization.[284] The *Phillips* court's rationale for the intended-use analysis is derived from an early Second Circuit case interpreting the CFAA, *United States v. Morris*.[285]

In *Morris*, the defendant used a computer that he had been given authority to access; however, he used it to send out a damaging "worm" that spread and

274. 440 F.3d 418, 420–21 (7th Cir. 2006).
275. *See* 581 F.3d 1127, 1133 (9th Cir. 2009).
276. *See* 597 F.3d 263, 273 (5th Cir. 2010).
277. *See* 628 F.3d 1258, 1263 (11th Cir. 2010).
278. *See Citrin*, 440 F.3d at 420–21.
279. *Id.*
280. *Id.*
281. *Id.*
282. *Id.*
283. *See* United States v. Phillips, 477 F.3d 215, 220–21 (5th Cir. 2007).
284. *Id.* at 219–21.
285. *See id.* at 219–20 (citing United States v. Morris, 928 F.2d 504 (2d Cir. 1991)).

infected computers throughout the United States.[286] The defendant argued that his access was not without authority, but that he had only exceeded authorized access; the court rejected this argument.[287] The court determined his access was without authorization for three reasons: (1) he accessed computers on the network that he had not been authorized to access; (2) he misused the functions available to him in an unintended way; and (3) the worm he created exceeded his authorized access by spreading to other computers that he had not been authorized to access.[288] The rationale for the intended-use analysis comes from the second of these reasons.[289] The first and third reasons demonstrate that, for purposes of access without authorization, a person may have authorization to access certain computers but not others—for which he will then be treated as an outsider without authorization.[290]

At the opposite end of the spectrum from *Citrin* is the Ninth Circuit's *Brekka*[291] opinion. The *Brekka* court found that once an insider had been given authorization to access the computer, no matter how disloyal his acts or interests may become, that authorization to access does not terminate and become unauthorized unless actually terminated by the employer—the grantor of the access.[292] The employee in *Brekka* did not have a written employment contract or any other limitation placed on his access to, or use of, the computer.[293] This is an important fact to keep in mind when considering the Ninth Circuit's recent

---

286. *Morris*, 928 F.2d at 505.

287. *Id.* at 510.

288. *Id.* at 509–10.

289. *See Phillips*, 477 F.3d at 219.

290. *Phillips*, 477 F.3d at 219–20 (citing *Morris*, 928 F.2d at 505, 510).

> Courts have therefore typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user. Applying such an intended-use analysis, in *United States v. Morris*, . . . the Second Circuit held that transmission of an internet worm designed "to demonstrate the inadequacies of current security measures on computer networks by exploiting . . . security defects" was sufficient to permit a jury to find unauthorized access within the meaning of § 1030(a)(5)(A). The *Morris* court determined that conduct, like "password guessing" or finding "holes in . . . programs," that uses computer systems not "in any way related to their intended function" amounts to obtaining unauthorized access.

Id. (citations omitted).

291. LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).

292. *Brekka*, 581 F.3d at 1135.

> [W]e hold that a person uses a computer "without authorization" under §§ 1030(a)(2) and (4) when the person has not received permission to use the computer for any purpose (such as when a hacker accesses someone's computer without any permission), or when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.

Id.

293. *Id.* at 1129, 1133.

opinion in *United States v. Nosal*,[294] which shed considerably more light on how the Ninth Circuit intends for *Brekka* to be read.

While it is an "exceeding authorized access case" rather than a "without authorization" case, the *Nosal* opinion is nevertheless instructive.[295] In *Nosal*, the employer had contractually defined its computer access and use restrictions from the outset, and the employee's subsequent violation of those restrictions was held to have exceeded his authorized access but was not without authorization.[296] The Ninth Circuit, in *Nosal*, focused on the distinction between without authorization and exceeds authorized access in distinguishing its *Brekka* and *Nosal* decisions;[297] this distinction has added a measure of clarity and structure to this issue.[298] That is, the court maintained the rationale of *Brekka*, that an insider, once given authorization, will not subsequently be treated as an outsider with no authorization absent a termination of that authorization by his or her grantor.[299] Thus, if such an insider is given unfettered authorization to access computers with no restriction, he will not be found to have exceeded any authorization unless the authorization is terminated or restricted before his disputed conduct occurs.[300] If the insider's authorization is limited beforehand, the violation of those limits will be deemed to have exceeded authorized access.[301]

b. "Exceeding Authorized Access"

The CFAA defines the phrase "exceeds authorized access" as "access[ing] a computer with authorization and [using] such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter[.]"[302] Even though this phrase is defined, its interpretation and application has proven to be fertile ground for litigation.[303] Congress originally intended to apply this branch of access to those who were likely to be insiders with some rights to access the computer.[304] The analysis, therefore, begins with the fact that initial access to the computer is authorized, as simple logic dictates that authorization that does not already exist cannot thereafter be exceeded. The granting of that authorization is often embodied in contractual agreements, and

294. 642 F.3d 781 (9th Cir. 2011).

295. *See id.* at 788.

296. *Id.* at 787, 789.

297. *Id.* at 786–88.

298. *See infra* text accompanying notes 328–334.

299. *Nosal*, 642 F.3d at 787 (citing LVRC Holdings, Inc. v. Brekka, 581 F.3d 1127, 1132 (9th Cir. 2009)).

300. *Id.*

301. *Id.* at 788.

302. 18 U.S.C. § 1030(e)(6) (2006).

303. *See, e.g.*, AtPac, Inc. v. Aptitude Solutions, Inc., 730 F. Supp. 2d 1174, 1181 (E.D. Cal. 2010) (interpreting the meaning of "exceeds authorized access" in the context of the CFAA).

304. *See supra* text accompanying note 261.

in many of the CFAA cases, that contractual relationship is between employer and employee.[305]

A straightforward example of an exceeds authorization case is *United States v. Czubinski*,[306] an early CFAA case in which an Internal Revenue Service employee was found to have exceeded his authorized access to IRS computer systems by looking at taxpayer records for his own personal, non-work related purposes.[307]

The First Circuit Court of Appeals, in *EF Cultural Travel BV v. Explorica, Inc.*,[308] was one of the first courts to use the rationale of the intended-use analysis in an exceeds authorized access case. In *EF Cultural*, the court found that a former employee exceeded authorized access when he used confidential information—in violation of his confidentiality agreement—obtained while working for his former employer to access the employer's website and gather pricing information.[309] In this case, the First Circuit addressed a situation in which former employees, who gained extensive knowledge of their employer's computer codes through their employment, took that knowledge and formed a new business that utilized a high-speed computer program to mine the former employer's public website for vital information.[310] The former employees had entered into an employment agreement with a broad confidentiality provision that protected their former employer's computer codes as proprietary information.[311] While the First Circuit has not ruled on this issue since 2001,[312] *EF Cultural* has not been overruled or criticized by the court, so one must assume that the First Circuit would still adhere to its rationale.

The Fifth Circuit Court of Appeals in *United States v. John*,[313] applied the intended-use analysis to find that access to a computer, as well as the permissible use of the information available from the computer, can be defined by the grantor's policies, and any access or use in violation of those policies exceeds authorized access.[314] The defendant in *John* worked for Citigroup as an account manager and was authorized to access the company's computer system containing customer account information.[315] Citigroup's policies prohibited the misuse of company computers and customer information.[316] The defendant obtained customer account information, which she provided to others to use for

305. *See* United States v. Phillips, 477 F.3d 215, 221 (5th Cir. 2007).
306. 106 F.3d 1069 (1st Cir. 1997).
307. *Id.* at 1071, 1078.
308. 274 F.3d 577 (1st Cir. 2001).
309. *Id.* at 579, 581.
310. *Id.* at 579–80.
311. *Id.* at 583.
312. *See id.* at 577.
313. 597 F.3d 263 (5th Cir. 2010).
314. *Id.* at 272–73.
315. *Id.* at 269.
316. *Id.* at 272.

making fraudulent charges.[317] The defendant was found guilty of violating the CFAA by exceeding authorized access to a protected computer.[318] The court, in upholding the conviction, found that a grantor of access can establish policies limiting *the use* of information obtained by permitted access to a computer system and the data available on that system, the violation of which exceeds authorized access.[319]

The Eleventh Circuit Court of Appeals, in *United States v. Rodriguez*,[320] applied the reasoning of the intended-use analysis to find that access to a computer can be defined by the grantor's policies and any access in violation thereof exceeds authorized access.[321] In *Rodriguez*, the court addressed a case in which an employee of the United States Social Security Administration had improperly accessed personal information that he was authorized to access for business purposes, but did so for non-business purposes, in violation of the Administration's policy.[322] Rodriquez was indicted and a jury found him guilty on all counts.[323] The Eleventh Circuit held that "Rodriguez exceeded his authorized access and violated the [CFAA] when he obtained personal information for a nonbusiness reason."[324] The court reasoned that because the Administration had a clear policy prohibiting such conduct, when he violated the policy, he therefore exceeded his authorized access.[325] *Rodriguez* is an application of the intended-use theory in that the grantor of access, the Administration, had implemented policies that limited the authorization of access to work computers for business reasons only.[326] When Rodriguez used his access to the computer for non-business reasons, he exceeded the intended-use as defined by the policies and, therefore, exceeded his authorized access and violated the CFAA.[327]

The most recent case in this line of exceeds authorized access cases is *United States v. Nosal*.[328] With *Nosal*, the Ninth Circuit joined the Fifth and Eleventh, and likely First and Second, Circuits by holding that a grantor of authorization may, through its policies, set restrictions defining the limited circumstances under which access and use is permitted; an access or use in

317. *Id.*
318. *Id.* at 269–70.
319. *Id.* at 272–73.
320. 628 F.3d 1258 (11th Cir. 2010).
321. *See id.* at 1263.
322. *Id.* at 1260.
323. *Id.* at 1262.
324. *Id.* at 1263.
325. *Id.*
326. *Id.*
327. *Id.* In *United States v. Salum*, the Eleventh Circuit Court of Appeals reached a similar conclusion where it found that although the defendant may have had authority to access a computer database, there was sufficient evidence to establish that the defendant exceeded his authority by accessing it for an improper purpose. 257 F. App'x 225, 230 (11th Cir. 2007).
328. 642 F.3d 781 (9th Cir. 2011).

violation of those restrictions then exceeds authorized access.[329] The court explained that the holding of *Nosal* was merely an application of the *Brekka* reasoning that requires the decision to allow or terminate the employee's authorization to come from the employer, not the employee.[330] Here, the employer was not terminating the authorization, but placing limitations on access.[331] To ensure that it was not confusing the distinction between access without authorization and exceeds authorized access, the *Nosal* court was explicit in stating that in this case such a violation is in excess of authorization:

> Our decision today that an employer's use restrictions define whether an employee "exceeds authorized access" is simply an application of *Brekka*'s reasoning. As we held in that case, "[i]t is the employer's decision to allow or to terminate an employee's authorization to access a computer that determines whether the employee is with or 'without authorization.'" Based on the "'ordinary, contemporary, [and] common meaning'" of the word "authorization," we held that "an employer gives an employee 'authorization' to access a company computer when the employer gives the employee permission to use it[.]" Therefore, the *only* logical interpretation of "exceeds authorized *access*" *is that the employer has placed* limitations on the employee's "permission to use" the computer and the employee has violated—or "exceeded"—those limitations.[332]

The circuit courts have decided numerous exceeds authorized access cases; however, with the Ninth Circuit's recent *Nosal* decision explaining the *Brekka* decision, the picture just may be coming into focus more clearly, though the circuits are far from settling on a unified approach. Prior to *Nosal*, the different approaches that the circuit courts have applied to the without authorization analysis are generally those that have been applied to the exceeds authorization cases as well, in no small part due to the fact that clearly differentiating between the two has not always been a primary focus of the analytical process.[333] However, with the *Nosal* opinion, the Ninth Circuit made clear that, while the access means access theory remains in effect for without authorization cases, it does not apply to exceeds authorized access cases.[334] Instead, for those cases, the Ninth Circuit adopted the intended-use analysis of the Fifth and Eleventh Circuits, as used most recently, and quite possibly the First and Second Circuits,

---

329. *See id.* at 788–89 (citing *Rodriguez*, 628 F.3d at 1263; United States v. John, 597 F.3d 263, 271 (5th Cir. 2010)).

330. *Id.* at 787 (citing LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009)).

331. *Id.* at 783.

332. *Id.* at 787 (citations omitted) (quoting *Brekka*, 581 F.3d at 1132–33).

333. *See supra* Part III.D.4. The three theories are the "agency theory," the "intended-use analysis," and the "access means access theory." *See supra* text accompanying notes 274–277.

334. *Nosal*, 642 F.2d at 787.

though those courts have not addressed the issue for quite some time.[335] Thus, there now appear to be only two viable theories for exceeds authorization cases: agency theory or intended-use analysis.

5. *"Damage," "Loss," "Damages," for Civil Claims?*

In terms of both complexity and frequency litigated, the competition is close between the issues of access and damages. Section 1030(g) of the CFAA seems simple enough in that it provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[336] The proverbial devil is in the details, however, as the CFAA then incorporates definitions, qualifications, and limitations by cross references to other subsections of the CFAA.[337] This section implicitly sets forth the minimum threshold of damages or loss necessary to bring a civil claim, as well as the types of remedies that are available in a civil claim, and additional procedural requirements and limitations for those remedies.[338] It should be noted at the outset that the terms "damage" and "loss" are jurisdictional terms of art and do not limit the damages that are ultimately recoverable.[339] Given this complexity, it is best to start the analysis by looking at the statutory language:

> Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.[340]

Because a civil action is only available if the violation involves at least one of five subsection (c)(4)(A)(i) factors,[341] that is necessarily the starting point in the analysis.[342]

---

335. *See id.*

336. 18 U.S.C. § 1030(g) (2006).

337. *Id.* (referencing § 1030(c)(4)(A)(i)(I)–(V) (Supp. IV 2010)).

338. *Id.*

339. Frees, Inc. v. McMillian, No. 05-1979, 2007 WL 2264457, at *5 (W.D. La. Aug. 6, 2007).

340. 18 U.S.C. § 1030(g) (Supp. IV 2010) (footnote omitted).

341. § 1030 (g) (Supp. IV 2010). The five specified factors are as follows:

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

Of these five factors, the single factor that is almost exclusively relied upon for private civil matters is where the statutory violation caused (or would have caused) a loss to one or more persons in any one year period aggregating at least $5,000.[343] Damages for a violation of this factor are limited to only economic damages.[344] Before moving deeper into this analysis, a summary of the requirements for bringing a civil claim thus far in the analysis will be helpful.

Any person who suffers damage or loss caused by a violation of the CFAA may bring a civil claim against the person violating the CFAA to obtain compensatory damages, injunctive relief, or other equitable relief.[345] However, the claim can only be brought if the conduct violated one of the factors set forth in subsection (c)(4)(A)(i) of the CFAA.[346] In most business cases, the only factor that is usually available is where the violation caused loss to one or more persons during any one year period that is at least $5,000 in the aggregate,[347] and in such cases, the only damages that can be recovered are economic damages.[348] Thus, a plaintiff who can establish the threshold loss of a $5,000 is only entitled to sue for economic damages.[349]

a. Meeting the $5,000 Threshold for a Civil Claim

In order to bring a civil claim under the CFAA in most business cases, a plaintiff must plead that, during any one year period, one or more persons sustained loss of at least $5,000 because of the CFAA violation.[350] This

---

(II) the modification or impairment, or potential modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security[.]

§ 1030(c)(4)(A)(i)(I)–(V) (Supp. IV 2010).

342. *See* Ipreo Holdings LLC v. Thomson Reuters Corp., No. 09-CV-8099(BSJ), 2011 WL 855872, at * 6–7 (S.D.N.Y. Mar. 8, 2011) (quoting Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010)).

343. *See* § 1030(c)(4)(A)(i)(I). The other potential qualifying factors—impairment of medical diagnosis or treatments, physical injury, public health or safety, or United States Government computers—are all exempted from the $5,000 loss requirement. Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 646 n.2 (E.D. Va. 2010). The aforementioned factors would not often arise in *most* business cases, though, of course, there will be exceptions to this overly broad statement.

344. § 1030(g) (2006).

345. A.V. *ex rel* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009) (citing § 1030(g)).

346. § 1030(g).

347. *See supra* text accompanying note 343.

348. § 1030(g).

349. *Id.*

350. *Id.*

requirement is essential to meeting the jurisdictional threshold for the court to hear the claim, and was purposefully implemented by Congress to keep from clogging the courts with trivial cases by "limit[ing] federal jurisdiction to cases of substantial computer crimes."[351] Many of the CFAA cases that are dismissed for failure to adequately state a claim are dismissed because the plaintiff has not met this threshold pleading requirement.[352] Thus, whether prosecuting or defending a CFAA claim, it is important to carefully examine the allegations pled to ensure compliance with this threshold requirement. Simply reciting the language of the statute may suffice for some courts.[353] However, the failure to adequately plead a loss can be fatal to a claim.[354] The courts do not have jurisdiction to decide the case unless the $5,000 threshold loss is properly pled, even when it is obvious that the economic damages are in the millions.[355]

The term loss is defined by the CFAA as:

> [A]ny reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service[.][356]

A reading of the statutory language makes it clear that unless there has been an interruption of service, only "costs" can qualify as a loss.[357] A prospective plaintiff that has been harmed by a violation of the CFAA, that is not an interruption of service, and intends to assert a claim under the CFAA should

---

351. *In re* Doubleclick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 522 (S.D.N.Y. 2001).

352. *See supra* text accompanying notes 208–209.

353. *See* Lapp Insulators LLC v. Gemignani, No. 09-CV-0694A(Sr), 2011 WL 1198648, at *8 (W.D.N.Y. Mar. 9, 2011). In this case, the plaintiff "allege[d] that it ha[d] suffered damage and loss . . . in an amount to be determined at trial, but not less than $5,000." *Id.* (citation omitted). Based on this allegation, the court held that the plaintiff "alleged loss and unauthorized access sufficient to withstand the instant motion to dismiss." *Id.*

354. *See* Garelli Wong & Assocs., Inc. v. Nichols, 551 F. Supp. 2d 704, 710–11 (N.D. Ill. 2008); *see also* M-I LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010) (holding that plaintiff failed to allege facts showing at least $5,000 of loss); Mktg. Tech. Solutions, Inc. v. Medizine LLC, No. 09 Civ. 8122(LMM), 2010 WL 2034404, at *7 (S.D.N.Y. May 18, 2010) (holding that the complaint was inadequate for failure to "allege with some particularity the 'damage' and 'loss' (as defined in the CFAA) claimed to be involved, with, moreover, facts showing that the $5,000 threshold of Section 1030(a)(4) is satisfied").

355. *See* Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 770, 776 (S.D. Tex. 2010).

356. 18 U.S.C. § 1030(e)(11) (2006).

357. *Stelly*, 733 F. Supp. 2d at 780 ("[C]ase law has consistently interpreted the loss provision to encompass only the costs incurred as a result of investigating or remedying damage to a computer, or costs incurred because the computer's service was interrupted.").

understand the need to conduct a thorough investigation, to undertake sufficient remedial measures, or do both such that it meets the $5,000 loss requirement.[358]

Once the plaintiff has incurred the requisite $5,000 loss, it is required to plead with some particularity the factual allegations establishing that its loss is sufficient to meet this $5,000 minimum threshold.[359] While the subsection authorizing civil claims uses the terms loss and damage, the (c)(4)(A)(i)(I) factor limitation only refers to loss, not damage.[360] Given this language, it appears that the damage prong is irrelevant for these types of business litigation cases.[361] Nonetheless, the term damage is defined by the statute and means "any impairment to the integrity or availability of data, a program, a system, or information[.]"[362]

To further complicate this issue, there are two categories of losses as well: response costs and interruption of service damages.[363] The most frequently used losses are response costs.[364] There is no requirement that there be both response costs and interruption of service—either will suffice.[365] Regardless of whether the alleged loss is for response costs or interruption of service, it must be adequately proven.[366] In *Global Policy Partners, LLC v. Yessin*,[367] the United States District Court for the Eastern District of Virginia provided an excellent

---

358. *See id.* (dismissing plaintiff's claim for failure to "allege facts showing at least $5,000 of loss, or any loss as a result of investigation or interruption of computer service").

359. *Mktg. Tech. Solutions*, 2010 WL 2034404, at *7. It is interesting to note that courts have held that the pleading requirement for a CFAA claim is not subject to the heightened pleading requirements of Rule 9 for claims of common law fraud. *See supra* text accompanying notes 171–173. It now appears, however, as though the requirement for pleading the threshold loss or damage under § 1030(a)(4) may in some courts be evolving to such a heightened pleading standard. *Compare Mktg. Tech. Solutions*, 2010 WL 2034404, at *7, *and supra* note 172, *with supra* note 353 and accompanying text.

360. § 1030(c)(4)(A)(i)(I) (Supp. IV 2010).

361. White Buffalo Ventures, LLC v. Univ. of Tex., 420 F.3d 366, 378 n.24 (5th Cir. 2005) ("Even in the CFAA context, however, courts rely on the 'loss' rather than the 'damage' language in the statute."); *see also* Mortensen v. Bresnan Commc'n, L.L.C., No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *7 (D. Mont. Dec. 13, 2010) (stating that "'loss' is treated differently from 'damage'" (quoting § 1030(e)(11) (2006))).

362. § 1030(e)(8).

363. Alliantgroup, L.P. v. Feingold, No. H–09–0479, 2011 WL 1157315, at *15 (S.D. Tex. Mar. 24, 2011) ("The term 'loss' encompasses only two types of harm: costs to investigate and respond to an offense, and costs incurred because of a service interruption." (citing Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010))); *see also* § 1030(e)(11).

364. *See infra* Part III.D.5.b.

365. *See* Lapp Insulators LLC v. Gemignani, No. 09–CV–0694A(Sr), 2011 WL 1198648, at *7 (W.D.N.Y. Mar. 9, 2011); AssociationVoice, Inc. v. AtHomeNet, Inc., No. 10-cv-00109-CMA-MEH, 2011 WL 63508, at *7 (D. Colo. Jan. 6, 2011) ("Only those costs in the second half of the definition need to relate to an interruption of service. Costs that need not relate to an interruption include 'the cost of responding to an offense' and 'conducting a damage assessment.'" (citing § 1030(e)(11))).

366. Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 646 (E.D. Va. 2010) (citing § 1030(c)(4)(A)(i) (Supp. III 2009)).

367. *Id.*

analysis of the "qualifying-loss" requirement and guidelines.[368] Citing the Fourth Circuit in *A.V. v. iParadigms, LLC*,[369] the court observed that the loss definition is broadly worded and contemplates costs incurred as part of the response to a CFAA violation, including the investigation of an offense.[370]

The plaintiff must also show "that the costs are 'reasonable' and that they were 'caused' by a CFAA violation."[371] The court reasoned that the CFAA incorporates traditional principles of tort causation requiring that plaintiffs must "show that the losses they claim were the reasonably foreseeable result of the alleged CFAA violations, and that any costs incurred as a result of measures undertaken" to restore data, program, system, or information "were reasonably necessary in the circumstances."[372] The question of reasonableness is often one that invokes questions of practical, rather than legal judgment; it is therefore usually treated as a question of fact that is left for the jury to decide.[373] It should be noted, however, that when the defendant makes it difficult to discover his identity, the extent of the unauthorized access, methods used to obtain access, or activities undertaken therein, the defendant should not be allowed to complain about the reasonableness of the costs the plaintiff must then incur to investigate these matters.[374] The plaintiff is not required, however, to show that there was actual damage caused in order for the costs to be reasonable.[375] For example, when the plaintiff incurs costs for investigating a violation, even though it may later turn out there was no actual damage caused by the violation, that turn of events alone will not negate the reasonableness of the costs.[376]

b. Specific Examples of What Has and Has Not Constituted a Loss

As with the access issue, courts are taking different positions on what types of costs are qualifying costs for purposes of loss. For each type of cost, with enough research, one can likely find case law that permits it to qualify and case law that holds it does not. Listed below are several examples of specific losses that have been argued to fit within the CFAA's definition of loss. Some have

368. *See id.* at 646–48 (citations omitted).

369. 562 F.3d 630 (4th Cir. 2009).

370. *Yessin*, 686 F. Supp. 2d at 647 (citing A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009)).

371. *Id.* (citing *iParadigms, LLC*, 562 F.3d at 646).

372. *Id.* (citing United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000)).

373. 1st Rate Mortg. Corp. v. Vision Mortg. Servs. Corp., No. 09-C-471, 2011 WL 666088, at *3 (E.D. Wis. Feb. 15, 2011); *see also* Ipreo Holdings LLC v. Thomson Reuters Corp., No. 09 Cv. 8099(BSJ), 2011 WL 855872, at *7 (S.D.N.Y. Mar. 8, 2011).

374. AssociationVoice, Inc. v. AtHomeNet, Inc., No. 10-cv-00109-CMA-MEH, 2011 WL 63508, at *8 (D. Colo. Jan. 6, 2011).

375. *Ipreo Holdings LLC*, 2011 WL 855872, at *7 ("[T]he costs of investigating security breaches constitute recoverable losses, even if it turns out that no actual data damage or interruption of service resulted from the breach." (quoting Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010))).

376. *See id.* (citing *Univ. Sports Publ'ns Co.*, 725 F. Supp. 2d at 387).

been successful and some have not. For many of them, however, it is important to bear in mind that different courts have found differently in different cases and circumstances, which can be said for each of these examples. The categorization listed below simply represents the Author's view of how these issues are *usually* decided. Given the continuously evolving nature of this issue, however, there is no doubt that any given court on any given occasion could find differently.

The CFAA's definition of loss clearly states that costs are what is contemplated.[377] This has been interpreted to mean "any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made."[378] Included within this category have been costs incurred to assess the damage to a computer or to files stored on the computer,[379] costs to conduct a forensic analysis and investigation,[380] and to have diagnostic measures performed.[381] "[R]etaining specialized services that report and record the cyber-attacks and their origins" has been found to be a loss, as well as "security enhancements to Plaintiff's computer systems" to prevent future incursions.[382] Likewise, costs associated with investigating the offender's identity and means of access are considered a loss.[383] Costs to repair damage to the computer data qualifies as a loss.[384] It is well settled that the value of time for employees who investigate the access qualifies as a loss.[385] Moreover, some courts may permit losses to be aggregated in some circumstances,[386] though others may not.[387]

The category of claims not usually qualifying as a loss begins with one often argued, but not often successful: lost revenue due to a former employee's transfer of trade secrets.[388] Likewise, the value of misappropriated trade secret

---

377. 18 U.S.C. § 1030(e)(11) (2006).

378. Lapp Insulators LLC v. Gemignani, No. 09-CV-0694A(Sr), 2011 WL 1198648, at *7 (W.D.N.Y. Mar. 9, 2011) (quoting Penrose Computer Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 208 (N.D.N.Y. 2010)) (internal quotations omitted).

379. *Ipreo Holdings LLC*, 2011 WL 855872, at *7; Patrick Patterson Custom Homes, Inc. v. Bach, 586 F. Supp. 2d 1026, 1036 (N.D. Ill. 2008).

380. *Lapp Insulators LLC*, 2011 WL 1198648, at *7.

381. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir. 2001).

382. Integrated Waste Solutions, Inc. v. Goverdhanam, No. 10-2155, 2010 WL 4910176, at *9 (E.D. Pa. Nov. 30, 2010) (citation omitted).

383. AssociationVoice, Inc. v. AtHomeNet, Inc., No. 10-cv-00109-CMA-MEH, 2011 WL 63508, at *7 (D. Colo. Jan. 6, 2011); *see also* SuccessFactors, Inc. v. Softscape, Inc., 544 F. Supp. 2d 975, 980–81 (N.D. Cal. 2008) (citations omitted).

384. *Patrick Patterson Custom Homes, Inc.*, 586 F. Supp. 2d at 1036.

385. *See AssociationVoice, Inc.*, 2011 WL 63508, at *8.

386. *See* Mortensen v. Bresnan Commc'n, L.L.C., No. CV 10-13-BLG-RFC, 2010 WL 5140454, at *7 (D. Mont. Dec. 13, 2010) (citing *In re* Apple & AT & TM Antitrust Litigation, 596 F. Supp. 2d 1288, 1308 (N.D. Cal. 2008); *In re* Toys R Us, Inc., Privacy Litigation, No. 00-CV-2746, 2001 WL 34517252, at *11 (N.D. Cal. 2001)).

387. *See* LaCourt v. Specific Media, Inc., No. SACV10–1256–GW(JCGx), 2011 WL 1661532, at *6 & n.4 (C.D. Cal. Apr. 28, 2011).

388. *See* Advantage Ambulance Grp., Inc. v. Lugo, No. 08-3300, 2009 WL 839085, at *1, 4 (E.D. Pa. Mar. 30, 2009).

information is not usually considered a loss even if it is extremely valuable because, despite its value, it constitutes neither a cost to investigate and respond to a computer intrusion nor a cost associated with a service interruption.[389] Predictably, not all courts rule this way; it has been held that "loss of confidential and proprietary information for the benefit of defendants' competing enterprise" is considered to be a loss,[390] thus demonstrating the uncertain nature of this issue. Also not typically considered a loss, are lost profits, loss of customers, and loss of future business opportunities.[391] While these may certainly be legitimate costs and expenses, they do not qualify because they do not assert "damages whatsoever relating to [an] investigation of computer damage, or costs incurred because any computer service was interrupted."[392] While there are many more costs, these are only a few examples that are included to emphasize the point that this body of law is still evolving and there are many uncertainties. These uncertainties require that the litigators who will be going to battle over these claims keep abreast of how the law continues to evolve.

IV. CONCLUSION

Fraud 2.0—it's here to stay. Computers are an integral part of our personal and business lives and they are used for nearly everything. Given the breadth of what is considered a computer under the CFAA,[393] it takes little effort to comprehend that indeed everything does have a computer in it. Just as computers have become the instruments of war among nations, so too have they in the business world. Business and war, whether they truly are one in the same is a matter of perspective, but they each have the same objective—to win, to defeat the enemy.

In the business world, there are scores of business competitors, as well as skilled individuals, who pose a threat to businesses from subversive activities that they can easily cause with computers. Chief among their activities is using computers as artifices of fraud. This threat will not go away until there is something more efficient than a computer to replace it as their weapon of choice. Why? Because for some it is just part of their human nature to do anything to get what they desire, regardless of how dishonest of means they must employ. Because computer fraud is a very lucrative business, it incentivizes the dishonest to continue to adapt their techniques and find more efficient means of

389. *See* Quantlab Techs. Ltd. (BVI) v. Godlevsky, 719 F. Supp. 2d 766, 776 (S.D. Tex. 2010) (citations omitted).

390. Res. Ctr. for Indep. Living, Inc. v. Ability Res., Inc., 534 F. Supp. 2d 1204, 1211 (D. Kan. 2008); *see also* Meats by Linz, Inc. v. Dear, No. 3:10-CV-1511-D, 2011 WL 1515028, at *3 (N.D. Tex. Apr. 20, 2011).

391. M-I LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010).

392. *Id.* at 780.

393. *See* 18 U.S.C. § 1030(e)(1) (2006).

accomplishing their reprehensible purposes. The epidemic of computer fraud will certainly continue to increase.[394]

Right now, somewhere, someone is directing a computer fraud attack against businesses that will cause them harm. Those businesses will seek help and guidance from litigators. Many of these situations will result in courtroom battles where attorneys will serve as their clients' generals. The companies will look to these generals to direct this battle as efficiently as possible, using the most effective weapons available. In all likelihood, the battle will involve the CFAA.

In such a situation, an attorney's understanding of the CFAA will prove invaluable. The CFAA is a highly complex federal law that provides civil remedies for economic damages, equitable relief, and perhaps most important of all, injunctive relief that, when properly used, can end a battle almost as quickly as it begins. This is very powerful. However, the CFAA's complexity makes it a veritable mine-field of procedural and substantive requirements that must be satisfied in order to successfully assert and ultimately prevail on a CFAA claim. To add to its complexity, the CFAA is a relatively new body of law and its jurisprudence is continuing to evolve in a way that often makes its provisions unpredictable from case to case and court to court No one can predict exactly how courts will apply the CFAA to each case, for it is not static. There are few well-settled rules for the CFAA. Regardless of how skilled a litigator one may be, in order to be adequately prepared, the attorney must not only have an appreciation of this fact, but also have enough of an understanding of how the CFAA works to be able to argue the reasoning for how and why certain rules *should* apply.

Sun Tzu was correct: in every battle, preparation is indeed the key to winning.[395] Because of the CFAA's complexity, unsettled evolving nature, and the great many cases interpreting and applying it, both time and effort are required to adequately prepare for this battle. Accordingly, the litigator should prepare himself beforehand—he should "mak[e] many calculations in his temple before the battle is fought"[396] to be the general who wins. That is what clients expect and deserve from their litigators: to be prepared and, more often than not, to win.

Will you, as your client's general, be prepared for this battle?

---

394. *See* INTERNET CRIME COMPLAINT CENTER, 2010 INTERNET CRIME REPORT 7, 9 (2011), *available at* http://www.ic3.gov/media/annualreport/2010_IC3Report.pdf (reporting an increase from 231,493 complaints in 2005 to over 300,000 complaints in 2010, 9.1% of which were Computer Crimes).

395. *See* SUN TZU *supra* note 4, at 12.

396. *Id.*

*