CONTENTS

ABSTRACTS

ARTICLES

THE COMPUTER FRAUD AND ABUSE ACT: REVENUE PROTECTION WEAPON FOR AIRLINES           Kenneth S. Nankin

THE IMPOTENCE OF THE CHICAGO CONVENTION’S DISPUTE SETTLEMENT PROVISIONS               Gabriel S. Sanchez

CODE-SHARING IN THE U.S. AIRLINE INDUSTRY: EFFECTIVE DISCLOSURE REQUIREMENTS FOR AN ASPECT OF AIR TRANSPORT THAT IS COMPLEX, IMPORTANT, AND OFTEN MISUNDERSTOOD       Daniel Friedenzohn

AIRLINE MERGERS – RESPONDING TO MARKET CHANGES AND INDUCING NEW MARKET STRUCTURES       Iva Savić

UNITED + CONTINENTAL IS A MARKET SOLUTION THAT CAN BENEFIT ALL STAKEHOLDERS – IS AMERICAN + US AIRWAYS NEXT?        Paul Mifsud, Carlos Bonilla, and Vaughn Cordle

MODERN APPROACHES TO THE POWERS OF THE AIRCRAFT COMMANDER UNDER ARTICLE 6 OF THE TOKYO CONVENTION          Aaron B. Swerdlow

THE AIR TRANSPORT ASSOCIATION’S CHALLENGE TO THE EUROPEAN UNION’S EXTENSION OF ITS EMISSIONS TRADING SCHEME TO INTERNATIONAL AVIATION: A LEGAL ANALYSIS          Matthew D. Kasper
The Computer Fraud and Abuse Act: Revenue Protection Weapon for Airlines

by Kenneth S. Nankin*

Until the last few years, airlines sustained significant revenue losses from "bust-outs" by Airlines Reporting Corporation (ARC)-accredited travel agencies. In a bust-out, an agency's owners validate and sell vast numbers of tickets in a short period of time to individuals and other agencies, fail to report the sales to ARC, and disappear with the proceeds.1 Due to technological innovations and aggressive enforcement activities, primarily driven by ARC, bust-outs are now comparatively rare.

Airlines still suffer revenue losses from ticket-related fraud, but now that type of fraud mostly results from online conduct by persons who are not affiliated with ARC agencies. Online fraud, primarily the illicit sale of tickets purchased over the Internet by persons using stolen credit and debit card numbers, is a significant source of revenue loss for airlines. This past summer, federal authorities charged thirty-eight defendants "in a series of indictments that allege an extensive network of black market travel

---

* Kenneth S. Nankin is a partner with Nankin & Verma PLLC, a law firm based in Bethesda, Maryland. He has been representing airlines since starting practice in 1988. He litigates against travel agents and others in cases involving unreported and underreported sales, unauthorized reservations and sales, refund and exchange fraud, abusive ticketing practices, stolen tickets, and frequent flyer mileage and award brokering. He also defends airlines against personal injury, delay, baggage, and cargo claims, litigates contract claims for airlines in cases involving vendors, leasing companies, and freight forwarders, and pursues airline claims for aircraft hull damage repair costs and lost revenues arising from ground incidents. Mr. Nankin analyzes airline industry legal developments on his Internet weblog, The NV Flyer, at www.nvflyer.com. He is a member of the Bars of the District of Columbia, Maryland, New York, and Virginia. He graduated from Harvard Law School and received his undergraduate degree from Washington and Lee University.

agents who used the stolen identities of thousands of victims as part of a multi-million dollar fraud scheme to purchase airline tickets for their customers.\textsuperscript{2} Losses from this scheme allegedly exceeded $20 million.\textsuperscript{3} According to one survey, airlines suffered losses of over $1.4 billion in 2008 due to online fraud.\textsuperscript{4}

Airlines also sustain online-related revenue losses from fraud by frequent flyer mileage brokers and website abuse by “screen scraper” travel information providers. Ironically, just as technology was instrumental in reducing the incidence of bust-outs, it is technology, mainly in the form of the Internet, which makes these other forms of fraud and abuse possible.

Alaska Airlines’ recent successful use of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (CFAA), in federal court against a defiant, long-time frequent flyer mileage broker demonstrates that the Act can be effectively used to combat online fraud and abuse. Having the CFAA as a gateway to federal court, through federal question jurisdiction under 28 U.S.C. § 1331, is particularly important for airlines because, in general, cases move more quickly, and summary judgment is more readily available, in federal district courts than in state courts. Moreover, airlines can no longer depend as heavily as they once did on federal trademark infringement or other Lanham Act causes of action to obtain federal question jurisdiction, as mileage brokers appear to be lessening their use of airline logos, trade names, and other trademarks on their websites in an effort to avoid drawing airlines’ attention.\textsuperscript{5}

A CFAA cause of action can serve as a powerful weapon, but, in general, courts are cautious about using the CFAA in a civil

\textsuperscript{2} News Release, Office of the U.S. Att’y, W. Dist. of Mo., Black Market Travel Agents – 38 Defendants Indicted in Multi-Million Dollar Fraud (July 9, 2010), available at www.justice.gov/criminal/cybercrime/bowers

\textsuperscript{3} Id.


\textsuperscript{5} For a fairly recent example of what can happen to the broker who prominently makes use of an airline’s trademarks to perpetuate a fraud against the airline, see Northwest Airlines, Inc. v. Bauer, 467 F. Supp. 2d 957 (D.N.D. 2006). In that case, Northwest was able to obtain a temporary restraining order under the Lanham Act against a discount coupon broker who was conducting his brokering business via a website with the domain name “northwestdiscountcoupons.com.” Northwest then proceeded to steamroll right along, obtaining a preliminary injunction and then a permanent injunction, both with the defendants’ consent.
setting and thoroughly scrutinize evidence offered by a plaintiff in support of its CFAA cause of action. As a result, an airline must make sure that its website’s terms of use are correctly set up so they can help support a CFAA cause of action, and as soon as online-based fraud or abuse is detected, an airline needs to take steps to ensure that it will be able to prove the elements of a CFAA cause of action, particularly with respect to the “loss” element, which various federal courts have construed differently. These protective measures are discussed in detail below.

I. Introduction to the Act

In the early 1980s, computer hackers began to penetrate government and private computer systems. Gradually, the public began to become aware of these shadowy figures, who used a combination of telephones and “social engineering” (trickling people into disclosing information) to hack into computer systems and steal information or cause damage.

Oddly, Hollywood provided a major impetus for legislative change to address the hacker problem. In 1983, the movie “War-Games” was released, and it dramatically increased the public’s – and Congress’ – awareness of computer hacking. In the movie, a high school-age computer geek unknowingly hacks into a NORAD computer system using his personal computer and a telephone and nearly causes a global nuclear war. Partly as a result of this movie, and its far-fetched premise that a teenage hacker could cause the launch of nuclear missiles, Congress enacted the CFAA, which was then called the “Counterfeit Access Device and Computer Fraud and Abuse Act of 1984.”

The Report of the House Committee on the Judiciary summarized the need for the legislation as follows: “The committee concluded that the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access to them, require a clearer statement of proscribed activity.”

For those who doubt that a movie featuring the escapades of Matthew Broderick and Ally Sheedy spurred the enactment of federal computer crime legislation, see H.R. Rep. No. 98-894, at 6 (1984), reprinted in 1984 U.S.C.C.A.N. 3689, 3695 (“For example, the motion picture ‘War Games’ [sic] showed a realistic representation of the automatic dialing and access capabilities of the personal computer.”).

The goal of articulating a "clearer statement of proscribed activity" has been difficult for Congress to achieve, and, as a result, it has repeatedly amended the CFAA over the years. The amendments have caused the Act's reach to broaden substantially, just as the prevalence of computers themselves has increased. For example, the CFAA initially was a criminal statute only. In 1994, Congress amended the Act to add a civil cause of action, which is now codified at 18 U.S.C. § 1030(g), under which victims of computer fraud or abuse can assert claims against violators of the statute. Also, the statute was originally intended to control interstate computer crime only, but, with the development of the Internet, virtually all computer use has become interstate use and thus subject to the Act.8

II. The Act's Civil Cause of Action

Although the CFAA prohibits seven separate types of activities,9 airline plaintiffs typically proceed against offenders under Section 1030(a)(4), which prohibits a person from "knowingly and with intent to defraud, access[ing] a protected computer without authorization, or exceed[ing] authorized access, and by means of such conduct further[ing] the intended fraud and obtain[ing] anything of value."

The Act defines a "protected computer" as a computer "which is used in or affecting interstate or foreign commerce or communication."10 Thus, as noted above, the Act covers, in essence, any computer that is connected to the Internet, which means that it covers virtually all modern computers.11 Certainly, any computer that hosts an airline's website or frequent flyer mileage program constitutes a "protected computer" under the Act.

To prevail on a claim under Section 1030(a)(4), an airline plaintiff must prove that the defendant caused a "loss" to the airline "during any 1-year period . . . aggregating at least $5,000 in

---

8 "[T]he original version of the CFAA did not intend to enact sweeping federal jurisdiction. However, the CFAA was intended to control interstate computer crime, and since the advent of the Internet, almost all computer use has become interstate in nature." Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).
value." The Act defines the term "loss" as "any 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." The "cost of responding to an offense" includes the "consequential" costs incurred in investigating an offense and taking remedial measures in response to it.

An airline plaintiff that has sustained a "loss" through violations of the Act is entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." Actions must be brought within two years of the offensive conduct or the date of the discovery of the actionable damage.

III. History of Cases Brought by Airlines Under the Act

In court, airlines have had some successes with CFAA causes of action. Although issues regarding whether defendants have accessed airline computers "without authorization" or have "exceed[ed] authorized access" have been litigated in several cases, the primary battleground has been the issue of whether the airline plaintiff has been able to prove that it sustained a "loss" within the meaning of Section 1030(c)(4)(A)(i)(I).

A. Southwest's Cases

Of all airlines, Southwest Airlines has been, by far, the most active in bringing CFAA causes of action in court. Southwest's

---

14 See A.V. ex rel. Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009) ("This broadly worded provision plainly contemplates consequential damages of the type sought by iParadigms - costs incurred as part of the response to a CFAA violation, including the investigation of an offense.") (citations omitted).
15 18 U.S.C. § 1030(g).
16 Id.
17 In addition to the three cases discussed infra, Southwest has pursued CFAA causes of action in at least the following cases: Southwest Airlines Co. v. Infare Solutions A/S, Case No. 3:10-cv-01674 (N.D. Tex.) (filed Aug. 26, 2010); Southwest Airlines Co. v. Checkinsooner.com, LLC, Case No. 3:10-cv-1512 (N.D. Tex.) (filed Aug. 3, 2010); Southwest Airlines Co. v.
experiences in litigating the "loss" element of the CFAA cause of action in the three cases are instructive.

Southwest v. FareChase. In 2003, Southwest sued a software company that developed and licensed software that had the ability to send out "a robot, spider, or other automated scraping device" via the Internet to obtain fare, route, and schedule information from southwest.com, as well as a company that was using such software, pursuant to a license, for use by its corporate traveler customers. In its complaint, Southwest claimed that the defendants' activities directed at southwest.com were unauthorized and were deceiving Southwest's customers by providing them with incomplete and inaccurate information. Southwest alleged twelve causes of action in its complaint, including a CFAA cause of action.

The defendant that had been using the software moved to dismiss, among other things, Southwest's CFAA claim pursuant to Federal Rule of Civil Procedure 12(b)(6) because the complaint supposedly had failed to adequately allege "loss" and unauthorized access to southwest.com. The court rejected both arguments.

As to the "loss" issue, the court held that, because the complaint alleged "loss" aggregating at least $5,000 pursuant to Section 1030(e)(1)(I), Southwest did not need to also allege "damage" to its computer or data pursuant to Section 1030(e)(8), as the defendant had contended. The court also held that Southwest had adequately alleged unauthorized access under the CFAA because southwest.com's Use Agreement, which was accessible from all pages on the site, specifically informed users that the use of "automated scraper devices" on the site was prohibited.

Smith, Case No. 3:07-cv-1883 (N.D. Tex.) (filed Nov. 9, 2007); Southwest Airlines Co. v. Sharif, Case No. 3:07-cv-1271 (N.D. Tex.) (filed July 17, 2007); Southwest Airlines Co. v. Carameros, Case No. 3:07-cv-1149 (N.D. Tex.) (filed June 26, 2007); Southwest Airlines Co. v. Sternberg, Case No. 2006-cv-1326 (S.D. Tex.) (filed Apr. 18, 2006); Southwest Airlines Co. v. Seward, Case No. 4:06-cv-1327 (S.D. Tex.) (filed Apr. 18, 2006); Southwest Airlines Co. v. QL2 Software, Case No. 3:05-cv-1588 (N.D. Tex.) (filed Aug. 5, 2005); Southwest Airlines Co. v. The Travel Company, Case No. 3:05-cv-207 (N.D. Tex.) (filed Jan. 28, 2005).

18 Id.
19 Id. at 439.
20 Id.
Southwest v. BoardFirst. In 2006, Southwest sued BoardFirst to prevent it from continuing to assist Southwest customers trying to obtain “A” boarding passes, which allow the holder to board flights earlier during the boarding process. Southwest customers would provide their name, flight confirmation number, and credit card information to BoardFirst. BoardFirst personnel then would log onto Southwest’s website using the customer’s personal information and attempt to secure an “A” boarding pass. If BoardFirst obtained an “A” pass, the customer would be charged a fee.

In its complaint, Southwest alleged, among other things, that BoardFirst’s conduct violated the CFAA, and Southwest moved for summary judgment on its claims. The court held that Southwest was not entitled to summary judgment on its CFAA claim. The court agreed with Southwest that, by logging on to southwest.com, BoardFirst had been “intentionally access[ing]” Southwest’s computer within the meaning of the CFAA. However, the court asked the parties to provide additional briefing on the issue of whether BoardFirst had acted “without authorization” or had “exceed[ed] authorized access,” as well as whether the court should apply the “rule of lenity” in interpreting the CFAA in the context of the case. The rule of lenity “counsels courts to construe ambiguities in a criminal statute, even when applied in a civil setting, in a narrow way.”

The court then addressed whether Southwest had satisfied the CFAA requirement that it show a “loss” of more than $5,000 in a one year period due to BoardFirst’s conduct. To support its “loss” claim, Southwest had submitted the declaration of its corporate representative on damages, which stated that “Southwest spent at least $6,500 within a single one year period in investigating and responding to BoardFirst’s unauthorized access to Southwest’s computer system.”

The court ruled that, although “investigative and responsive costs fit within the concept of ‘loss’ as used in the CFAA,” the corporate representative’s declaration was “fairly conclusory,” and thus inadequate to establish “loss,” because the declarant had

---

23 Id. at *13.
24 Id. at *15 (citation omitted).
25 Id. at *16.
failed "to identify the precise steps taken by Southwest in 'investi-
gating and responding to' BoardFirst's unauthorized access."\textsuperscript{26} This failure, according to the court, prevented it from being able to determine if Southwest's response costs were "reasonable," as required by the Act's definition of the term "loss." However, Southwest did succeed in shutting down BoardFirst's operations; on the basis of Southwest's breach of contract claim, the court permanently enjoined BoardFirst from continuing to use southwest.com to obtain boarding passes for its customers.\textsuperscript{27}

\textit{Southwest v. Harris.} In 2007, Southwest sued eight defendants, alleging that they had engaged in brokering of the airline's Rapid Rewards frequent flyer plan miles and awards. In its complaint, Southwest advanced a CFAA cause of action, its only federal cause of action, as well as numerous state statutory and common law causes of action.

The defendants moved to dismiss the complaint for lack of subject matter jurisdiction, alleging that they had not "accessed" Southwest's computer system within the meaning of the CFAA. Southwest focused its opposition solely on the "access" element of the CFAA because that is the only one that the defendants had disputed, but, in deciding the motion, the United States Magis-
trate Judge decided to analyze all the elements of the CFAA cause of action, including whether Southwest had sustained a "loss" within the meaning of Sections 1030(c)(4)(A)(i)(I) and (e)(11).\textsuperscript{28}

In his ruling, the Magistrate Judge noted that, under the Act, Southwest was required to show that it had sustained a "loss aggregating at least $5,000 in value over a one-year period." The Magistrate Judge also noted that, under Section 1030(e)(11), the Act defines the term "loss" as "any 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."\textsuperscript{29}

In its complaint, Southwest alleged that it had incurred a "loss" within the meaning of the Act because it had lost more than

\textsuperscript{26} Іd.
\textsuperscript{27} Іd. at *19.
\textsuperscript{28} Southwest Airlines Co. v. Harris, 2007 WL 3285616, at *3-4 (N.D. Tex. 2007).
\textsuperscript{29} Іd. at *3.
$5,000 in revenue in one year due to numerous passengers having traveled on its flights using awards that were void because defendants had brokered them in violation of the Rapid Rewards program’s terms. Taking a narrow view of the Act’s definition of “loss,” the Magistrate Judge ruled that the form of loss alleged by Southwest did not fall under the definition set forth in Section 1030(e)(11) because the revenue at issue had not been lost “because of interruption of service.” Accordingly, the Magistrate Judge recommended that the defendants’ motion to dismiss be granted, and the District Court accepted his recommendation.\textsuperscript{30}

The court in \textit{Harris} is not alone in its view that lost revenue must result from a service interruption in order to constitute a “loss” within the meaning of Section 1030(e)(11). In fact, this appears to be the majority view on this issue.\textsuperscript{31} However, some courts have ruled that lost revenue does constitute “loss” within the meaning of Section 1030(e)(11) even if it does not result from a service interruption.\textsuperscript{32} This issue was recently addressed in a case brought by Alaska Airlines.

\section{Alaska Airlines v. Carey}

Brad Carey is no stranger to lawsuits brought against him by airlines seeking injunctive relief against, and damages arising from, his frequent flyer mileage brokering. Northwest Airlines sued Carey for mileage brokering in 1991, and, the next year, the court granted the airline a permanent injunction\textsuperscript{33} and a stipulated judgment for $200,000.\textsuperscript{34} United Airlines sued Carey for

\begin{itemize}
\item \textsuperscript{30} \textit{Id.} at *5.
\item \textsuperscript{31} \textit{See} Costar Realty Info., Inc. v. Field, 2010 WL 3369349, at *15 (D. Md. 2010) ("[T]his Court is persuaded by the rationale of courts holding that a violation of the CFAA must cause an interruption of service in order for lost revenue to constitute as a qualifying ‘loss’ under the statute because, otherwise, the language of ‘because of interruption of service’ in the definition of ‘loss’ would be inoperative and violate a rule of statutory interpretation.").
\item \textsuperscript{32} \textit{See}, e.g., Frees, Inc. v. McMillian, 2007 WL 2264457 at *6 (W.D. La. 2007) ("[T]he CFAA does not limit the recovery of lost profits as an element of compensatory damages solely to instances where there was an interruption of service.").
\item \textsuperscript{33} Northwest Airlines, Inc. v. Carey, No. 91-cv-747 (W.D. Wash. July 7, 1992).
\item \textsuperscript{34} Northwest Airlines, Inc. v. Carey, No. 91-cv-747 (W.D. Wash. Oct. 29, 1992).
\end{itemize}

In 2007, Alaska Airlines filed a lawsuit in the United States District Court for the District of Washington against Carey, his wife, and Carey Travel, Inc. seeking damages and injunctive relief related to Carey’s brokering of Alaska Airlines frequent flyer miles and award tickets. Like other frequent flyer programs, the terms of Alaska Airlines’ program, which is known as the “Mileage Plan,” prohibit its members from selling, purchasing, or bartering miles or award tickets, and stipulate that miles and award tickets “are void if transferred for cash or other consideration.”

In its amended complaint, Alaska Airlines set forth eight causes of action, but its CFAA cause of action was the only federal statutory cause of action in its pleading and, thus, the sole basis for the court’s subject matter jurisdiction under 28 U.S.C. § 1331.

According to Alaska Airlines, Carey operated the following scheme in violation of the CFAA. Carey would solicit Mileage Plan members to sell their miles to him. He would pay the members a set number of cents per mile, and the members would provide him with their online Mileage Plan username and password. Carey would then be contacted by persons looking to buy an Alaska Airlines ticket, and he would agree to sell them a ticket. Carey would then log on to Alaska Airlines’ website using a Mileage Plan member’s username and password and purchase the requested ticket in the name of the buyer. Carey would then pass the electronic ticket information to the buyer, along with the instruction that, if asked, the buyer should explain that the award ticket was received “free, free, free” as a gift.

In the litigation before the District Court, Alaska Airlines claimed that Carey was violating the CFAA by, “with intent to defraud,” accessing its computer system “without authorization” by using others’ account information without the airline’s permission for the sole purpose of fraudulently causing the airline to

---

issue tickets and provide transportation based on void miles and award tickets.

The District Court agreed with Alaska Airlines that Carey had violated the CFAA, and it entered summary judgment in its favor and a permanent injunction against the defendants. The Ninth Circuit agreed as well, affirming the District Court’s rulings in all respects.\textsuperscript{38} However, neither the District Court’s order granting summary judgment, its amended order granting summary judgment, nor the Ninth Circuit’s memorandum opinion affirming the District Court’s decision contains an extensive discussion of the CFAA cause of action. Only the transcript of the District Court’s oral decision at the hearing on Alaska Airlines’ motion for summary judgment offers insight into either court’s thinking on the CFAA issues.

At the summary judgment hearing, the District Court ruled that Alaska Airlines had proven the elements of its CFAA cause of action. As to the unauthorized access element, the court held that using a frequent flyer program member’s online username and password, even with the member’s permission, to perpetrate a fraud against the airline constitutes “access[ing] a protected computer without authorization” in violation of the CFAA. In ruling in this manner, the court rejected Carey’s contention that his access was authorized because the selling Mileage Plan members had given him permission to use their website login information. The court pointed out that the victim of Carey’s fraud was Alaska Airlines and that the airline owned and operated its site, solely determined authorized access to it, and had not given Carey the authority to use its site to perpetrate a fraud against it.\textsuperscript{39}

In addition, the court ruled at the summary judgment hearing that Alaska Airlines had proven the “loss” element of its CFAA cause of action:

The statutory dollar value, the Court is satisfied, is met in aggregating the cost of policing the system in order for Alaska Airlines to maintain the contin-


\textsuperscript{39} In its summary judgment memorandum, Alaska Airlines cited \textit{United States v. Willis}, 476 F.3d 1121, 1123 (10th Cir. 2007), in support of its successful contention that using another person’s username and password to access a website to commit a fraud violates the CFAA.
ued integrity and viability of its frequent flyer system.

The fact of damage here is not a close question in my judgment. Not only do we have the in excess of $5,000 spent by Alaska Airlines to fulfill its business interest in maintaining the integrity of its mileage system, but as in the Texas case of Frequent Flyer Depot v. American Airlines, it is also clear to me that there has been a loss of goodwill. Any time a valid frequent flyer mile customer does not have a seat available on a plane because of someone who improperly aggregated miles and obtained a travel award in violation of the terms and conditions, that results in a loss of goodwill, a loss of respect and confidence in the system that Alaska Airlines and, I might add, most other carriers have promoted and spent a goodly amount of money in advertising and promoting for their economic advantage.40

The District Court was able to conclude that Alaska Airlines had incurred costs in excess of $5,000 in a one-year period responding to Carey’s offenses because the airline had submitted, in support of its summary judgment motion, the declaration of its Director, Customer Loyalty & Marketing Programs, in which he attested that the airline had expended over $5,000 in manpower in a one-year period while “tracking and attempting to curtail Defendants’ abuses of the system.” The court relied on this declaration in ruling that Alaska Airlines had satisfied the “loss” element of its CFAA cause of action.

IV. CFAA Pointers

The CFAA is a potentially powerful weapon against mileage brokers, “screen scrapers” and others who threaten an airline’s revenues through conduct that involves accessing the airline’s computers. But, in general, judges appear to be reluctant to award relief under the CFAA because the law is relatively new and it was originally enacted as a criminal statute designed to stop computer hackers, and a mileage broker is very different from a hacker. This means that, knowingly or unknowingly,

judges are likely to apply “the rule of lenity” in analyzing whether an airline has proven the elements of a CFAA claim. However, if an airline takes the following steps, it can substantially increase the odds of obtaining favorable and relatively quick relief under the CFAA:

• The frequent flyer program’s rules should contain a term that clearly states that a member is not authorized to allow a third party to use the member’s user identification or password in order to log in to the member’s account to perform any transaction that violates the program’s terms. This term would make it difficult for a mileage broker to successfully argue, using an agency theory, that he did not violate the CFAA because the member had given him “authorization” to “access” the airline’s computer by using the member’s login information.

• To combat automated “screen scraper” devices, the terms of use of an airline’s website should specifically prohibit such devices, and the terms of use should be accessible from all pages on the site. This term would help an airline satisfy the requirement that it show that the CFAA offender had accessed the airline’s computer “without authorization.”

• An airline should focus on proving its damages as soon as online fraud or abuse is detected. At the outset in most fraud cases, the plaintiff’s focus is primarily on proving liability, and the computation of damages is often left for discovery or for an expert witness to handle at a later time. However, to help prosecute a CFAA claim, an airline must prepare to prove its “loss” before the litigation and as soon as the offending conduct is identified. If the defendant moves to dismiss a CFAA cause of action on the grounds that the airline has failed to properly plead a “loss” (i.e., the defendant makes a “factual attack” on subject matter jurisdiction grounds), the airline will be required to oppose the motion with admissible evidence.\(^{41}\) Such evidence must be collected before the case is filed.

• To ensure that an airline has sufficient evidence of “loss,” as soon as online fraud or abuse is detected, the airline personnel (or outside contractors) investigating and responding to the offending conduct should keep daily logs describing the tasks

---

\(^{41}\) See, e.g., Chas. S. Winner, Inc. v. Polistina, 2007 WL 1652292, at *4 (D.N.J. 2007) (“Since Autoport has challenged the underlying factual assertions of plaintiff’s CFAA claim, which claim is the basis for this Court’s jurisdiction, the burden shifts to plaintiffs to prove this Court can exercise jurisdiction.”) (citation omitted).
they have performed and the time spent performing them. It is critically important that the logs (and the contractor invoices, if any) describe how the tasks performed were in direct response to the CFAA violations. Otherwise, there is a substantial risk that a court will hold that the airline has failed to prove that the employee time, or other response costs incurred, constitute "reasonable" costs within the meaning of Section 1030(e)(11).42

- In the court complaint, in addition to alleging revenue and goodwill loss due to the defendant's CFAA offenses, an airline should separately allege that, as "the cost of responding to" such offenses, it has incurred aggregated costs exceeding $5,000 in a one-year period. "The cost of responding to an offense" is considered "loss" under the CFAA. Courts have held that employee response time counts toward the $5,000 threshold.43 Once the airline has its "foot in the door" as to the CFAA by proving that its response costs exceeded $5,000 in a one-year period, then it can seek to recover revenue under common law fraud and other causes of action that was lost for reasons other than an "interruption of service."

- If damages are relatively unimportant, difficult to prove, or likely to be impossible to recover, and an airline's primary objective is to stop the defendant's online fraud or abuse, then the airline should consider dismissing its damages request at some point, particularly where a state statute could provide a cause of action for attorneys' fees and costs.44 Streamlining the case in this manner would increase the likelihood that an airline would be able to obtain a permanent injunction at the

42 See, e.g., Global Policy Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010) ("[P]laintiffs in this case 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 and resecure the e-mail system were reasonably necessary in the circumstances.") (citation omitted).

43 See U.S. v. Millot, 433 F.3d 1057, 1061 (8th Cir. 2006); U.S. v. Middleton, 231 F.3d 1207, 1213-14 (9th Cir. 2000) ("[D]amage under CFAA was properly computed "by multiplying the number of hours that each employee spent in fixing the computer problems by their respective hourly rates (calculated using their annual salaries).")

44 In Alaska Airlines v. Carey, the court awarded Alaska Airlines attorneys' fees of over $122,000 and litigation expenses of over $4,500 in connection with its successful claim that the defendants had violated the Washington Consumer Protection Act.
summary judgment stage and end the case without having to engage in potentially costly and time-consuming damages-related discovery.