

UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
ORLANDO DIVISION

03/17/03 PM 0:39  
RECEIVED  
MIDDLE DISTRICT OF FLORIDA  
ORLANDO, FLORIDA

DIRECTV, Inc., a California corporation,

Plaintiff,

v.

JEFF THACKER, BENNETT LEVE and  
HAROLD HOOVER,

Defendants.

Case No. 6:03-CV-239 ORL-28 DAB

**AMENDED COMPLAINT FOR  
COMPENSATORY, STATUTORY  
AND OTHER DAMAGES, AND  
FOR INJUNCTIVE RELIEF**

---

Plaintiff, DIRECTV, Inc., through its attorneys, alleges as follows:

**INTRODUCTION:**

**DIRECTV AND THE SATELLITE  
TELEVISION BROADCASTING BUSINESS**

1. Plaintiff, DIRECTV, a California company, operates the United States' premier digital satellite entertainment service, delivering over 225 channels of digital entertainment and informational programming to homes and businesses equipped with specialized digital satellite system equipment. DIRECTV has invested more than \$1.25 billion to develop its direct broadcast satellite system.

2. DIRECTV delivers television programming to millions of subscribers in the United States. In order to receive and view DIRECTV's satellite signal, each subscriber must be equipped with digital satellite system hardware, which consists of a satellite dish, an integrated receiver/decoder ("IRD") and an access card that is necessary

1  
2 to operate the IRD. Through this technology, DIRECTV offers programming including  
3 major cable networks, studio movies and special events offered on a pay-per-view basis,  
4 local network channels in select areas, and a variety of other sports and special interest  
5 programs and packages, some of which DIRECTV has the exclusive right to broadcast  
6 via satellite.

7         3. DIRECTV does not manufacture digital satellite system hardware.  
8 DIRECTV sells programming, most of which it purchases from program providers such  
9 as cable networks, motion picture distributors, sports leagues, event promoters, and other  
10 programming copyright holders. DIRECTV contracts and pays for the right to distribute  
11 the programming to its subscribers, and holds exclusive satellite distribution rights in  
12 certain of the programming. DIRECTV also creates its own original content  
13 programming, for which DIRECTV owns the copyright.

14         4. DIRECTV provides different levels of programming to its customers  
15 based on the particular subscription package that DIRECTV subscribers purchase.  
16 DIRECTV encrypts its satellite transmissions and employs conditional access technology  
17 to prevent unauthorized access to its television programming by non-subscribers. The  
18 conditional access technology relies in part on "access cards" that are provided to  
19 consumers as components of the digital satellite system equipment and which, upon  
20 activation by DIRECTV, decrypt DIRECTV's programming and permit the consumer to  
21 access and view it. The software code contained in the access cards protects DIRECTV's  
22 programming against unauthorized access.

23         5. Each DIRECTV customer is required to obtain a DIRECTV access card  
24 and other system hardware (including a small satellite dish) and create an account with  
25 DIRECTV. Upon activation of the access card by DIRECTV, the customer can receive  
26 and view in a decrypted format (*i.e.*, unscrambled) those channels to which the customer

1  
2 has subscribed or otherwise made arrangement to purchase from DIRECTV.

3 6. Consumers who have purchased digital satellite system equipment can  
4 subscribe to various packages of DIRECTV programming, for which the subscriber pays  
5 a periodic fee, usually monthly. Subscribers can also order pay-per-view events and  
6 movies either by using an on-screen menu and a hand-held remote control device, or by  
7 calling DIRECTV and ordering the program over the telephone.

### 8 **DIRECTV'S SECURITY SYSTEM**

9 7. All programming distributed by DIRECTV is delivered to one or both of  
10 DIRECTV's broadcast centers in Castle Rock, Colorado, and Los Angeles, California.  
11 At the broadcast centers, DIRECTV digitizes and compresses the programming, and  
12 encrypts the signal that is sent to its subscribers to prevent receipt of the programming  
13 without authorization. DIRECTV then transmits the encrypted signal to multiple  
14 satellites located in orbit approximately 22,300 miles above the earth.

15 8. The satellites relay the encrypted signal back to Earth, where it can be  
16 received by DIRECTV's subscribers equipped with digital satellite system dishes and  
17 IRDs. The satellite receiving dishes can be mounted on a rooftop, windowsill or deck  
18 railing at the subscriber's home or business. The signal is received by the dish and  
19 transmitted by wire to the IRD. The IRD (boxes that are approximately the size of a  
20 VCR player) acts like a computer which processes the incoming signal using the credit  
21 card sized access card.

22 9. After a customer installs the dish, IRD, and access card at his or her home  
23 or business, the access card blocks access to DIRECTV programming until the customer  
24 purchases one or more programming packages from DIRECTV. When the customer  
25 subscribes to a package, DIRECTV electronically activates the subscriber's access card  
26 in accordance with that subscription. The access card then acts as a reprogrammable

1  
2 microprocessor and uses "smart card" technology to (a) control which DIRECTV  
3 programming the subscriber is permitted to view, and (b) capture and transmit to  
4 DIRECTV the subscriber's impulse pay-per-view information.

5 10. Because DIRECTV generates its revenues through sales of subscription  
6 packages, it must be able to condition access to programming on the purchase of  
7 legitimate subscriptions. Accordingly, DIRECTV devotes substantial resources to the  
8 continued development and improvement of its conditional access system.

9 11. DIRECTV's need to develop increasingly sophisticated security measures  
10 is driven by the actions of satellite television "pirates." Satellite pirates endeavor to  
11 circumvent DIRECTV's security measures to gain unlimited access to all DIRECTV  
12 programming, including pay-per-view events, without paying a fee. Because the access  
13 cards are the primary security mechanism relied on by DIRECTV, the modification of  
14 access cards using various hardware and software devices designed to disable the access  
15 cards' security is the primary focus of satellite piracy.

16 12. As part of its ongoing effort to prevent piracy, DIRECTV periodically  
17 updates its access cards to improve both functionality and security controls. DIRECTV's  
18 most recent generation of access cards are commonly referred to as "P4" cards. Prior  
19 generations of access cards are commonly known as "H", "P2", "HU", or "P3" cards.

20 13. As part of its efforts to combat piracy, DIRECTV periodically develops  
21 and administers electronic countermeasures, which are commonly referred to in the  
22 satellite piracy community as "ECMs." ECMs involve sending a stream of data that  
23 targets access cards using known modified software code and disables those access cards.

24 14. In response to DIRECTV's ECMs, and in particular to a highly successful  
25 ECM known in the pirate community as "Black Sunday," satellite pirates have developed  
26 devices referred to as, among other things, bootloaders, dead processor boot boards,  
glitchers, HU loaders, emulators, and unloopers, that employ hardware and software in

1 combination to restore pirate access cards' ability to illegally circumvent DIRECTV's  
2 encryption protection and view DIRECTV programming.

3  
4 15. DIRECTV's ability to attract and retain subscriber revenues and goodwill,  
5 and distribution rights for copyrighted programming, is dependent upon maintaining and  
6 securing the integrity of its programming, technology and products, including the access  
7 cards and copyrighted programming, and in prohibiting unauthorized reception and use of  
8 its protected communications.

#### 9 PARTIES

10 16. On May 25, 2001, in the matter of DIRECTV v. Derek E. Trone, et al.,  
11 Case No. SA CV-01-370-DOC (Anx), filed in the United States District Court, Central  
12 District of California, DIRECTV executed Writs of Seizure, with the assistance of local  
13 law enforcement, at Fulfillment Plus, a mail shipping facility used by several major  
14 sources of pirate technologies including Vector Technologies, DSS-Stuff, DSSPro, DSS-  
15 Hangout, Whiteviper Technologies, Meadco, Intertek, Shutt Inc., and Canadian Security  
16 and Technology. During and subsequent to the raids, DIRECTV came into possession of  
17 a substantial body of sales records, shipping records, email communications, credit card  
18 receipts and other records. Those records evidence certain of the Defendants' purchases  
19 of illegal Pirate Access Devices. In reliance upon those records and other information,  
20 and upon information and belief, DIRECTV sets forth the allegations in this Complaint.

21  
22 17. Plaintiff, DIRECTV, Inc., is a corporation duly incorporated under the  
23 laws of the State of California with its principal place of business at 2230 East Imperial  
24 Highway, El Segundo, California. DIRECTV has significant interests in maintaining and  
25 securing the integrity of its satellite transmissions of television programming, and in  
26

1  
2 prohibiting the unauthorized reception and use of the same.

3 18. Each Defendant is currently a resident of this District and/or was a  
4 resident of this District when this cause of action arose. DIRECTV alleges that  
5 Defendants have purchased and used illegally modified DIRECTV Access Cards and  
6 other devices ("Pirate Access Devices") that are designed to permit viewing of  
7 DIRECTV's television programming without authorization by or payment to DIRECTV.  
8

9 19. Defendant, BENNETT LEVE ("LEVE"), is a resident of Orlando, Florida.  
10 Upon information and belief, beginning on or about October 8, 2000, LEVE purchased  
11 one or more Pirate Access Devices from Whiteviper Technologies. LEVE placed each  
12 order by using interstate or foreign wire facilities, and received his orders via the United  
13 States Postal Service or commercial mail carriers. Specifically, these illegal purchases  
14 included the following transactions:  
15

16 a. On or about October 8, 2000, LEVE purchased a Pirate Access Device  
17 from Whiteviper Technologies, consisting of a Viper Reader/Writer & Whiteviper  
18 Unlooper Combo. The device was shipped to LEVE's address in Orlando, Florida.

19 20. Defendant, HAROLD HOOVER ("HOOVER"), is a resident of  
20 Windermere, Florida. Upon information and belief, beginning on or about August 2,  
21 2000, HOOVER purchased one or more Pirate Access Devices from Whiteviper  
22 Technologies. HOOVER placed each order by using interstate or foreign wire facilities,  
23 and received his orders via the United States Postal Service or commercial mail carriers.  
24 Specifically, these illegal purchases included the following transactions:  
25

26 a. On or about August 2, 2000, HOOVER purchased a Pirate Access Device

1  
2 from Whiteviper Technologies, consisting of a Viper Reader/Writer & Whiteviper  
3 Unlooper Combo. The device was shipped to HOOVER's address in Windermere,  
4 Florida.

5         21. Viper Reader/Writer & Whiteviper Unlooper Combos, like the one  
6 purchased by Defendants, are devices that read data from, and write data to, ISO7816  
7 smartcards, like those utilized in the DIRECTV system. The Reader/Writer and  
8 Unlooper components of the "Combo" unit purchased by the Defendants each have  
9 separate functionalities.  
10

11         22. Satellite pirates use smartcard Readers/Writers to predominately hack the  
12 second generation of DIRECTV's access cards, also known as "P2" or "H" cards.  
13 Typically, pirates modify software stored in the electronically Erasable Programmable  
14 Read-Only Memory ("EEPROM") of a DIRECTV access card. EEPROM memory  
15 stores information that will change during the life of the smartcard but that survives even  
16 if power is removed from the card.  
17

18         23. Because of software vulnerabilities in DIRECTV's P2 card, satellite  
19 pirates are able to modify the P2 internal software without manipulating the smartcard's  
20 voltage or clock. DIRECTV has eliminated many of these software vulnerabilities  
21 through over-the-air software updates sent by DIRECTV's engineering team. Once a P2  
22 card has received a software update that fixes its EEPROM memory, satellite pirates  
23 resort to "unlooper" devices and smartcard readers to hack the access card. The  
24 "Unlooper" component of the device purchased by the Defendants serves that purpose.  
25

26         24. An "unlooper," the device purchased by LEVE on October 8, 2000,