UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

SOUTHERN DIVISION

HONORABLE DAVID O. CARTER, JUDGE PRESIDING

- - - - - - -

ECHOSTAR SATELLITE CORP., et al., Plaintiffs,	)	
vs.	)	No. SACV-03-950-DOC Vol. IV
NDS GROUP PLC, et al., Defendants.	)	

REPORTER'S TRANSCRIPT OF PROCEEDINGS

Santa Ana, California

April 9, 2008

SHARON A. SEFFENS
Federal Official Court Reporter
United States District Court
411 West 4th Street, Room 1-053
Santa Ana, California 92701
(714) 543-0870

SHARON SEFFENS, U.S. COURT REPORTER

♀

I-N-D-E-X

SHARON SEFFENS, U.S. COURT REPORTER

SANTA ANA, CALIFORNIA; WEDNESDAY, APRIL 9, 2008; 2:30 P.M.

(Jury present.)

THE COURT: The jury is present. Counsel are present, and the parties are present.

This is the opening statement by Mr. Stone on behalf of NDS.

MR. STONE: Thank you, Your Honor.

Good afternoon. My name again is Richard Stone. I have the privilege and honor of representing NDS in this case. We, too, have a team concept. Here with me is Dov Rubin, the General Manager of NDS Americas; David Eberhart; Darin Snyder; and Ken Klein who will be helping me present the evidence in this long trial.

We just heard an amazing string of accusations. It kind of sounded like a novel. The one thing it has in common with a novel is it's complete fiction. Counsel invited me to set the record straight, and I am going to do that. That is going to take a little while, and I am going to go through a lot of evidence, not argument, but I am going to tell you about the evidence in this, and I am going to set the record straight.

The truth is the evidence will show that NDS did

not engage in any conspiracy post any code or instructions on the Internet to hack EchoStar. NDS has done nothing to create piracy of EchoStar. NDS has done nothing to

illegally harm or damage EchoStar. All NDS has done is compete hard but fair in the marketplace.

You are going to learn that contrary to the facts as presented by plaintiffs NDS is the leader in fighting satellite piracy. NDS has assisted law enforcement agencies such as the FBI, U.S. Customs, and the Department of Justice in identifying, capturing, and prosecuting numerous satellite pirates. NDS has helped law enforcement fight EchoStar piracy as well.

You don't have to take my word for it because you are going to hear from a former federal prosecutor, Anthony Peluso, who will come here and testify about NDS's willingness to drop everything and help the United States government prosecute satellite pirates and, specifically, John Norris and his team's willingness to drop everything and pitch in and help whenever the federal government needed it.

You are going to hear Mr. Peluso explain that these pirates just don't do DirecTV. The majority of them if they are hacking DirecTV they are hacking EchoStar, so when satellite pirates are prosecuted, it benefits EchoStar as well. You will hear that this federal prosecutor had evidence of EchoStar piracy. He was willing to prosecute EchoStar piracy, but plaintiffs told him we don't have a significant piracy problem. On the other hand, NDS has

worked hand in hand with law enforcement to disrupt pirate

organizations, to have them prosecuted, have assets seized, and to send pirates to prison. Plaintiffs have benefited from NDS's aggressive approach against piracy. Yet they come in here and tell you we are the bad guy in this drama.

There is going to be a lot of evidence that NDS had nothing to do with the Internet postings that you briefly heard about in plaintiffs' opening, did not engage in any piracy of the EchoStar system, and I am only going to have time to go through some of it. I will just give you sort of an overview and hit the key points, but I am warning you there is going to be lot of it.

Then I am even going to go forward and tell you the evidence of why we are really here. Why are we here? It's not because NDS did anything wrong or illegal, and it's certainly not because plaintiff suffered any damages from some December 2000 Internet postings. I am going to give you a number that the plaintiffs don't want you to remember, $1.2 billion in revenues.

The year after these postings that supposed destroyed their system their revenues went up $1.2 billion. That number right there tells you something else is going on in this lawsuit. There is an ulterior motive at work here that has nothing to do with these postings that they claim. I am going to cover that a little bit later.

♀

14:38:37 I am going to give you just a little preview that the story you are going to hear and the evidence that you are going to see is a lot different than what you have been told. First, we are going to take up reverse engineering. You are going to hear a lot of evidence that reverse engineering is an entirely legitimate common practice in many industries, including the high-tech industries. It amounts to taking product, breaking it apart, looking at it to see what makes it work, see how it operates, find out the state of technology.

You will hear about it from NDS's engineering expert, and you are going to hear about it from plaintiffs' expert who has a company that specializes in reverse engineering. In fact, they reversed engineered the Apple iPhone three weeks after it was released to find out what weaknesses it had and what security problems it had. They didn't do that because Apple asked them to. In fact, Apple asked them not to, but they did it anyway, and they published of the weakness in the Apple iPhone.

What is interesting about that is that their own expert speaks at these conferences called the black hat security conferences, so when plaintiffs make a big deal out of black hat, their own expert will tell you that it's a well-known and well-used term in computer security. Those of you involved in the computer industry probably heard it

♀

14:39:58 before. Black hat refers to computer security teams that provide protection. You have to think like a hacker to prevent against it, and they have conferences where these folks come and speak about computer security. They are called black hat conferences. So it's a completely legitimate term, and it's disingenuous to claim otherwise.

You are going to hear from NDS's expert about a conference of engineers where they took apart a Toyota Priuss on stage and then published the results. So reverse engineering is nothing mystical. There is nothing wrong with it. In fact, it keeps the marketplace honest when you think about it. If your competitor is saying our product does X, Y, and Z, and the customer thinks, well, it does X, Y, and Z, but if you opened up the product and looked at it and said, no, it does X and Y but it doesn't do Z, now you keep your competitor honest. So it creates honesty in the marketplace to know what products are actually capable of as opposed to what the proponent of the product might be

telling folks.

Now, reverse engineering serves another purpose in this industry. There is rampant piracy. That is true. If somebody else is going to be pirated, you know that the money, skills, and knowledge from that piracy is going to come back at you, so you need to monitor piracy and figure out where is it going to come from? Who is it going to hit

14:41:27 next, and is it going to boomerang?

The evidence is going to show the plaintffs know better than to spin this as something sinister or wrong by NDS because plaintiffs' reverse engineered the NDS DirecTV system. They have done the exactly same thing that NDS has done. Plaintiffs extracted and analyzed the ROM code from NDS access cards, ROM coded essentially the guts of the card, the main part of the code. That's what Mr. Mordinson analyzed. They have analyzed the same thing. You will an e-mail, Exhibit 816. It's right in there.

They admit they subscribed to DirecTV. Now, why does EchoStar subscribe to DirecTV? They are not trying to send DirecTV money. The reason they did it is they analyzed the system. They logged the data stream. They reverse engineered NDS's electronic countermeasures used for the DirecTV system. They set out to find out as much as they could about the NDS DirecTV system, and it's not like they called up NDS and DirecTV and asked for permission. They just did it and kept it quiet.

NDS is not here complaining about that. Okay. So far, that's fair competition. Fine. But what they forgot to tell you is that the real unfair competition in this case is the plaintiffs went out and had one of their pirate informants provide them stolen NDS internal documents. I don't mean one, and I don't mean two. I mean 26,000 pages

10

14:43:10 on CDs. Plaintiffs executives, Mr. Guggenheim and Mr. Gee (phonetic) flew to Canada for the handoff of these CDs in the Vancouver airport.

Where did the CDs come from? A gentleman named Ron Ereiser, and you are going to be hearing a lot about Ron Ereiser in this case. Mr. Ereiser had been sued and indicted by NDS in the United States. He is a notorious satellite pirate. He is now on their payroll for $12,000 a month if I recall correctly. So they knew these documents were stolen. A satellite pirate that NDS had sued and had prosecuted shows up with 26,000 pages of NDS documents, including the highly sensitive technical documents, and they didn't ask a single question. Ron, where did you get the documents? Didn't NDS just have you indicted? You have got their documents. Not a single question. So when we deposed Mr. Ereiser, he refused to answer where he got NDS's stolen documents.

So this is just a little preview that the evidence is going to tell you a little bit different story than you have heard so far.

Now let me give you another point that sort of gives you a little preview of maybe things are a little bit different than you have been told. You heard about the supposed damages that the plaintiffs are going to be claiming in this month long trial. Well, they forgot to

♀

11

14:45:05 tell you that two months after the postings on the Internet, which I am going to get to in a minute in detail, they launched two things: a killer electronic countermeasure that killed all the pirate cards that used whatever was posted on the Internet.

There is a guy in Switzerland that -- a little bit

of an oversimplification but not much -- presses a button, zap, down the satellite signal, kills any card that uses these instructions, but they did more. They can also send a software patch through the satellite signal. So they send a code through the signal, and it goes to the card, and it completely prevented the type of attack posted on the Internet through an electronic software patch.

So think about that for a moment. These Internet postings that they claim cost them $100 million in damages were completely neutralized within 60 days of the Internet postings through the satellite signal, and, again, you don't have to take my word on it. You are going to hear from the CEO of the plaintiff EchoStar at the time, Alan Guggenheim. His job responsibility was security of the system. He has testified under oath that the patch was completely effective and blocked and prevented any of the attacks of the kind shown in the Internet postings.

Guess what? Plaintiffs' software expert agrees. And guess what? Our expert looked at the actual patch code.

♀

He finally had an opportunity to do so, and he has confirmed that it completely prevents any buffer overflow attack, including the one posted on the Internet.

Mr. Jones is going to tell you about some more evidence, that well before these Internet postings plaintiffs knew their cards had this vulnerability. They knew the pirates were using this vulnerability. They knew they could patch it and prevent it, and they chose to do nothing until December of 2000 when the Internet postings hit. If they had simply electronicly patched their cards when they first knew about it, we all would not be here.

So this is just a little preview of the evidence that is going to be a bit different, and as we hear it over the next four to five weeks, it's going to show you that

contrary to what you have been told NDS did not do anything wrong or illegal, and plaintiffs have no real damages here.

Now, bear in mind, they go first, so it might be awhile before you hear all of that evidence, so I am going to go through it with you here in some detail.

First, let me explain briefly the satellite security industry. You have heard a little about it. Companies like NDS provide the technology that scrambles the signal that comes down to the home. They also provide the smart card. You need the Smart Card for when the scrambled signal comes in. The Smart Card processes it and

descrambles it so that the customer can watch what they are authorized to watch. The card keeps track of what you are allowed to watch.

Some satellite security companies like NDS also investigate piracy on behalf of their customers, and they collect evidence to sue pirates or to help law enforcement go after pirates to stop piracy. Everyone agrees this is a highly competitive industry where you have to stay on top of the technology. You have to stay on top of what competitors are doing and capable of doing and learning all you can about the competition.

You have to stay on top of piracy, both piracy of your system as well as the other guy's system, because piracy is a tough, ugly, complicated thing to stop. It's not easy. Satellite television has been attacked from all directions. You have hackers who are smart, sometimes brilliant, techs who want to just hack anything that's on a computer. You have got hobbists who are people who are somewhat tech savvy, and they just want to get free TV for themselves, and then you have got pirates who are well-organized, well-funded criminal organizations, and they make pirated cards and pirated devices to try to make as much money as they can from piracy.

24 And now you have got the Internet, so these folks
25 can work together and share information. And you will find

14:49:35 1 that the pirates also use the Internet to fight with each
2 other. They put false information on the Internet, and they
3 hack each other's pirate stuff and put it on the Internet.
4 So there is this constant game of payback and revenge that
5 the pirates play out on the Internet itself.
6 Now, because of the piracy problem, you are going
7 to hear some evidence that's a little unusual. Not many
8 industries have the kind of evidence you are going to hear
9 here because of the piracy problem. You are going to hear
10 about informants, sting operations, uncover operations,
11 converting hackers or pirates to become part of any piracy
12 teams. You are going to be hear about monitoring the
13 Internet on a global basis to track down piracy and stop it.
14 Now, not all satellite security companies are
15 alike. Some are more proactive in fighting piracy. NDS has
16 been one of the more proactive ones. It has used the
17 intelligence it has gathered in it's uncover operations and
18 from it's sting operations to help law enforcement pursue
19 many pirates.
20 You will also hear from former law enforcement
21 like Mr. Peluso who is going to testify about NDS's role in
22 helping law enforcement identify and prosecute pirates. One
23 thing you didn't hear so far is many of the witnesses for
24 plaintiffs are some of the same pirates that NDS has
25 aggressively and successfully pursued. Guys like Ron

14:51:02 1 Ereiser plaintiffs now employ and who was indicted with the
2 help of NDS and sued successfully for $14 million or Jan

Saggiori, another pirate who was sued by NDS successfully.

Let me tell you just a little bit about NDS. Then I will get right to the heart of the plaintiffs' case. NDS's conditional access system is used in 72 million set-top-boxes for satellite broadcasters around the world. NDS employs 3,400 people across the globe and 200 in its U.S. headquarters right here on 3500 Highland Avenue in Costa Mesa.

NDS prides itself on being a global technology leader in its industry, and it dedicates substantial resources every year to researching and developing new products and new technology to improve its Smart Cards, but because NDS recognizes this is a very competitive industry, it also analyzes competitors and what the competition is doing and what the state of the art is. Again, it's the same thing plaintiffs do.

NDS isn't going to come before you and say they have never been hacked. Everyone in this industry is hacked sooner or later. NDS has understood that its system is going to be under attack from well-financed pirates as well as engineers and whiz kids. It's a constant game of cat and mouse. You have to have newer technology to prevent the hacking. You have got to have better electronic

♀

14:52:31 countermeasures, which are specialized computer viruses that go seek and destroy pirate cards, and you have to have lawsuits and criminal prosecutions to deter pirates and shut them down.

So in addition to fighting piracy at a technological level, NDS has been very proactive in instigating investigations, lawsuits, and cooperating with law enforcement to stop piracy, and the team that does it is called Operational Security. The head of Operational Security in North America is John Norris, and you are going

to hear from him. He is going to describe for you his efforts working hand in hand with law enforcement to prosecute the worst pirates.

You are also going to hear that both plaintiffs and NDS use pirates or former pirates to gain valuable intelligence to find out what the pirates are up to so that they can use that intelligence to stop then or design countermeasures.

And you are going to hear about Chris Tarnovsky. Mr. Tarnovsky was a very bright tech savvy individual. He is at the center of their accusations as you know. He has contributed to shutting down many powerful satellite pirates. NDS and its undercover agents like Chris Tarnovsky have made many enemies in the pirate community. NDS has cost the pirates millions of dollars, shut down hundreds of

14:53:52 websites, and has helped send many of them to prison.

Now, there is one last piece of evidence about NDS that you didn't hear about, and I think you should keep it in mind when you evaluate the accusations in this case. You heard testimony about the 1994 or '95 or '96 time frame that NDS had problems with hacking and piracy, and it did, but it didn't sit there and blame somebody else. It didn't wallow in misery. It made a better product. It got more aggressive against the pirates, and it improved itself, and it didn't need to hack plaintiffs in the year 2000 to compete.

How do I know that? Because after this lawsuit was filed, EchoStar approached NDS to hire NDS to be its security supplier. You didn't hear about that did you, but you are going to hear about it from the president of EchoStar Technologies Corporation at the time, Mark Jackson. You are going to hear about it from Mr. Rubin, the General Manager of NDS Americas, who was invited to these meetings and attended them.

So when you hear these allegations about NDS was desperate and needed to do something desperate, I want you to remember that even up to 2007 plaintiff EchoStar was haggling over price with NDS to use NDS as its security company because its current security provider, Nagra, was well behind the times in the technology war against pirates.

14:55:33 Now let's talk about the plaintiffs' case. The evidence is going to show it's nothing more than one big deception. They make some facts without outright false allegations. They take evidence of NDS's anti-piracy efforts and they twist that truth into false evidence of piracy. They take NDS's legitimate competition and competitive intelligence-gathering and they spin it as something sinister. I am going to through each of these deceptions and tell you what the evidence actually proves. There are seven major deceptions in this case.

The first deception, that Chris Tarnovsky caused all the damages to the plaintiffs by posting on the Internet the receipe to hack EchoStar cards in December 2000. That's the claim. There are two Internet postings in December 2000 that they claim caused all their damages.

Now, there are two important names you need to remember: Alan Guggenheim and JJ Gee, Alan Guggenheim and JJ Gee. These are the two gentlemen who were the lead investigators into the source of these Internet postings. You heard about an expert, Dr. Rubin, who comes in years later and says it kind of looks the same. They had two investigators whose job it was to investigate these postings.

You are going to see Exhibit 511-A, which is the actual posting. It's posted by xbr2121 on the dr7 website.

19

14:57:14 Now, during a lawsuit, we are able to send questions to the other side. They are called interrogatories. It's extremely important. They have to answer them truthfully under oath under penalty of perjury. The reason that is done is it makes it difficult for people to try to change their story if it turns out there is no real evidence to support their accusations.

For four years of this lawsuit, the plaintiffs accused Mr. Tarnovsky of being xbr21, the person who posted information on one way to hack the EchoStar security system on the dr7 website. They even stated under oath that all of their damages were caused by this December 23, 2000, posting by Chris Tarnovsky using the alias xbr21. So under oath, Mr. Tarnovsky's xbr21 was the person who posted this.

But we knew Mr. Tarnovsky was not xbr21, so we took plaintiffs' information and we conducted our own investigation. Guess what? We found the real xbr21. His name is Marco Pizzo. He lives in St. Louis, Missouri. You are going to hear him testify in this case. He is going to explain how the information on the EchoStar hack ended up on the dr7 website. He put it there himself. He took the NipperClause file that was posted from a European pirate website called interestingdevices.com, and he was the first one to put it on the dr7 website the plaintiffs base their claim on. He actually posted it twice because the first

♀

20

14:58:51 time he posted it there was a problem, and then he reposted it. Mr. Pizzo has never been employed by NDS, has no dealings with NDS, and doesn't know Chris Tarnovsky. No one told Mr. Pizzo to make this posting. He did it all on his own so that he could discuss this with other hackers.

Now, you have heard this statement that they are

going to claim some other posting on December 21. Apparently, it was there so momentarily nobody has ever seen it because there is no evidence of any posting on December 21. Mr. Pizzo will tell you that he was the first person to post this on the dr7 website. He didn't see any other postings or chatter referencing any prior posting. Mr. Pizzo is also going to testify that he knew there were pirates all over attacking the Nagra system, which he believed was a weak system that EchoStar used. So this evidence was a huge problem for the conspiracy story.

Plaintiffs' lead investigator on the Internet postings, Mr. Gee, testified that if it turned out that Chris Tarnovsky was not xbr21 then it would be true that NDS was not responsible for plaintiffs' piracy problems after the December 2000 postings. You are going to see that evidence. You are going to see that Mr. Tarnovsky is not xbr21. NDS is not responsible for plaintiffs' piracy problems, and NDS did not cause any damage to the EchoStar security system.

♀

15:00:18 The evidence will show you that their own investigator, Mr. Gee, testified under oath that if Chris Tarnovsky was not xbr21 then NDS would not be the cause of damage to the EchoStar system. So when you hear the new story about something on December 21, remember for over four years they consistently and falsely accused Mr. Tarnovsky of being xbr21 and being responsible for the posting that they claim under oath caused all of their damages. The evidence is undeniable that Marco Pizzo as xbr21 is the only guy to post the so-called recipe on the dr7 website that they complain about.

Now, there is one more amazing fact about this. At the time of the December postings, the owner/operator of the dr7 website, Mr. Menard, whose name you heard was recovering from major hip surgery, so because of that, he

had other people running his website. In fact, during December 2000, one of the administrators of the dr7 website was Charles Perlman, who we now know was a pirate informant paid by EchoStar. The evidence is going to show that the very time these postings were made on the dr7 website they had an informant running the website named Charles Perlman.

You are going to hear testimony that an administrator of a website or a web master can monitor who is posting, can block post, control the servors, you know, basically run the website. So if somebody else other than

15:02:11 xbr21 posted something, then Mr. Perlman should have been able to provide a screen shot, an electronic file, a report, something that proved that. And if the posting on dr7 was supposed so dangerous and unstoppable, why didn't the plaintiffs ask they inside guy to block it or delete it?

There is going to be more evidence that Mr. Tarnovsky did not put the NipperClause posting as we call it in this case -- you will see the file has a name NipperClause in it -- on the dr7 website either on or before December 23.

Now, they claim that this reverse engineering Headend Report is the source of the posting. That's not true, not true, but even taking their claim at face value, Mr. Mordinson has testified he didn't even show the Headend Report to Mr. Tarnovsky until mid 2001 well after the posting. Mr. Tarnovsky has also testified he did not see the Headend Report until 2001 after the posting, and Mr. Tarnovsky is going to tell you why he knows it was 2001.

Now, we had an expert, Isle Jones (phonetic), compare the posting to the Headend Report, so you have the Headend Report from 1998 and the posting in 2000. Mr. Jones is an expert in embedded systems. Embedded systems are basically Smart Cards or microwaves or cell phones, anything

that has a chip or a little computer embedded in it. He has written hundreds of programs for such systems, and he has

15:03:48 actually written code for the very processor that's in the EchoStar cards, so he has lots of experience with this code.

He will tell you that the hypothetical attack that Mr. Mordinson sketched out when he did his reverse engineering report is dramatically different than the xbr21 code in ten major areas. Another fact that is critically important -- and you are going to hear this evidence -- the code that was posted by xbr21 on the dr7 website has software code instructions and hardware addresses that are not in the Headend Report and NDS didn't know about. Mr. Jones is going to show you all the reasons why he can confidently conclude that the posting on the Internet did not come from the Headend Report.

Now, plaintiffs' expert obviously disagrees with that, but Mr. Rubin is not a Smart Card or an embedded systems expert. He doesn't design products or write code for products. He never worked with a code that EchoStar uses in its cards unlike Mr. Jones.

Now, he is a smart computer professor, but his speciality is network security, but it's interesting because he agrees with Mr. Jones that the programs are dramatically different. In his report, Dr. Rubin has said -- and I want to get this right -- the programming methodologies and styles are different. The programs are of different lengths. The hexadecimal byte sequences are different.

15:05:18 Different addressing methodologies are used, and many other specific aspects of the two programs are different.

Now, because he is a hired expert in this case, Dr. Rubin tries to downplay all those differences he was forced to concede exist, but our expert will point out why those are all very significant differences in addition to the fact that there is information in a posting that the Headend Report didn't disclose and NDS didn't know.

Now, let me talk about the next deception, that only NDS could be the source of EchoStar piracy. The evidence is going to show that there were many skilled pirates and hackers who had access to the EchoStar ROM code before the December 2000 postings. Their own expert agrees that a reasonably skilled pirate who had access to the ROM code could have done this attack.

In fact, we are going to bring before you one of the best hackers of the EchoStar system, a gentleman who went by the name of "Stuntguy." He is going to come in here and testify that pirates have been hacking EchoStar well before the December 23 posting.

They threw out two other names, Nipper and NipperClause. We know Tarnovsky is not xbr21, so who is this Nipper and NipperClause? Can we solve that mystery? You heard them accuse us of being that person. Mr. Tarnovsky supposedly was xbr21. That's been disproven.

♀

15:06:46 Now he is NipperClause. Well, we can solve that mystery. The reason we can solve it is plaintiffs have already solved it before they filed the lawsuit. So let me tell you about that.

Before the postings -- before the December 2000 postings, plaintiffs acquired a pirate device called the black box. It was used to illegally reprogram EchoStar Smart Cards. Now, using evidence traced from the black box, the plaintiffs had very strong leads about who was behind the Internet postings and the information Xbr21 found and posted. The plaintiffs just stopped investigating.

The hard evidence is going to show that they stopped investigating because it wasn't NDS. It wasn't Tarnovsky. It wasn't anyone associated with NDS. Now as a result of this lawsuit, we now know that plaintiffs know who Nipper and NipperClause is.

Let me explain. The evidence is going to show that about a year before the posting, in early 2000, there was a type of hack to the EchoStar access cards called the E3M hack floating around Canada. The plaintiffs suspected that this so-called E3M hack used a buffer overflow type of attack. That's the same type of attack in the Internet posting, so they paid their pirate informant, Mr. Ereiser, $65,000 to get one of these black box devices to confirm that.

♀

15:08:15 Ereiser acquired the black box pirate device. He gave it to plaintiffs who studied it in October 2000, months before the posting. What did they find? Well, they compared the code when the posting came out with the black box and found that it did the exact same thing, used the exact same methodology, and was connected to the postings. Remember, the black box comes from a pirate in Canada.

Now, there is going to be a lot of evidence about the black box pirate device, but there are just a couple of other important points I want to make about it. The evidence is going to show the plaintiffs acquired a pirate device, the black box, once before the postings. It breaks the EchoStar system by attacking it in the exact same vulnerability that was shown on the Internet and shown in the xbr21 posting, so now the question becomes where did Mr. Ereiser get the black box?

Well, the evidence is going to show plaintiffs know that Mr. Ereiser got the black box from a piracy group in Barrie, Ontario, Canada, a known hotbed of pirate

activity. You are going to hear NagraStar's own security man, JJ Gee, is going to testify that Mr. Ereiser got the black box from Jim Waters in Barrie, Ontario. Jim Waters is a known pirate.

Again, you are going to see Exhibit 375, which is Mr. Gee's notes that corroborates this testimony. In those

notes, it shows that Jim Waters of the Barrie Group provided the black box to Mr. Ereiser, and it also shows that Mr. Waters sold another black box or a looper, which is another name for it, to someone named Anthony Muldanado.

Now, I have mentioned four names. You have got JJ Gee, whose is their security man and the lead investigator. You have got Ronald Ereiser, their pirate informant. You have got Jim Waters, a pirate in Ontario, Canada, and Anthony Muldanado, also a known pirate, and Mr. Muldanado purchased a black box device from Mr. Waters that is connected to the postings.

So how did Mr. Gee known that Mr. Muldanado got a black box device from Jim Waters in Barrie, Ontario, that is connected to the postings? This is one of the most significant exhibits in the case. It's Exhibit 374. It's entitled "Report of an Investigation with Reference to Anthony J. Muldanado and Paul Thomas St. James for Mr. Alan Guggenheim, CEO, NagraStar, EchoStar March 23, 2001." It's a 120-page comprehensive report that describes when Mr. Gee accompanied the FBI on a raid of Mr. Muldanado's house on March 23, 2001, within three months of the postings.

So what did they find on this raid with the FBI? Well, you will see from this report and you will hear Mr. Gee's testimony that Mr. Muldanado worked for Motorola as an engineer in Arizona, but he had a double life as a

major EchoStar piracy distributor. When they went to his house, they seized 60 receivers, modified cards, all sorts of evidence of piracy.

So what did they learn from Mr. Muldanado? Well, during the FBI raid, there was an interview of Mr. Muldanado by the FBI and Mr. Gee. They asked -- remember, this is three months after the postings. It's a logical question. Do you know who Nipper is? Without prompting, Mr. Muldanado said yes, and Nipper also went by the name NipperClause.

So Mr. Muldanado went on to tell the FBI and Mr. Gee that Nipper was his piracy supplier, Jim, in Barrie, Ontario, who Mr. Gee determined was Jim Waters. So Jim Waters, the guy who sold the black box to plaintiffs' informant was Nipper according to Mr. Muldanado, a piracy distributor who was raided in March 2001.

Now, the evidence is going to show another amazing fact about Mr. Muldanado. He made his connection with his supplier Jim from Barrie, Ontario, on a pirate Internet form that plaintiffs now admit was hosted by their own informant, Mr. Ereiser. I am not making this up. So the evidence is going to show that even though EchoStar and NagraStar knew the source of their piracy problems Mr. Gee and his security team did not pursue any of these leads to the source of a black box in the postings. They did nothing to pursue Jim Waters in Barrie, Ontario. They had just been

given hot information from a pirate who told the FBI this, and they did nothing, nothing in 2001, 2002, 2003, ever.

You are also going to hear evidence that the source of the code in the black box may have come from a company that was doing the software development for plaintiffs. You are also going to hear evidence about inside leaks of source code from plaintiffs' companies that

were helping pirates.

So what the black box evidence shows is that plaintiffs had solid evidence within a couple months of the December 2000 postings of a black box pirate device connected to the postings that used a buffer overflow attack that came from Jim Waters in Barrie, Ontario, and that his distributor told the FBI and JJ Gee that he was Nipper.

Plaintiffs had every reason to investigate that thoroughly. Yet they didn't investigate any of it, and they can't give any reason why they did not. The reason is that they knew the investigation would show it was not NDS or Chris Tarnovsky, so they didn't want to investigate. The evidence is also going to show they didn't care because they fixed their problem with a software patch and an electronic countermeasure in February 2001. Those are the reasons they failed to even follow up on this.

Now, just when you thought it couldn't get any more suspicious, there is one more fact about the black box.

♀

15:14:37 After they paid $65,000 for the black box device, they had it, they studied it, what did they do it? The plaintiffs' explanation is they got rid of it. They gave it back to the pirates.

So if NDS or its experts wanted to analyze the black box pirate device and provide more evidence that NDS is not responsible for this, we can't do it. There are only two plausible explanations for why plaintiffs would get rid of critical evidence that they paid $65,000 for. They knew that if we had it it would conclusively prove that the black box that EchoStar had and the postings do not have any connection to NDS and that if anyone was helping the pirates it was a leak from the inside.

Now, there is a second posting you heard, the so-called Nipper 2000 posting on December 24. Everyone

agrees that this is a dump of a pirated card. In other words, it was a card that was modified and somebody dumped its contents on the Internet. The evidence is going to show that the posting itself is meaningless, and it has no connection to NDS or Tarnovsky.

You are going to hear from NDS's expert, Nigel Jones, who has examined it. He is going to tell you that it's completely inconsistent with the information in the Headend Report. The information didn't come from any card that NDS studied, and that if anyone used this posting it

would simply crash their card. Again, plaintiffs' expert agrees that if anyone were to use this posting it would simply crash your card.

Now, some further investigation. The Internet service provider for the posting from December 24 traces to Sudbarrie, Ontario, which is near Barrie, Ontario, where we know Jim Waters aka Nipper is located. So the computer used to post the code on December 24 comes from Ontario, Canada. More evidence that that posting has nothing to do with NDS.

Finally, the evidence is going to show that the plaintiffs were able to determine whose card was used to make that posting, and they have covered it up. Again, Mr. Guggenheim, the former CEO of NagraEchoStar, has testified that Nagra Vision in Switzerland was able to analyze this code that was posted on the Internet and find unique identifying information. He testified that process was done. When he was asked what were the results, whose card was it, I don't recall. Now, don't you think if it was NDS or Chris Tarnovsky Mr. Guggenheim would have recalled?

Well, guess what? We finally realized that buried in that code is a unique password that the plaintiffs' engineers used. It's the one piece of information that wasn't changed and redacted by whoever posted it, so we told the plaintiffs take this password and run it through your

database and tell us whose card this is.

Well, now we know, Exhibit 1510. It's the printout of the results. There is an interesting address on there. It says the card is owned by Margaret Kupes (phonetic), 600 Main Street, Tanawanda, New York. So we did some investigation. That's not a residence. It's a commercial address. It's a freight-forwarding company called M&M in Tanawanda, New York, that is within about 100 miles of the Canadian border.

What we also found out is this freight-forwarding company allowed its address to be used in the United States so that Canadian pirates could get U.S. subscriptions to EchoStar because EchoStar cannot be received in Canada, so now we have got the card that's tied to the posting is tied to a freight-forwarding company that allows its address to be used by Canadian pirates for illicit activities. Again, it has nothing to do with NDS, and they knew it.

So every time they try to investigate these postings we get away from NDS or Tarnovsky, so they weren't interested in that, so you are not going to see any reports of investigations into these postings with one exception. There is one report. It's the 120-page report that identifies Jim Waters as Nipper. That's the only investigative report on these postings.

Now I am going to talk about the ICG/TDI story. Because their own investigation proved that these postings

were not related to NDS, plaintiffs try to claim that TDI and ICG conducted some investigation that linked Mr. Tarnovsky to the Nipper alias. Well, because of the

false allegations against NDS, DirecTV did conduct an investigation, but we know Mr. Lebson of TDI who headed up the investigation has testified that when they say link they grabbed anything they could off the Internet, anonymous postings, rumors, so it's basically unsubstantiated Internet gossip and hearsay. In fact, that's exactly what the reports are.

Mr. Lebson testified he sent an e-mail to ICG and said do you have any evidence proving that Chris Tarnovsky is Nipper? He said no. We have got hearsay. We don't really have any evidence, and Mr. Lebson testified that never changed. Now, that's not surprising because we now know who Nipper is, but TDI hired nine separate subcontractors to investigate it. They never came up with any evidence that Mr. Tarnovsky was Nipper. They are not going to. It's Jim Waters. We know that from their own records.

Now, the hearsay that ICG found two years after the postings -- this report was done in 2002 -- two years later where does the hearsay come from? Charles Perlman, Dean Love, and Reggie Scullion. What they all have in common is they are EchoStar's paid pirate informants, so

♀

15:20:54 that's the source of the hearsay in the 2002 report.

You are going to hear from Mr. Betsa (phonetic), the president of ICG. Remember there is TDI, Mr. Lebson. There is ICG, which is owned by Mr. Betsa. He is going to testify and confirm that they never had any evidence, never had any confirmation, linking any particular person to any particular alias. He is also going to testify that ICG made no connection between Mr. Tarnovsky and EchoStar piracy. Again, it's not a surprise in light of what we now know.

One last point on ICG, if you look at Exhibit 360 in this case, it will be somewhat amusing. The same ICG

that supposedly made this link -- well, they also said that NagraStar's CEO, Alan Guggenheim, provided an EchoStar hack to dr7, and they recommended that his potential involvement in the pirate community should be further investigated. ICG said their own CEO ought to be further investigated for involvement in piracy. So under their theory of proof then, Mr. Guggenheim ought to be the defendant in this case, not NDS.

The testimony that it took a sophisticated lab to do this, that is going to be disapproved by a mountain of evidence. The system was weak. The Pizzo example is just one example of one hack of the system. It's an attack that is one of the oldest in the history of computing. Every pirate knows about buffer overflow attacks. It's one of the

15:22:31 first things you learning in a standard software security class according to their own expert, and their own expert even referred to it as a very bad security mistake.

Mr. Rubin admitted that any pirate who basically had access to the ROM code could have figured this out, and we are going to show you there are lots of pirates who had access to the ROM code. You are going to hear from our expert, Nigel Jones, that the cards were full of security holes. In fact, he found so many obvious deliberate mistakes in the failure to prevent this attack that Mr. Jones thinks it's more likely than not that this began as an inside job.

He found when he was finally able to look at the source code for the ROM 3 card, which is the subject of the posting, that the software programmer deliberately failed to check for the ability to overflow the communications buffer, deliberately didn't do it, the basic step. It would have take two lines of code to do that.

Plaintiffs' expert, Dr. Rubin, raised even more suspicions about this. When he looked at the code, he said,

hey, there are two other buffers that the programmer specifically checked to make sure they couldn't be overflowing, but those can't be used for any piracy attack. So get this. The same programmer put in two lines of code for the two buffers that can't be used for a pirate attack

15:24:00 and deliberately could not check for buffer overflow on the one buffer that can be used for a piracy attack.

Plaintiffs' expert admitted there are many other major security flaws in this system. For example, there is something called the box keys. The security system depends heavily on those remaining a secret. It turns out that you can use your remote control on your couch at home and punch up the secret box keys on this system, and once you have the box keys, those can be used for hacking. So your remote control on your TV at home can get secret codes. Their own expert had to call that a really bad security design. You are going to hear lots of evidence of weaknesses in their product that made they inherently vulnerable to known methods of attack.

Now, there were numerous groups of pirates attacking EchoStar as well, including skilled engineers. You are going to hear from "Stuntguy." We went out and we found "Stuntguy." The reason we found "Stuntguy" is "Stuntguy" published on the Internet a bible of hacking EchoStar, a detailed manual on how to hack EchoStar, and he published this a year before the postings. His name is Chris Dahla. Ironically, he lives within about 20 miles of the EchoStar headquarters in Denver, Colorado.

He began publishing this hacking bible in the early fall of '99 and updated it all the way through the

15:25:33 year 2000. He has absolutely no connection to NDS, no connection to Chris Tarnovsky. He even performed complete studies of the ROM 3 code and the prior version, the ROM 2 code, before these postings. Mr. Dahla even received source code to the EchoStar system that was posted by EchoStar employees on a corporate FTP site that pirates were able to access. He also figured out a backdoor password that was an easy way to dump the card before these Internet postings. So it does the same thing as the postings, but it's even easier.

You heard about the DISH Plex Group. Something counsel didn't tell you is it's not exactly a retailer. DISH Plex was a piracy group in Ontario, Canada. One of their informants was part of that group, Larry Pilon, whose testimony you will see.

The DISH Plex piracy group had a sophisticated piracy lab in Thunder Bay, Ontario. They had a scanning electron microscope that was used to extract code. Plaintiffs' own database entries, Exhibit 515, shows that the Thunder Bay scanning electron microscope owned by the DISH Plex Group was used to provide "Stuntguy" with his information to create this bible of hacking.

The other thing they forgot to tell you is that the posting was like one way to hack just the ROM 3 card, but every other version of their card has been hacked, and

15:27:09 they admit that it has been done by actual pirates, so ROM 2, 10, 11, 101, they admit were done by actual pirates. The card that they provided for the swap, that was done in 2005. It was hacked before the swap was completed. They are facing what is called free-to-air piracy. That's where people buy off-the-shelf receivers. You don't even need a Smart Card, and you can steal their signal right out of the

air. That's their biggest piracy problem. It's by actual pirates. So they want you to believe that only NDS could do this one hack of this one card in this one time frame, but they admit pirates did everything else.

You are also going to hear evidence about plaintiffs' own internal security leaks that contributed to their piracy problem. So while they are here accusing NDS, there is going to be evidence that a lot of this was from the inside.

Now, the next major deception is that John Norris is somehow involved in a scheme to commit piracy. The evidence is going to show that this is one of the most vile aspects of their scheme to falsely blame NDS or to accuse John Norris. John Norris has dedicated his career to fighting piracy. He has worked hand in hand with law enforcement for over a decade. He has spent his whole career fighting piracy.

You are going to hear from Mr. Norris. After he

served in Vietnam and achieved the rank of captain, he was honorably discharged in 1973. He began providing security work for companies like General Instruments thereafter, and for the last 12 years, he has headed up NDS's security operation for both North and South America. He has provided instruction to law enforcement on numerous occasions, including on topics like how to successfully prosecute satellite piracy crimes, how to catch satellite hackers, how satellite criminal organizations are organized. Through his efforts, NDS has sued and prosecuted numerous pirates.

You are going to hear from Mr. Peluso who I have discussed, a former federal prosecutor who worked with John Norris on many prosecutions. Mr. Peluso also served in Vietnam and after Vietnam became an Army prosecutor for 16 years for the judge -- advocate general support. He resigned in the early '90s and became an Assistant United

States Attorney for the Middle District of Florida.

He is going to tell you three important things: John Norris and his team always provided valuable assistance in his fight against piracy and in helping the U.S. Government and that invariably the piracy that they fought was both DirecTV and EchoStar.

Now, he is also going to tell you that during the same time period they claim their system was destroyed and they suffered hundreds of millions of dollars of damages

15:30:03 they told Mr. Peluso, a federal prosecutor, they had no significant piracy problem. Even when Mr. Peluso brought out major pirates who had successfully hacked them and who he had convicted, EchoStar denied to Mr. Peluso that they had a piracy problem. You are going to hear that this attitude frustrated Mr. Peluso.

You are also going to hear that Mr. Peluso did hear from EchoStar that they blamed NDS and Tarnovsky for piracy while denying that actual pirates he had convicted had hacked their system. But Mr. Peluso will tell you he was willing to investigate any source of piracy. If it was NDS or Tarnovsky, he would have investigated it, but he never got any evidence from EchoStar or any other source that NDS or Tarnovsky was engaged in any piracy.

Now, the evidence is going to show that John Norris did recommend that NDS hire Chris Tarnovsky. He was well aware that Chris had engaged in some questionable satellite piracy activities after Mr. Tarnovsky returned from serving in the Army in Europe, but he thought he could be turned around and serve as a available intelligence asset, which is exactly what happened.

Chris not only obtained important information to help NDS prosecute pirates, but he worked very hard to help them secure their products and improve their technology.

25 The people that are coming in here and telling you that John

15:31:30 1 Norris has engaged in piracy who are trying to ruin his
2 reputation, these are the same pirates that John Norris went
3 after. They are paid pirates who are out for revenge.
4 A perfect example is Graham James who you may or
5 may not hear about. Mr. James admitted he lied under oath
6 in his previous trial. The result, he was convicted of
7 armed robbery. They want you to accept the word of people
8 like that that John Norris is somehow engaged in piracy.
9 The next deception, Mr. Tarnovsky was in fact
10 terminated by NDS. That is true. But what plaintiffs
11 haven't told you is that the $40,000 in cash they talked
12 about has absolutely nothing to do with these postings. In
13 early 2001, NDS learned that these packages had come. The
14 money had been intercepted, and Mr. Tarnovsky had not
15 claimed the money. He understood that drug-sniffing dogs
16 had hit on the packages, so they had Mr. Tarnovsky take a
17 drug test. He passed. They interviewed Mr. Tarnovsky. He
18 said he didn't know where the money came from. He believed
19 he had been set up.
20 Now, there is a certainly plausible explanation
21 because Mr. Tarnovsky was working uncover. He had made a
22 lot of enemies in the pirate community. NDS had pursued a
23 lot of pirates successfully, and the U.S. Government had
24 just revealed that a sting operation called
25 operationsmartcard.net was actually a government sting

15:33:10 1 operation and not a pirate website as people thought.
2 Mr. Tarnovsky was working uncover in that
3 operation with government agents, and that had recently been

disclosed when these packages came in, so his story certainly seemed plausible. So he wasn't terminated at that point in time, and that's where it is at. He continued to be an exemplary employee and continued to work hard.

But then during this lawsuit for the first time, NDS obtained records that showed that a fingerprint traced to Al Menard from his associate Merve Main, so it was Merve Main's fingerprint apparently connected to Al Menard, and Mr. Tarnovsky was terminated. He was terminated not for engaging in piracy. He was terminated for not being completely candid because this fingerprint seemed to show some connection, and he said he had knew of no connection, so that was the reason he was terminated.

One thing you should know about Mr. Tarnovsky when he was in the Army in Europe is when he began his efforts to understand satellite conditional access systems. He was a driver for his colonel. The Army trained him in telecommunications. His colonel offered to sell him a satellite system that came with two cards that were broken, so-called pit cards, so Mr. Tarnovsky fixed these pit cards so that he could get English TV in Germany where he was stationed. This was very common amongst American soldiers

15:34:46 stationed in Germany at that point in time. If fact, Mr. Tarnovsky will tell you that if you wanted to look for the latest information on how to fix these cards, you would just go to the "Stars and Stripes" magazine or newspaper to find it.

So then he came back to the U.S. He was honorably discharged after serving in the Army for seven years. In 1996, he was approached by Ron Ereiser. Ron Ereiser asked him if he would engage in piracy of the DirecTV system. Chris was still interested in that kind of stuff, and, honestly, he took a wrong turn in life, and he agreed. From September 1996 to June 1997, he worked with Ron Ereiser

in piracy of the DirecTV system, and Mr. Tarnovsky will admit that. He will candidly tell you that he did that.

In 1997, NDS recruited him to serve on the Anti-Piracy Team to use his skills and aptitude to fight piracy. Chris Tarnovsky agreed. It was a way for him to continue to do what he loved but to have a legitimate job and fight piracy. So when they portray Mr. Tarnovsky as this evil figure, let me give you the timeline. He worked for Ronald Ereiser for ten months engaged in piracy in 1997. He then worked for ten years fighting piracy for NDS.

After he was employed by NDS, he did not hack the DirecTV system. The incident counsel referred to you will hear about. You will hear about Operation Johnny Walker.

♀

15:36:30 These are uncover operations. Guess who was the target of that 1998 operation that involved the money to the mailbox that counsel told you about? Guess who was the target? Ron Ereiser. Chris Tarnovsky and John Norris will tell you about that operation and how successful it was.

They also will try to spin this Al Menard relationship as something nefarious, but keep in mind Chris's job was to get close to people like Al Menard who ran a website, to gain intelligence, to find out what pirates were up to. It's true that Mr. Tarnovsky developed sort of an e-mail pen pal friendship with Mr. Menard, but I don't think the plaintiffs can exactly criticize that because, as you know, they did exactly the same thing. Their informant, consultant Charles Perlman, was so friendly with Mr. Menard he was in control of the website in December 2000 when these postings were made.

Now, two last things. The notion that this $40,000 in cash has anything to do with this case is just not true. In fact, the allegation that it somehow proves NDS is engaged in piracy, that was investigated by the

United States government. NDS cooperated with that investigation. Plaintiffs could provide whatever evidence they wanted. You are going to see when it was all said and done the United States Attorney for the Central District of California sent NDS a formal letter confirming they were

15:38:15 closing the books on that investigation. It's Exhibit 1268. It's a letter from Assistant United States Attorney James Spertus.

So now they talk about the termination. Chris Tarnovsky and Al Menard were fired. Well, you have to understand how Al Menard was hired. In about 2003, Mr. Menard was able to figure out and trace how somebody had stolen sensitive documents from DirecTV relating to the latest generation of their Smart Card. The way he was able to track down the person behind this who was ultimately prosecuted was ingenuous, so NDS hired him as a consultant, and he went around educating law enforcement on how to stop Internet piracy, Internet crimes, and he also served as an intelligence resource monitoring pirate websites.

Now, the notion that, well, gosh, they fired him right before their depositions so that's something nefarious, it's the exact opposite. Think about it. Mr. Menard was fired. He had no motive to lie for NDS. Chris Tarnovsky had no motive to lie for NDS. Mr. Menard had no love lost for NDS. In fact, at the time of his deposition, he had an agreement with EchoStar that there would be no adverse consequences to his testimony. He had been fired by NDS, no love lost for them, and he had essentially immunity from EchoStar, and he confirmed under oath that NDS has no involvement, no role, no conspiracy in

any EchoStar piracy.

The same thing for Chris Tarnovsky. If NDS had put up Chris Tarnovsky to some conspiracy to hack EchoStar, don't you think after he was fired he would spill the beans? Instead, he confirmed under oath these allegations are false.

The fifth deception is this notion that because NDS was keeping tabs on the competition that's somehow proof that they did something wrong. The evidence is going to show that the plaintiffs gathered intelligence on the NDS DirecTV system in the exact same way. What NDS did was perfectly legitimate, fair competition. We reversed engineered their product. They reversed engineered our product. If it stopped there, nobody has a beef.

For NDS, it did stop there. This harping on you couldn't improve your product, well, who knew until you opened this card that there really wasn't much there. It was pretty vulnerable. It wasn't very well made. So how are you going to improve when it had the most basic common mistake in computing a buffer overflow vulnerability?

But it was plaintiffs who crossed the line, not NDS. They flew to Canada to get stolen documents from Ron Ereiser, and these are highly confidential documents. In fact, you are going to see one of these documents, Exhibit 391. It shows ways to attack the NDS P3 card. It shows the

♀

weaknesses in the card. It shows NDS and DirecTV's internal analysis of the weaknesses and ways to hack their own card. Now, there are many more documents like that they obtained.

What they didn't tell you is that Mr. Ereiser has a reverse engineering lab up in Canada, but when Mr. Gee and Mr. Guggenheim were deposed in 2007, he still hadn't gotten around to visit him. So they have got a guy up in Canada a thousand miles away, so when they complain about monitoring,

you are going to hear the testimony that John Norris visited Chris Tarnovsky frequently. They have got their consultant with a lab up in Canada nobody has ever visited.

Now, they try to make a big deal out of the fact that NDS's engineers traveled to Israel to -- from Israel to North America to test their theory about the vulnerability. That's because the EchoStar broadcast stream cannot be received outside of North America. Now, their engineers didn't have to travel because they had the DirecTV receivers in their lab in Colorado where you can get the DirecTV stream.

However, the evidence is going to show that plaintiffs also went to Canada to start their process of analyzing the NDS DirecTV cards. The evidence is also going to show that NDS DirecTV ROM code, countermeasures, and DirecTV piracy devices were all sent to Switzerland to be analyzed. So, again, when they come in here and complain,

15:43:06 you are going to see lots of evidence that they had done exactly the same thing.

Finally, there is an issue about motive, NDS had a motive. The evidence is going to show it doesn't help NDS to have another system hacked. If another system is hacked, then the DirecTV NDS subscribers may go get the free TV that can be hacked. The other problem with that is if the other system is hacked the pirates build up knowledge, money. Guess where that comes back to haunt? It comes back on you. That's why whenever John Norris can -- and he is in a position to do so -- he has fought EchoStar piracy, including their free-to-air piracy, which is the biggest problem. Because it's such a big problem, he is concerned that that money that's made from there is then going to be turned on the DirecTV system.

The notion that they had some motive to hack to

keep DirecTV, that's completely false. You will hear from Ray Kahn, who was the Senior Director of Engineering of DirecTV at the time. He is going to testify that DirecTV was not considering using the existing Nagra system. He said that the fact that there was any compromise of the EchoStar system played no role in their decision not to use Nagra.

At the end of the trial, we will present you a timeline of events that is going to show that the

15:44:34 accusations of bad motive are completely wrong and don't make any sense.

The final deception, No. 7, the idea that these December 2000 postings destroyed their conditional access system and resulted in a card swap, the first witness you are going to hear from is their CEO, Charles Ergan. He owns 50 percent of the shares of EchoStar and is the person who authorized the filing of the complaint.

You are going to learn that even though he authorized the filing of the complaint he knew almost nothing about the factual allegations in the complaint. As of last week, he still hadn't gotten around to reading the lawsuit, but he does have information about two subject matters.

One deals with the motive to authorize the filing of this lawsuit. His testimony on cross-examination is going to make it clear that his real motive is that he was upset with News Corp. for its role in a transaction that is unrelated to this litigation, which ultimately cost EchoStar $600 million. It also forced EchoStar to face a stronger competitor. So this lawsuit against NDS, which is a News Corp. company, was an opportunity for EchoStar to even the score and get NDS to pay for their card swap.

The second subject about which Mr. Ergen possesses some information is government filings called 10-Ks, which

♀

15:45:54 are annual reports that must be filed by law with the Securities & Exchange Commission. They are required to be truthful and accurate because the investing public relies upon these documents to make judgments about the financial health of companies.

You are going to learn that the information in the 10-Ks is not consistent with the positions they are taking in this lawsuit. While they allege here their system was destroyed and completely compromised due to two Internet postings in December 2000, there is no reference to that in any of the 10-Ks. In fact, they don't state it. They don't reference it. The 10-Ks don't indicate that anything out of the ordinary occurred in the year 2000.

In fact, what they show is is that one year after these postings that are at the heart of this lawsuit, supposedly destroyed their whole security system, their revenues went up $1.2 billion. So the question is how could that be? If the system was destroyed, how could your revenues go up $1.2 billion in the year following that destruction?

Well, you know the answer. It comes from Mr. Guggenheim. It comes from our expert. It comes from their documents. They were able to issue an electronic countermeasure in a patch that blocked and prevented and completely neutralized these postings, and you are going to

♀

15:47:16 see it in their own documents.

The evidence is also going to show they knew about these vulnerability before these postings. Remember I told you the evidence about the E3M cards and the black box and

all that stuff. That's all before the postings. So when you know about it, why not issue that patch and that electronic countermeasure then? If they had, we wouldn't be here. So to the extent they claim any damages, it's a completely self-inflicted wound, and they have no explanation, no excuse, no reason, for why you wouldn't do that as soon as you know about the problem.

The evidence is going to show that this card swap occurred many years after these postings. They changed all the card versions they had out there, and it was not because of these Internet postings. You have heard the evidence that during the same time they say their system was completely destroyed they were telling law enforcement officials they had no significant problem.

Okay, so why are we here? The evidence is going to show that there is a conspiracy, but it's not the one plaintiffs claim. It's a conspiracy amongst plaintiff EchoStar, plaintiff NagraStar, and Kudelski to falsely blame a competitor to try to stick us the costs of a routine upgrade of technology that occurred many years after the postings they complain about. The reason is NagraStar was

♀

15:48:43 embarrassed by its defective technology and the fact that it could not compete with NDS.

Mr. Guggenheim was the CEO of NagraStar. His job was to get new business in North America, new customers, so he tried to persuade NDS's customers to switch. He went to DirecTV and was told no. He wasn't to Galaxy Latin America who was using NDS, and they said, no, we would like to stay with NDS. He went to DirecTV Latin America, and they said no. We are happy with NDS. In fact, in his testimony, Mr. Guggenheim couldn't identify a single new customer he was able to secure for Nagra in North America.

It gets worse because not only could he not

persuade people to drop NDS and switch to them, then EchoStar's largest customer, El Express View in Canada, said you should go talk to NDS. You should try to use them. They have a very good track record, and EchoStar did. Now Mr. Guggenheim is threatened with the fact that he couldn't get any new business, and now the one client they do have in the United States is talking to NDS.

Plaintiff NagraStar and its 50-percent owner, Kudelski in Switzerland, were trying to hide the fact that they sold defective technology to EchoStar. The defect we have talked about, the vulnerability to buffer overflow. It's one of the oldest most common attacks on computers.

The posting that they try to blame on us, it

15:50:11 relates to the raw version card, but every other version they had was pirated and hacked, and they don't blame that on NDS. As soon as they swapped the cards, the new cards were hacked. Frankly, they had an inferior system, and they could not compete with NDS in the marketplace, so they are trying to accomplish in this lawsuit what they could not in the marketplace.

While this was going on, NDS worked with DirecTV to have the secure P4 card. NDS took an aggressive approach to stopping piracy, and the DirecTV system became secured. NagraStar, on the other hand, refused to get involved. They refused to prosecute pirates. They refused to upgrade their technology. They were not ready for the onslot of piracy when DirecTV became secured.

EchoStar has a financial motive obviously. These ROM 3 cards and these cards they replaced, they were out in the field for five, six, seven, eight years. The testimony will show that in this industry that's too long of a time to have a card out there when it's constantly under attack. So these were basically old cards. They needed to be changed, so they are trying to get us to pay for them.

Finally, there is the oldest motive known to man, revenge. EchoStar tried to buy DirecTV once upon a time, and then NDS's parent corporation, News Corp., stepped in and was able to buy DirecTV, but Mr. Ergen had agreed that

15:51:42 if the deal fell apart between EchoStar and DirecTV they would have to May a $600 million failed deal fee. Now, since he and his family own 50 percent of the shares, this is a very personal $300 million hit.

So what did they do? Well, News Corp. bought DirecTV. Mr. Ergen and EchoStar had to watch the $600 million go away, and then within a week of filing this lawsuit, EchoStar filed a petition with the Federal Communications Commission to stop News Corp. from buying DirecTV. One of the reasons they gave was the lawsuit that they filed a week before. Is it starting to make sense? So the evidence is going to show that EchoStar has about 600 million reasons to falsely blame NDS in this case.

When you have heard all the evidence, we believe you are going to see that the true conspiracy in this case is the conspiracy to cover up the fact that the plaintiffs knew their system was vulnerable to one of the oldest hacks known to computing because it was defective. They knew Chris Tarnovsky was not xbr21. They knew that neither NDS or Tarnovsky were behind these postings. They knew who Nipper was. They knew the December 2000 postings did not amount to a significant security breach, let alone the destruction of their system because it was completely neutralized. They have known that actual pirates around the world -- it's the same ones that attack DirecTV -- are

15:53:08 responsible for their problems, not NDS. Finally, they knew that their paid pirate consultant, Mr. Ereiser, had wrongly obtained highly confidential stolen documents.

I know we have covered a lot of material. I want to tell you that in these openings statements counsel have made a promise to you. We have both made a promise to you. What is the evidence going to show? At the end of the case, we are going to come back and see who kept their promise here.

I want to thank you for your attention here today, and I want to thank you for your willingness to listen to all the evidence before you make your decision, not the accusations but the evidence. NDS has waited a long time to present all of this evidence. When we are done, we are going to ask you for a verdict first in favor of NDS on the plaintiffs' claims, and equally importantly, I am going to ask you for a verdict in favor of NDS on our counterclaim for the misuse of its stolen documents.

Thank you very much.

THE COURT: Counsel, why don't you take a recess and come back at ten after 4:00. We will take some testimony. Mr. Ergen is waiting in the hallway.

Don't discuss this matter amongst yourselves or form or express an opinion.

-oOo-

-oOo-

CERTIFICATE

I hereby certify that pursuant to Section 753, Title 28, United States Code, the foregoing is a true and correct transcript of the stenographically reported proceedings held in the above-entitled matter and that the transcript page format is in conformance with the regulations of the Judicial Conference of the United States.

Date: April 9, 2008

Sharon A. Seffens 4/9/08

SHARON A. SEFFENS, U.S. COURT REPORTER

SHARON SEFFENS, U.S. COURT REPORTER

♀