

CC TO JUDGE KN

Chief Judge Coughenour

*[Handwritten signature]*  
FILED \_\_\_\_\_ ENTERED \_\_\_\_\_  
LODGED \_\_\_\_\_ RECEIVED \_\_\_\_\_  
SEP 30 2002 KN  
CLERK U.S. DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
DEPUTY

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff,

v.

VASILIIY GORSHKOV,  
a/k/a Vassili Gorchkov,  
a/k/a "kvakin,"

Defendant.

NO. CR00-550C

GOVERNMENT'S SENTENCING  
MEMORANDUM

The United States of America, by and through John McKay, United States Attorney for the Western District of Washington, and Floyd G. Short, Assistant United States Attorney for the District, respectfully submits the following sentencing memorandum. Sentencing is scheduled for October 4, 2002.

**I. INTRODUCTION**

Defendant Vasiliy Gorshkov is before the Court for sentencing following his conviction at trial on one count of conspiracy and 19 counts of substantive crimes involving computer intrusions, computer extortions, and wire fraud. Trial began on September 19, 2001, and concluded on October 9, 2001, when the jury convicted defendant on all counts.

In essence, defendant participated in a scheme with Alexey Ivanov and others in which the conspirators hacked into computers in the United States and elsewhere, stole credit card information and other sensitive information from those computers, extorted victims by

*163*

1 demanding payments on threat of publishing the stolen data to embarrass the victims or  
2 destroying the victims' computers and data, and employed the stolen credit card data in a fraud  
3 scheme involving eBay and PayPal to generate fraudulent financial transactions and obtain  
4 computer goods and other parts that they purchased with stolen credit cards and had shipped to  
5 Kazakstan. The conspirators also used victims' computers to store hacking tools, to launch  
6 attacks on other victims, and to serve as proxies in the eBay/PayPal fraud scheme to disguise the  
7 true location of their operations in Russia. Defendant worked with Alexey Ivanov and others to  
8 perpetrate these crimes through an enterprise that came to be known as tech.net.ru.

9 The charged counts reflected this broad conspiracy, as well as particular substantive  
10 crimes committed against Speakeasy Network, an Internet Service Provider (ISP) located in  
11 Seattle; Nara Bank, a bank located in Los Angeles, California; CNB-Waco, a bank located in  
12 Waco, Texas; eBay, an internet auction company located in California; and PayPal, an online  
13 payment company also located in California.

## 14 II. FACTS

15 The evidence at trial proved that defendant and his enterprise, which began as a "hacker's  
16 club" and evolved into tech.net.ru, were responsible for a series of computer intrusions and wire  
17 frauds beginning in the fall of 2000 and continuing until or beyond the arrest of defendant and  
18 co-defendant Alexey Ivanov on November 10, 2000. The evidence consisted of the testimony of  
19 a relatively small number of the victims affected by defendant and his coconspirators, and the  
20 victims' records; video and audio recordings of the Invita FBI undercover meeting on  
21 November 10, 2000, that took place immediately before defendant's arrest; data from  
22 defendant's two Russian computers, named tech.net.ru and freebsd.tech.net.ru, that the FBI was  
23 able to copy data remotely during the days following the arrest; expert testimony regarding that  
24 data and other aspects of the case; and testimony of law enforcement agents. In addition,  
25 defendant testified that he had no knowledge of or involvement in the crimes.

26 The victims' accounts of the crimes were presented by:

- 27 1. Employees of Speakeasy Network (which suffered an unauthorized intrusion, an  
28 extortion, and harm to its systems at the hands of Ivanov in late 1999);

- 1 2. An employee of BP Radio (a customer of Speakeasy that had its credit card data  
2 stolen from Speakeasy's network);
- 3 3. The network administrator for the St. Clair County Intermediate School District  
4 (a public school district in Michigan whose network was compromised, used to  
5 host tech.net.ru's domain name server, and exploited as a proxy to commit further  
6 hacks and fraud);
- 7 4. An employee of Nara Bank (the online banking server of which was compromised  
8 with the loss of confidential customer information, which then received an  
9 extortionate email, and which suffered the creation of bogus accounts in an effort  
10 by defendant to transfer funds via PayPal, all in 2000);
- 11 5. An employee of CNB-Waco (a bank whose online banking server was  
12 compromised and whose confidential customer information was stolen in 2000);
- 13 6. Tad Brooker, a computer parts seller (who shipped parts to Kazakstan and was  
14 paid with stolen credit cards via PayPal in 2000);
- 15 7. Employees of Verio and WebCom (ISPs who defendant compromised in the fall of  
16 1999 and from whom he obtained confidential information); and
- 17 8. Employees of eBay and PayPal (who were the victims of an automated wire fraud  
18 involving scripts and programs created by defendant and his coconspirators to  
19 generate bogus online auctions and use stolen credit cards to obtain money and  
20 property).

21 Defendant's involvement in these activities was proven through his own statements at the  
22 Invita undercover meeting, as corroborated by the victims' testimony and by the data and  
23 programs on the Russian computers. At the undercover meeting, defendant spoke extensively  
24 about hacking computers and contacting victims in usually unsuccessful efforts to get them to  
25 pay money. He took personal responsibility for the hack of WebCom. He acknowledged that  
26 they had obtained a computer account at an ISP named CTS, an account obtained for hacking  
27 purposes. Defendant stated that his company, tech.net.ru, had about four hackers to create  
28 hacking tools, as well as other employees. He talked about scanning and hacking banks, as well.  
He became coy only when discussing the topic of credit cards, stating that such topics were  
"better discussed in Russia," where the FBI could not get to him. See PSR ¶¶31-36; Exh. E  
(Government's Exhibit 1C, admitted at trial, pages 113-168).

The data from the two Russian computers, together with the testimony of the victims,  
confirmed that defendant's enterprise had committed these crimes. The Russian computers held  
huge databases of stolen credit cards and confidential financial information. Defendant's own

1 account on each of the computers – the accounts named “kvakin” – contained the hacking tools  
2 and customized scripts needed for the computer intrusions and eBay/PayPal frauds. The expert  
3 witness for the United States, Philip Attfield, testified at length about these programs and scripts,  
4 the significance of their location in defendant’s “personal workspace” on those computers, and  
5 the various links between the computer data and the victims’ experience.

6 In his own testimony, defendant falsely portrayed his enterprise as a solely legitimate web  
7 design and computer security business. He acknowledged managing the business, which had  
8 about six employees by the summer of 2000, but he falsely testified that he knew nothing about  
9 the hacking, extortion, or fraud that was perpetrated using his own computers. He denied  
10 knowledge of the hacking tools and scripts that were in his accounts on the two computers.  
11 Defendant testified, incredibly, that during the Invita undercover meeting he was merely posing  
12 as a hacker, playing the part at the request of Ivanov. Defendant testified that it was only during  
13 the trip from Russia to Seattle that he learned from Ivanov that he had to pretend to be a hacker  
14 in the meeting with Invita. Exh. C. (Transcript of Defendant’s Testimony, selected pages).  
15 Needless to say, the jury rejected this testimony and convicted defendant of his participation in  
16 the conspiracy and his responsibility for all of the charged substantive crimes as well.

17 The evidence of defendant’s guilt was substantial, and it has been further corroborated by  
18 the recent guilty plea of Alexey Ivanov. On August 2, 2000, in the District of Connecticut,  
19 pursuant to Rule 20 of the Federal Rules of Criminal Procedure, co-defendant Alexey Ivanov  
20 pled guilty to the same conspiracy of which defendant was convicted at trial as well as one of the  
21 substantive counts relating to the attack on Speakeasy Network (Count Four) See Exhs. A (Plea  
22 Agreement and Stipulation of Offense Conduct) and B (Transcript of Plea Colloquy, selected  
23 pages, as redacted by the court). In the Stipulation of Offense Conduct that Ivanov signed, he  
24 corroborated the involvement of defendant in a broad scheme to hack into the computers of  
25 commercial businesses and financial institutions in the United States, steal from those computers  
26 credit card information and other confidential financial data, extort payments from the victims,  
27 and commit fraud using the stolen credit cards. The scheme began in the fall of 1999, and the  
28 entity that became known as tech.net.ru was the base for these operations. Tech.net.ru

1 computers were used both to perpetrate the crimes with various hacking tools and scripts and to  
2 store the stolen credit cards and financial information. Exh. A.

3 In addition to the Speakeasy crimes, Ivanov specifically admitted the involvement of  
4 defendant and himself in attacks on Verio, Nara Bank, CNB-Waco, the St. Clair County  
5 Intermediate School District. Ivanov also acknowledged the fraud that he and defendant  
6 operated against eBay and PayPal through the use of automated scripts and their solicitation of  
7 sellers of computer parts, which they purchased using credit cards via PayPal. Exh. A. During  
8 his plea colloquy, Ivanov further explained that he and defendant had “a number of people” who  
9 were working on the programs that implemented the automated fraud. Exh. B, pp. 94-95.  
10 Ivanov also clarified that his criminal agreement with defendant continued through the time of  
11 the Invita meeting in Seattle. Exh. B, pp. 102-103.

### 12 **III. PRESENTENCE REPORT AND SENTENCING GUIDELINE CALCULATIONS**

13 The United States has no objections to the facts set forth in the Presentence Report, and  
14 agrees with the Probation Officer’s calculations under the United States Sentencing Guidelines.  
15 The Total Offense Level is 36. Based on a Criminal History Category of I, the applicable range  
16 of imprisonment is 188-235 months.

17 Defendant, through his counsel’s letters to the Probation Officer, indicated objections to  
18 nearly every paragraph in the PSR. Most of these objections reflect an effort to re-litigate or re-  
19 argue issues that were resolved at defendant’s three-week trial last year. In other words,  
20 defendant fails to acknowledge that he was tried and convicted of conspiracy and 19 substantive  
21 counts of computer abuse and wire fraud for actions that began no later than November 1999  
22 and continued until his arrest on November 10, 2000. The evidence at trial clearly proved that  
23 defendant was part of a conspiracy that included himself, Alexey Ivanov and others; that  
24 defendant owned the business that became known on the Internet as tech.net.ru; that tech.net.ru  
25 was used to hack computers, steal information, cause damage to victims’ computers, and defraud  
26 eBay and PayPal; that defendant exhibited his knowledge and involvement in these activities  
27 through the statements he made during the Invita undercover operation; and that as of mid-  
28 November 2000, defendants’ own accounts (named “kvakin”) on the two Russian computers that

1 were searched by the FBI – the computers named tech.net.ru and freebsd.tech.net.ru – contained  
 2 numerous scripts and programs used for hacking computers as well as defrauding eBay and  
 3 PayPal in an automated fashion using databases of stolen credit card information.

4 With respect to the substantive counts, defendant was convicted because he committed  
 5 the crimes himself, he aided and abetted the commission of the crimes, and/or his  
 6 coconspirator(s) committed these reasonably foreseeable crimes in furtherance of the conspiracy  
 7 of which he was a member. Regardless of which theory or theories of criminal liability are  
 8 accepted, at a bare minimum defendant knowingly assisted and supported all of the charged  
 9 crimes. Because the jury found, beyond a reasonable doubt, that defendant was guilty of the  
 10 conspiracy and all substantive counts, defendant is now precluded from re-litigating that result at  
 11 sentencing. It is irrelevant that the evidence could not establish precisely and in every case  
 12 which member of the conspiracy committed the substantive crimes; all of the crimes were  
 13 reasonable foreseeable and within the scope and in furtherance of the conspiracy.

14 Alexey Ivanov's post-trial statements fully corroborate the evidence presented at trial.  
 15 Defendant managed tech.net.ru and assigned numerous criminal tasks to Ivanov and others in the  
 16 computer hacking and fraud conspiracy. In light of the information Alexey Ivanov has provided  
 17 after defendant's conviction, it is uncertain what objections defendant will continue to lodge  
 18 against the PSR. However, the anticipated guideline issues are addressed below. The United  
 19 States will file a supplementary sentencing memorandum to address arguments raised in  
 20 defendant's sentencing memorandum to the extent necessary.

21 **A. The Sentencing Guidelines that Became Effective on November 1, 2000, Apply to**  
 22 **Defendant's Sentencing.**

23 Defendant has contested the PSR's application of the Sentencing Guidelines that became  
 24 effective on November 1, 2000, arguing that his crimes did not extend beyond that date.<sup>1</sup>  
 25 However, defendant was charged with a conspiracy that began in the fall of 1999 and continued

---

26 <sup>1</sup> Neither the Probation Officer nor the parties are claiming that the currently effective  
 27 Guidelines apply, because the high loss amount in this case would lead to an even higher total  
 28 offense level and a sentence that would raise constitutional *ex post facto* clause issues. *See*  
 U.S.S.G. §1B1.11(b)(1) (court should use guidelines in effect on date that offense was  
 committed if use of current guidelines would violate *ex post facto* clause).

1 until or beyond his arrest on November 10, 2000. Given the jury's verdicts that defendant was a  
2 member of the conspiracy and that he was responsible for substantive counts that began in  
3 November 1999 and continued through the summer of 2000, defendant's involvement in the  
4 criminal conspiracy continued until either he was stopped or he withdrew. He was not stopped  
5 until November 10, 2000, and defendant cannot possibly demonstrate that he somehow withdrew  
6 from the conspiracy prior to November 1, 2000. Defendant's own incriminating statements  
7 during the Invita undercover meeting demonstrate that he was ready and willing to continue  
8 engaging in hacking and credit card fraud. Moreover, as of November 10, 2000, defendant  
9 continued to maintain the same hacking tools, computer scripts, and stolen credit card databases  
10 on his computer system in Russia that he used throughout the scheme. There is no question that  
11 the charged offense continued into the period after November 1, 2000, and that the Sentencing  
12 Guidelines that became effective on that date should apply in the present case. *See U.S.S.G.*  
13 *§1B1.1(b)(3)* (if defendant is convicted of two offenses, one of which is committed after  
14 revised edition of guidelines, then revised addition is applied to both offenses).

15 **B. The PSR's Loss Calculation is Correctly Based on the Conservative Calculation of**  
16 **56,000 Stolen Credit Cards Stored on Defendant's Tech.Net.Ru Computers.**

17 Defendant has challenged the PSR's imposition of a 16-level enhancement under Section  
18 2F1.1(b)(1)(Q) of the Sentencing Guidelines, based on a loss amount of \$28 million. The loss  
19 amount is derived from the extraordinary volume of stolen credit cards that were stored in  
20 databases on defendant's two Russian computers. Expert witness Philip Attfield testified at trial  
21 that he had searched the data on the two computers to determine the number of unique credit  
22 cards, and had found approximately 56,000 credit cards. He did the search by constructing a  
23 program or script that looked for patterns of numbers meeting the criteria for appearing to be a  
24 credit card, including bank identification or "BIN" numbers which consist of four-digit numbers  
25 at the beginning of credit cards. Mr. Attfield further testified that he was familiar with credit  
26 card patterns based on his previous experience in online credit card transaction processing.  
27 Exh. D (Transcript of trial testimony, pp. 1289-1290). Under Application Note 17 to  
28 Section 2F1.1 of the Sentencing Guidelines, each and every stolen credit card is counted for a

1 minimum of \$500 of loss, regardless of actual loss amounts. Thus, 56,000 credit cards results in  
2 a loss amount of \$28 million.

3 These estimates are, in fact, conservative. As Mr. Attfield testified at trial, there were  
4 databases of credit cards that existed on the Russian computers that were not obtained by the  
5 FBI. Mr. Attfield was able to deduce the existence of these additional credit card databases from  
6 defendant's scripts which tapped the databases for stolen credit card information to use in the  
7 eBay/PayPal fraud scheme. Those databases – named mm, mm1, and fuckebay – contained  
8 untold numbers of additional stolen credit cards. Exh. D, pp. 1215-1216, 1243-1248, 1283-84,  
9 1289-1290. Therefore, the 56,000 figure does not include the additional stolen credit cards from  
10 those databases or others that the United States is not seeking to attribute to defendant. See  
11 PSR ¶56-57.

12 Also left uncounted by the arithmetic of the Sentencing Guidelines is the tremendous and  
13 widespread harms to citizens of the United States and other persons whose personal, confidential  
14 identifying information was stolen and used by defendant to commit crimes. The Social Security  
15 numbers, bank account numbers, names, dates of birth, addresses, user names, passwords, and  
16 credit cards of thousands of people were stolen by defendant and his coconspirators. The  
17 personal, non-monetary harms of identity theft are not taken into account by the Sentencing  
18 Guidelines. These unaccounted for harms can justify an upward departure. PSR ¶148;  
19 U.S.S.G. §2F1.1, comment. (n.16). At a minimum, these harms emphasize the conservative  
20 nature of the PSR's calculation of loss.

### 21 C. The Two-Level Mass-Marketing Enhancement Applies.

22 Defendant has challenged the application of a two-level enhancement for commission of  
23 an offense through mass-marketing. See U.S.S.G. §2F1.1(b)(3). The relevant Application Note  
24 provides the following explanation of the enhancement:

25 "Mass-marketing," as used in subsection (b)(3) means a *plan, program,*  
26 *promotion, or campaign that is conducted through solicitation by* telephone,  
27 mail, *the Internet,* or other means to induce a large number of persons to (A)  
28 purchase goods or services; (B) participate in a contest or sweepstakes; or (C)  
invest for financial profit. The enhancement would apply, for example, if the  
defendant conducted or participated in a telemarketing campaign that solicited a  
large number of individuals to purchase fraudulent life insurance policies.



1 U.S.S.G. §2F1.1, comment. (n.3) (emphasis added). There are two independent and sufficient  
2 bases for this enhancement.

3 First, as part of the conspiracy, PayPal customers received email messages stating that  
4 they had received a bonus from PayPal and suggesting that they access a certain website where  
5 the customers were asked to enter their user names and passwords. In fact, the website was a  
6 fake website linked to computers at Lightrealm and surnet.ru, both of which were used by  
7 Ivanov during the conspiracy, and the customers' user names and passwords were being stolen  
8 for use in fraud. PSR ¶59.

9 Second, defendant engaged in a plan or scheme to solicit, via the Internet, large numbers  
10 of computer parts sellers to sell and ship to Kazakstan computer parts in exchange for credit card  
11 payments that defendant would make via PayPal using stolen credit cards. These are the emails  
12 that were sent under the pseudonyms of Greg Stivenson and Murat Nazirov. *Id.* Evidence of  
13 these mass-email solicitations were found on "memphis", one of the computers of the St. Clair  
14 County Intermediate School District that defendant and his coconspirators compromised.  
15 Defendant's own account on the freebsd.tech.net.ru computer contained corresponding evidence  
16 in the form of a file with hundreds of pages of these same emails. Exh. D, pp. 1278-1280. In  
17 addition, one of the computer parts sellers, Tad Brooker, testified that he had received an email  
18 solicitation, sold and shipped parts to Kazakhstan, and received payment via PayPal with what  
19 later turned out to be stolen credit cards. Defendant's mass-marketing merits the two-level  
20 enhancement, because he was able to multiply the force and impact of his fraud through the  
21 power of the Internet.

22 **D. The Two-Level Unauthorized Use of Means of Identification Enhancement Applies.**

23 A two-level enhancement should be applied for using any means of identification to  
24 obtain other means of identification. As noted in the PSR, stolen means of identification –  
25 whether user names, passwords, or credit cards – were the stock in trade of defendant's criminal  
26 activities. The gravamen of the conspiracy was to steal credit cards and associated identifying  
27 information and then use that to obtain further means of identification in the form of email  
28 names and accounts, eBay accounts, and PayPal accounts. In this era of rampant Internet-aided

1 identity theft, which led to this provision, the enhancement is particularly appropriate in a case  
2 like the instant one.

3 **E. The Four-Level Aggravating Role Enhancement Applies Because Defendant Was**  
4 **the Leader of an Extensive Criminal Activity that also Involved Five or More**  
5 **Participants.**

6 Defendant was certainly the leader of the extensive criminal activities that were charged  
7 in the Superseding Indictment and proven at trial. The PSR properly applies Section 3B1.1(a)(1)  
8 of the Sentencing Guidelines, which provides that “[i]f the defendant was an organizer or leader  
9 of a criminal activity that involved five or more participants or was otherwise extensive, increase  
10 by 4 levels.” By his own admission to law enforcement agents and at trial, defendant was the  
11 manager of tech.net.ru, whose computers were used to perpetrate the eBay/PayPal fraud via  
12 various proxy computers around the world. See Exh. C-2 (Transcript of defendant’s trial  
13 testimony), pp. 1800-1801. During the Invita undercover meeting, defendant stated that he had  
14 four “hackers” working for him, *i.e.*, people who were creating hacking tools. Exh. E  
15 (Transcript of Invita undercover meeting, selected pages), pp. 132-133. Even at trial, defendant  
16 testified that by September or October of 2000 he had six people working at his firm. Exh. C-1,  
17 pp. 1734-1736. Thus, by defendant’s own testimony, there were five or more participants in  
18 tech net.ru, which was a criminal enterprise.

19 Although defendant contests this four-level adjustment, there is no question it applies.  
20 Not only were there five or more participants, but the criminal activity “was otherwise  
21 extensive.” The number of computer intrusions, the geographic spread of the victims, the sheer  
22 volume of credit card data and private customer information, and the scope of the fraud in this  
23 case was spectacular. Indeed, the term “otherwise extensive” does not begin to capture the size  
24 and shape of the conspiracy.<sup>2</sup>

---

25  
26  
27 <sup>2</sup> At a bare minimum, even if the Court found that the criminal activity did not involve  
28 five or more persons or was not otherwise extensive, it is plain that defendant was an organizer,  
leader, manager, or supervisor, and therefore subject to at least a two-level enhancement under  
U.S.S.G. §3B1.1(c).

1 **F. The Two-Level Enhancement for Obstruction of Justice Applies Because Defendant**  
2 **Willfully Committed Perjury.**

3 The United States agrees with the PSR that defendant committed perjury at trial and is  
4 therefore subject to the two-level enhancement for obstruction of justice under Section 3C1.1.  
5 The enhancement applies to perjury if: (1) the defendant gave false testimony under oath,  
6 (2) concerning a material matter, (3) with the willful intent to provide false testimony, rather  
7 than as a result of confusion, mistake, or faulty memory. *See United States v. Jimenez*, 300 F.3d  
8 1166, 1170 (9th Cir. 2002) (citing *United States v. Dunnigan*, 507 U.S. 87, 95 (1993)). The  
9 Court must make findings as to each of these three elements.

10 Although defendant's false testimony consists of nearly everything he said on the witness  
11 stand, what particularly stands out as blatant perjury is his claim that he was merely posing as a  
12 hacker during the Invita undercover meeting because Ivanov persuaded him to do so during their  
13 trip from Russia to Seattle on November 9-10, 2000. *See Exh. C-1*, pp. 1747-1751, 1761-1766.  
14 Defendant's contention that he never knew anything about the hacking and fraud activities at his  
15 own company and that he made the incriminating statements during the undercover meeting  
16 strictly as part of some hacker role playing is outrageously false, as the jury obviously found.  
17 The testimony is certainly material, as it went to the heart of the issue of defendant's knowledge  
18 and participation in the charged conspiracy that had begun in the fall of 1999. Finally, it is  
19 equally plain that defendant's perjured testimony was willful, and not the product of a faulty  
20 memory or mistake or confusion, because it was specifically designed to explain away the  
21 devastatingly inculpatory statements that defendant made during the Invita undercover meeting.

22 Defendant's testimony was false, material, and willful, as the Court should find. The  
23 two-level enhancement applies.

24 **IV. GOVERNMENT'S SENTENCING RECOMMENDATION**

25 The United States agrees with the Probation Office that a sentence of 188 months is  
26 appropriate in this case in light of the broad swath of destruction that defendant and his  
27 coconspirators inflicted on e-commerce businesses, banks, schools, credit card companies, and  
28 other victims in the United States and around the world. Defendant and the people he employed

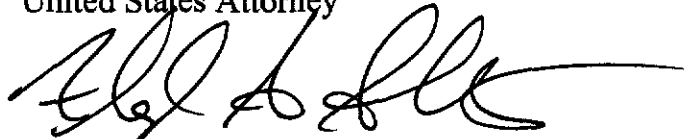
1 at tech.net.ru were engaged in a full-time criminal enterprise. Defendant believed that they  
2 could commit these acts with impunity from offshore, in Russia. He was wrong.

3 This case has achieved media attention in this country and abroad. It is important to  
4 inform the people of the world that they cannot attack victims in our country without facing the  
5 consequences. A sentence of 188 months is a lengthy one, and that is what is required to punish  
6 defendant for the immense harms he inflicted and to deter others who consider committing the  
7 same sorts of crimes.

8 The United States also recommends a three-year term of supervised release, an order to  
9 pay restitution in the amount of \$692,140, and a mandatory special assessment of \$2,000.

10  
11 Dated this 30<sup>th</sup> day of September, 2002.

12 Respectfully submitted,  
13 JOHN McKAY  
14 United States Attorney

15 

16 FLOYD G. SHORT  
17 Assistant United States Attorney

**LIST OF ATTACHED EXHIBITS**

- A. Plea Agreement and Stipulation of Offense Conduct of Alexey Ivanov
- B. Transcript of Plea Colloquy of Alexey Ivanov, selected pages
- C-1. October 4, 2001, Trial Testimony of Vasily Gorshkov, selected pages
- C-2. October 5, 2001, Trial Testimony of Vasily Gorshkov, selected pages
- D. Transcript of Trial Testimony of Philip Attfield, selected pages
- E. Trial Exhibit 1C (Transcript of FBI Invita Undercover Meeting), selected pages

**EXHIBIT A**

---



*United States Attorney  
District of Connecticut*

*Brien McMahon Federal Building  
915 Lafayette Boulevard, Room 309  
Bridgeport, Connecticut 06604*

*(203) 696-3000  
Fax (203) 579-5550*

July 31, 2002

**FILED UNDER SEAL**

C. Thomas Furniss, Esq.  
Furniss & Quinn, P.C.  
248 Hudson Street  
Hartford, Connecticut 06106  
Facsimile: (860) 241-1032

Morgan P. Rueckert, Esq.  
Shipman & Goodwin LLP  
One Landmark Square  
Stamford, CT 06901-2676  
Fax: (203) 324-8199

Re: United States v. Alexey V. Ivanov  
Crim. No. 3-00-CR-183 (AWT) (DCT)  
Crim. No. CR00-550C (WDWA)  
Crim No SA CR 01-96 (CDCA)  
Crim No. SA CR S-01-374 LKK (EDCA)  
Crim No 00-611 (KSH) (DNJ)

Dear Attorneys Furniss and Rueckert:

This letter confirms the plea agreement entered into between your client, Alexey V Ivanov (the "defendant"), and the United States Attorney's Offices for the District of Connecticut, the Western District of Washington, the Central and Eastern Districts of California and the District of New Jersey (the "Government") concerning the referenced criminal cases

**The Plea and Offense**

Alexey Ivanov agrees to plead guilty to Counts Two, Seven and Eight of an eight-count Indictment in the District of Connecticut charging him with Accessing a Protected Computer with the Intent to Defraud in violation of 18 U.S. C. §1030(a)(4), Interference with Commerce by Extortion in violation of 18 U.S.C §1951, and Possession of Access Devices with intent to Defraud in violation of 18 U.S C §1029(a)(3) and (c)(1)(A)(i). He further agrees, pursuant to Fed. R. Crim P. 20 to plead guilty to Counts 1 and 4 of a 20-count Indictment in the Western District of Washington charging him with conspiracy in violation of 18 U.S.C. § 371 and with Intentionally Causing Damage to a Protected Computer in violation of 18 U.S C §1030(a)(5)(A), respectively; a one-count substitute Information in the District of New Jersey charging him with Accessing a Protected Computer with the Intent to Defraud in violation of 18 U.S. C §1030(a)(4); Counts 1 and 11 of a 15-Count Indictment in the Central District of California charging him with wire fraud in violation of 18 U S C. § 1343 and Recklessly Causing Damage

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq  
July 31, 2002  
Page 2

**FILED UNDER SEAL**

to a Protected Computer in violation of 18 U.S.C. § 1030(a)(5)(B); respectively; and Count 12 of a 13-count Indictment in the Eastern District of California, charging him with Intentionally Causing Damage to a Protected Computer in violation of 18 U.S.C. § 1030(a)(5)(A). It is the understanding of the defendant and the Government that, pursuant to Rule 20, Federal Rules of Criminal Procedure, all pleas will be entered simultaneously before the United States District Court in the District of Connecticut. Following sentencing, the Government will dismiss the remaining charges against the defendant.

He understands that to be guilty of Accessing a Protected Computer with the Intent to Defraud in violation of 18 U.S.C. § 1030(a)(4), the following essential elements of the offense must be satisfied:

- 1 The defendant knowingly accessed without or in excess of authorization a protected computer system, that is, a computer system used in interstate or foreign commerce or communication;
2. The defendant acted with intent to defraud;
3. In furtherance of the scheme to defraud, the defendant obtained something of value

He understands that to be guilty of Interference with Commerce by Extortion in violation of 18 U.S.C. § 1951, the following essential elements of the offense must be satisfied.

- 1 The defendant attempted to or did wrongfully obtain the property of another;
2. The defendant attempted to obtain this property with the victim's consent, but that this consent was compelled by the wrongful use or threat of force, violence, or fear; and
3. As a result of the defendant's actions, interstate commerce, or an item moving in interstate commerce, was delayed, obstructed, or affected in any way or degree.

He understands that to be guilty of Possession of Access Devices with intent to Defraud in violation of 18 U.S.C. § 1029(a)(3) and (c)(1)(A)(i), the following essential elements of the offense must be satisfied:



C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 3

**FILED UNDER SEAL**

- 1 The defendant possessed fifteen or more unauthorized access devices, that is, any card, plate, code, account number (whether assigned or not) or other means of account access that can be used alone or in conjunction with another access device to obtain money, goods, services or any other thing of value, or that can be used to initiate a transfer of funds.
- 2 That the defendant acted knowingly, willfully and with the intent to defraud; and
- 3 That interstate or foreign commerce was affected by the defendants actions.

He understands that to be guilty of a conspiracy offense in violation of 18 U S.C. § 371, the following essential elements of the offense must be satisfied:

1. Two or more persons entered into an unlawful agreement as charged on or about the date charged,
2. The defendant knowingly and willfully became a member of the conspiracy charged,
3. One of the members of the conspiracy knowingly committed at least one of the overt acts charged; and
4. The overt acts committed were committed to further some objective of the conspiracy

He understands that to be guilty of wire fraud in violation of 18 U S C. §1343, the following essential elements of the offense must be satisfied:

1. There was a scheme or artifice to defraud or to obtain money or property by materially false or fraudulent pretenses, representations or promises;
2. The defendant knowingly and willfully participated in the scheme or artifice to defraud, with knowledge of the fraudulent nature and with the specific intent to defraud, and
3. In the execution of the scheme, the defendant used or caused the use of an interstate or international wire communication in furtherance of the scheme to defraud

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 4

**FILED UNDER SEAL**

He understands that to be guilty of Intentionally Causing Damage to a Protected Computer in violation of 18 U.S.C. § 1030(a)(5)(A), the following essential elements of the offense must be satisfied:

1. The defendant knowingly caused the unauthorized transmission of a program , code, command, or information to a protected computer system, that is, a *computer system used in interstate or foreign commerce or communication*;
2. The defendant caused the transmission of the program with the intent to impair the integrity or availability of data, a program, a system or information; and
3. The impairment of the data, program system or information resulted in losses to one or more individuals totaling at least \$5,000 in value at any time during a one year period.

He understands that to be guilty of Recklessly Causing Damage to a Protected Computer in violation of 18 U S C § 1030(a)(5)(B), the following essential elements of the offense must be satisfied:

1. The defendant intentionally accessed without authorization a protected computer, that is, a computer system used in interstate or foreign commerce or communication;
2. As a result of the defendant's access, defendant recklessly impaired the integrity or availability of data, a program, a system or information
3. The impairment of the data, program system or information resulted in losses to one or more individuals totaling at least \$5,000 in value at any time during a one year period

### The Penalties

Interference with Commerce by Extortion, in violation of 18 U S C. §1951, carries a maximum penalty of 20 years imprisonment and a \$250,000 fine; Possession of Access Devices with Intent to Defraud, in violation of 18 U.S.C. §1029(a)(3) and (c)(1)(A)(i), carries a maximum penalty of 10 years imprisonment and a \$250,000 fine; the substantive conspiracy offense carries a maximum penalty of 5 years imprisonment and a \$250,000 fine; the wire fraud offense carries a maximum penalty of 5 years imprisonment and a \$250,000 fine, and each of the offenses involving computers under 18 U S.C. §1030 carry a maximum penalty of 5 years imprisonment

C. Thomas Furniss, Esq.  
Morgan P Rueckert, Esq.  
July 31, 2002  
Page 5

**FILED UNDER SEAL**

and a \$250,000 fine. In addition, under 18 U.S.C. § 3583, the Court may impose a term of supervised release of not more than 3 years on each count, to begin at the expiration of any term of imprisonment imposed. The defendant understands that should he violate any condition of the supervised release during its term, he may be required to serve a further term of imprisonment of up to two years, with no credit for the time already spent on supervised release.

The defendant also is subject to the alternative fine provision of 18 U.S.C. § 3571. Under this section, the maximum fine that may be imposed on the defendant as to each count is the greatest of the following amounts: (1) twice the gross gain to the defendant resulting from the offense; (2) twice the gross loss resulting from the offense; (3) \$250,000; or (4) the amount specified in the section defining the offense.

In addition, the defendant is obligated by 18 U.S.C. § 3013 to pay a special assessment of \$100 on each count of conviction.

Finally, unless otherwise ordered, should the Court impose a fine of more than \$2,500 as part of the sentence, interest will be charged on the unpaid balance of a fine amount not paid within 15 days after the judgment date. 18 U.S.C. § 3612(f). Other penalties and fines may be assessed on the unpaid balance of a fine pursuant to 18 U.S.C. §§ 3572 (h), (i) and 3612(g).

#### Restitution

In addition to the other penalties provided by law, the Court must also order that the defendant make restitution under 18 U.S.C. § 3663A. See attached Rider

#### Financial Disclosure and Forfeiture

The defendant agrees to fully and completely disclose all funds and assets obtained as a result of the criminal conduct to which he is pleading guilty and to identify to the United States all assets obtained through such activity. The defendant further agrees that he will not make any claim which is adverse to the government in any forfeiture proceedings that may be instituted against these assets or any other assets obtained by or traceable to the criminal activity which forms the basis for the charges in this matter.

#### Sentencing Guidelines

##### 1 Applicability

The defendant understands that the Sentencing Reform Act of 1984 and the Sentencing Guidelines apply in this case. The defendant understands that the Court is required to consider

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 6

**FILED UNDER SEAL**

any applicable Sentencing Guidelines but may depart from those Guidelines under some circumstances. The defendant expressly understands that the Sentencing Guideline determinations will be made by the Court, based upon input from the defendant, the Government, and the United States Probation Officer who prepares the Presentence investigation report. The defendant further understands that he has no right to withdraw his guilty plea if his sentence or the Guideline application is other than he anticipated.

2        Acceptance of Responsibility

At this time, the Government agrees to recommend that the Court reduce by three levels the defendant's Adjusted Offense Level under section 3E1.1 of the Sentencing Guidelines, based on the defendant's prompt recognition and affirmative acceptance of personal responsibility for the offense. This recommendation is conditioned upon the defendant's full, complete, and truthful disclosure to the Probation Office of information requested, of the circumstances surrounding his commission of the offense, of his criminal history, and of his financial condition. In addition, this recommendation is conditioned upon the defendant timely providing complete information to the Government concerning his involvement in the offense to which he is pleading guilty. The defendant expressly understands that the Court is not obligated to accept the Government's recommendation on the reduction.

The Government will not make this recommendation if the defendant engages in any acts which (1) indicate that the defendant has not terminated or withdrawn from criminal conduct or associations (Sentencing Guideline section 3E1.1); (2) could provide a basis for an adjustment for obstructing or impeding the administration of justice (Sentencing Guideline section 3C1.1); or (3) constitute a violation of any condition of release. The defendant expressly understands that he may not withdraw his plea of guilty if, for the reasons explained above, the Government does not make this recommendation.

3.        Appeal Rights Regarding Sentencing

The parties reserve their respective rights to appeal and to oppose each other's appeal of the sentence imposed as permitted by the statute.

4.        Guideline Calculation

The Government and defendant have agreed that the applicable Guidelines analysis is as follows: The sentencing guideline range is determined level under U.S.G. § 2E1.1, which directs that the base level is determined by the underlying conduct involved in the racketeering activity, which here includes extortion and fraud.

C. Thomas Furniss, Esq  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 7

**FILED UNDER SEAL**

The relevant conduct here includes 6 extortions [OIB, Inc., Goodnews, Speakeasy, Dexis/Sterling, Casinovega and FSI]. Under U.S.S.G. § 2B3.2, each of these extortions has a base offense level of 18. Under U.S.S.G. § 3B1.3 each of these offense levels are enhanced by 2 level because of the defendant's use of a special skill, for adjusted offense levels of 20 each. Under U.S.S.G. § 3D1.1(d) these offenses are not grouped.

The relevant conduct here also includes fraud using access devices, including credit card and bank accounts. Under U.S.S.G. § 2F1.1 the base offense level is 6. The total number of unique access devices involved in the relevant offense conduct is over 50,000 which results in a minimum increase in offense level of 16 to 22. The relevant offense conduct involved more than minimal planning under § 2F1.1(b)(2), increasing the offense level an additional 2 levels. It involved mass marketing under § 2F1.1(b)(3), increasing the offense level an additional 2 levels. It involved the trafficking in unauthorized access devices under § 2F1.1(b)(5), increasing the offense level an additional 2 levels. Since a substantial part of the fraudulent scheme was committed from outside the United States, the offense level increased an additional 2 levels. Thus the total offense level is 30. The defendant asserts that the defendant's offense level is increased an additional three levels under U.S.S.G. § 3B1.1, and the Government asserts that the defendant's offense level is increased an additional four levels, under U.S.S.G. § 3B1.1. This results in an offense level of 33-34.

Under these calculations, grouping will not increase the total offense level beyond 33-34. Under U.S.S.G. § 3E1.1, the defendant's total offense level of 33-34 is reduced by 3 levels to 30-31.

Based on the defendant's representation of his criminal history, his criminal history category is I. The Government reserves the right to recalculate criminal history if defendant's representation proves inaccurate.

A total offense level of 30-31 with a criminal history category I results in a Guidelines range of 97-121 through 108-135 months' imprisonment (sentencing table) and a Guidelines fine range of \$15,000 to twice the proposed loss, no more than \$150,000, unless the defendant establishes that he is unable to pay and not likely to become able to pay any fine. U.S.S.G. § 5E1.2.

The defendant expressly understands that the Court is not bound by this agreement on the Guideline and fine ranges specified above. The defendant further expressly understands that he will not be permitted to withdraw the plea of guilty if the Court imposes a sentence outside the Guideline range or fine range set forth in this agreement. Each party reserves its right to make arguments for departures from this guideline range.

C. Thomas Furniss, Esq.  
Morgan P Rueckert, Esq.  
July 31, 2002  
Page 8

**FILED UNDER SEAL**

In the event the Probation Office or the Court contemplates any sentencing calculations different from those stipulated by the parties, the parties reserve the right to respond to any inquiries and make appropriate legal arguments regarding the proposed alternate calculations. Moreover, the parties reserve the right to challenge or defend any sentencing determination, other than that stipulated by the parties, in any post-sentencing proceeding.

### Waiver of Rights

#### Waiver of Right to Indictment

The defendant understands that he has the right to have charges to which he is pleading in the District of New Jersey presented to a federal grand jury, consisting of between sixteen and twenty-three citizens, twelve of whom would have to find probable cause to believe that he committed the offense set forth in the information before an indictment could be returned. The defendant expressly acknowledges that he is waiving his right to be indicted on these charges knowingly and intelligently

#### Waiver of Trial Rights and Consequences of Plea

The defendant understands that he has the right to be represented by an attorney at every stage of the proceeding and, if necessary, one will be appointed to represent him.

The defendant understands that he has the right to plead not guilty or to persist in that plea if it has already been made, the right to be tried by a jury with the assistance of counsel, the right to confront and cross-examine the witnesses against him, the right not to be compelled to incriminate himself, and the right to compulsory process for the attendance of witnesses to testify in his defense. The defendant understands that by pleading guilty he waives and gives up those rights and that if the plea of guilty is accepted by the Court, there will not be a further trial of any kind. The defendant further agrees to withdraw any outstanding pretrial motions prior to entering his plea.

The defendant understands that if he pleads guilty, the Court may ask him questions about each offense to which he pleads guilty, and if he answers those questions falsely under oath, on the record, and in the presence of counsel, his answers may later be used against him in a prosecution for perjury or making false statements.

The defendant understands and agrees that should the conviction following defendant's plea of guilty pursuant to this plea agreement be vacated or the plea agreement be breached for any reason, then any prosecution that is not time-barred by the applicable statute of limitations on the date of the signing of this plea agreement may be commenced or reinstated against defendant,

C Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 9

**FILED UNDER SEAL**

notwithstanding the expiration of the statute of limitations between the signing of this plea agreement and the commencement or reinstatement of such prosecution. In this respect, the defendant agrees to waive all defenses based on the statute of limitations with respect to any prosecution that is not time-barred on the date the plea agreement is signed.

Acknowledgment of Guilt; Voluntariness of Plea

The defendant acknowledges that he is entering into this agreement and is pleading guilty freely and voluntarily because he is guilty. The defendant further acknowledges that he is entering into this agreement without reliance upon any discussions between the Government and him (other than those described in the plea agreement letter), without promise of benefit of any kind (other than the concessions contained in the plea agreement letter), and without threats, force, intimidation, or coercion of any kind. The defendant further acknowledges his understanding of the nature of the offenses to which he is pleading guilty, including the penalties provided by law. The defendant also acknowledges his complete satisfaction with the representation and advice received from his undersigned attorneys. The defendant and his undersigned counsel are unaware of any conflict of interest concerning counsels' representation of the defendant in the case.

Scope of Agreement

The defendant acknowledges and understands that this agreement is limited to the undersigned parties and cannot bind any other federal authority, or any state or local authority. The defendant acknowledges that no representations have been made to him with respect to any civil or administrative consequences that may result from this plea of guilty because such matters are solely within the province and discretion of the specific administrative or governmental entity involved. Finally, the defendant understands and acknowledges that this agreement has been reached without regard to any civil tax matters that may be pending or which may arise involving him.

The defendant expressly acknowledges that he is not a "prevailing party" within the meaning of Public Law 105-119, section 617 ("the Hyde Amendment") with respect to the counts of conviction or any other counts or charges that may be dismissed pursuant to this agreement. The defendant voluntarily, knowingly, and intelligently waives any rights he may have to seek reasonable attorney's fees and other litigation expenses under the Hyde Amendment.

Collateral Consequences

The defendant further understands that he will be adjudicated guilty of each offense to which he has pleaded guilty and will be deprived of certain rights, such as the right to vote, to hold public office, to serve on a jury, or to possess firearms. The defendant understands that the

C. Thomas Furniss, Esq.  
Morgan P Rueckert, Esq.  
July 31, 2002  
Page 10

**FILED UNDER SEAL**

Government reserves the right to notify any state or federal agency by whom he is licensed, or with whom he does business, of the fact of his conviction.

Satisfaction of Federal Criminal Liability; Breach

The defendant's guilty pleas, if accepted by the Court, will satisfy the federal criminal liability of the defendant in the Districts represented below as a result of his participation in the conduct which forms the basis of the Indictments and Information in this case, including the conduct outlined in the attached Stipulation of Offense Conduct. Following sentencing, the Government will dismiss the remaining counts against the defendant in this case

The defendant understands that if, before sentencing, he violates any term or condition of this agreement, engages in any criminal activity, or fails to appear for sentencing, the Government may void all or part of this agreement. The defendant, however, will not be permitted to withdraw his plea of guilty.

No Other Promises

The defendant acknowledges that no other promises, agreements, or conditions have been entered into other than those set forth in this plea agreement, and none will be entered into unless set forth in writing, signed by all the parties.

This letter shall be presented to the Court and filed in this case.

Very truly yours,

JOHN A. DANAHER  
UNITED STATES ATTORNEY  
DIST. OF CONNECTICUT

  
MARK G. CALIFANO  
SHAWN J. CHEN  
ASSISTANT U.S. ATTORNEYS

JOHN MCKAY  
UNITED STATES ATTORNEY  
WESTERN DIST. OF WASHINGTON

FLOYD G. SHORT  
ASSISTANT U.S. ATTORNEYS



C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 10

UNDER SEAL

Government reserves the right to notify any state or federal agency by whom he is licensed, or with whom he does business, of the fact of his conviction.

Satisfaction of Federal Criminal Liability; Breach

The defendant's guilty pleas, if accepted by the Court, will satisfy the federal criminal liability of the defendant in the Districts represented below as a result of his participation in the conduct which forms the basis of the Indictments and Information in this case, including the conduct outlined in the attached Stipulation of Offense Conduct. Following sentencing, the Government will dismiss the remaining counts against the defendant in this case.

The defendant understands that if, before sentencing, he violates any term or condition of this agreement, engages in any criminal activity, or fails to appear for sentencing, the Government may void all or part of this agreement. The defendant, however, will not be permitted to withdraw his plea of guilty.

No Other Promises

The defendant acknowledges that no other promises, agreements, or conditions have been entered into other than those set forth in this plea agreement, and none will be entered into unless set forth in writing, signed by all the parties.

This letter shall be presented to the Court and filed in this case.

Very truly yours,

JOHN A. DANAHER  
UNITED STATES ATTORNEY  
DIST. OF CONNECTICUT

MARK G. CALIFANO  
SHAWN J. CHEN  
ASSISTANT U.S. ATTORNEYS

JOHN MCKAY  
UNITED STATES ATTORNEY  
WESTERN DIST. OF WASHINGTON



FLOYE G. SHORT  
ASSISTANT U.S. ATTORNEYS

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 11

**FILED UNDER SEAL**

DEBRA W. YANG  
UNITED STATES ATTORNEY  
CENTRAL DIST. OF CALIFORNIA

CHRISTOPHER J. CHRISTIE  
UNITED STATES ATTORNEY  
DIST. OF NEW JERSEY

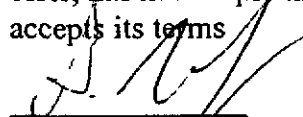
ARIF ALIKHAN  
ASSISTANT U.S. ATTORNEY

SCOTT S. CHRISTIE  
ASSISTANT U.S. ATTORNEY

JOHN K. VINCENT  
UNITED STATES ATTORNEY  
EASTERN DIST. OF CALIFORNIA

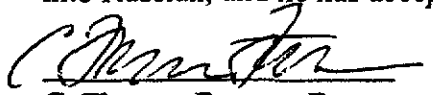
MARK L. KROTOSKI  
ASSISTANT U.S. ATTORNEY

The defendant certifies that he has read this plea agreement letter and its attachments, has been offered an opportunity to have it translated into Russian and has accepted/declined that offer, has had ample time to discuss this agreement with counsel and fully understands and accepts its terms


  
\_\_\_\_\_  
Alexey V Ivanov  
The Defendant

8/2/02  
Date

I have read the above and explained it to my client, who advises me that he understands and accepts its terms I have discussed with my client the option of having this letter translated into Russian, and he has accepted/declined this offer.

  
\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

8/2/02  
Date

  
\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

8/2/02  
Date


I have translated this agreement from English in to Russian for the defendant.

\_\_\_\_\_  
Translator

\_\_\_\_\_  
Date

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 11

UNDER S

DEBRA W. YANG  
UNITED STATES ATTORNEY  
CENTRAL DIST. OF CALIFORNIA  
  
ARIF ALIKHAN  
ASSISTANT U.S. ATTORNEY

CHRISTOPHER J. CHRISTIE  
UNITED STATES ATTORNEY  
DIST. OF NEW JERSEY  
  
SCOTT S. CHRISTIE  
ASSISTANT U.S. ATTORNEY

JOHN K. VINCENT  
UNITED STATES ATTORNEY  
EASTERN DIST. OF CALIFORNIA

MARK L. KROTOSKI  
ASSISTANT U.S. ATTORNEY

The defendant certifies that he has read this plea agreement letter and its attachments, been offered an opportunity to have it translated into Russian and has accepted/declined that offer, has had ample time to discuss this agreement with counsel and fully understands and accepts its terms.

\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

\_\_\_\_\_  
Date

I have read the above and explained it to my client, who advises me that he understands and accepts its terms. I have discussed with my client the option of having this letter translated into Russian, and he has accepted/declined this offer.

\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

I have translated this agreement from English in to Russian for the defendant.

\_\_\_\_\_  
Translator

\_\_\_\_\_  
Date

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
August 1, 2002  
Page 11

UNDER SEAL

DEBRA W. YANG  
UNITED STATES ATTORNEY  
CENTRAL DIST. OF CALIFORNIA

CHRISTOPHER J. CHRISTIE  
UNITED STATES ATTORNEY  
DIST. OF NEW JERSEY

ARIF ALIKHAN  
ASSISTANT U.S. ATTORNEY

SCOTT S. CHRISTIE  
ASSISTANT U.S. ATTORNEY

JOHN K. VINCENT  
UNITED STATES ATTORNEY  
EASTERN DIST. OF CALIFORNIA

  
MARK L. KROTOSKI  
ASSISTANT U.S. ATTORNEY

The defendant certifies that he has read this plea agreement letter and its attachments, has been offered an opportunity to have it translated into Russian and has accepted/declined that offer, has had ample time to discuss this agreement with counsel and fully understands and accepts its terms.

\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

\_\_\_\_\_  
Date

I have read the above and explained it to my client, who advises me that he understands and accepts its terms. I have discussed with my client the option of having this letter translated into Russian, and he has accepted/declined this offer.

\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

I have translated this agreement from English in to Russian for the defendant.

\_\_\_\_\_  
Translator

\_\_\_\_\_  
Date

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
August 1, 2002  
Page 11

UNDER SEAL

DEBRA W. YANG  
UNITED STATES ATTORNEY  
CENTRAL DIST. OF CALIFORNIA

CHRISTOPHER J. CHRISTIE  
UNITED STATES ATTORNEY  
DIST. OF NEW JERSEY

  
SCOTT S. CHRISTIE  
ASSISTANT U.S. ATTORNEY

ARIF ALIKHAN  
ASSISTANT U.S. ATTORNEY

JOHN K. VINCENT  
UNITED STATES ATTORNEY  
EASTERN DIST. OF CALIFORNIA

MARK L. KROTOSKI  
ASSISTANT U.S. ATTORNEY

The defendant certifies that he has read this plea agreement letter and its attachments, has been offered an opportunity to have it translated into Russian and has accepted/declined that offer, has had ample time to discuss this agreement with counsel and fully understands and accepts its terms.

\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

\_\_\_\_\_  
Date

I have read the above and explained it to my client, who advises me that he understands and accepts its terms. I have discussed with my client the option of having this letter translated into Russian, and he has accepted/declined this offer.

\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Date

I have translated this agreement from English in to Russian for the defendant.

\_\_\_\_\_  
Translator

\_\_\_\_\_  
Date

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 12

**FILED UNDER SEAL**

### STIPULATION OF OFFENSE CONDUCT

The defendant and the Government submit the following as a stipulation of conduct which forms the basis of the plea in this case:

#### The Enterprise and Conspiracy

Defendant ALEKSEY V IVANOV, Vassily Gorshkov, and other persons and entities were members and associates of an enterprise as defined by Title 18, United States Code, § 1961(4), to wit, a group of individuals and entities associated in fact whose members engaged in acts involving extortion; mail, wire and access device fraud, and money laundering. This enterprise defined above was engaged in and its activities affected interstate and foreign commerce.

One of the purposes, among others, of the enterprise was to secure economic benefits for its members through the associated individuals and entities (1) by obtaining unauthorized access to computer systems which were used by financial institutions and other commercial businesses in interstate and foreign commerce and communication, (2) by stealing confidential financial information and other data (including access devices) from these systems, (3) by obtaining funds through acts including extortion and mail, wire and access device fraud, and (4) by obtaining merchandise for their own use and benefit and for later resale. It was also the purpose of the enterprise to obtain, by acts involving mail, wire and access device fraud and money laundering, funds and merchandise in order to support and promote the operations of the enterprise and further its illegal goals and objectives

Beginning in or about 1999, in the District of Connecticut, the Western District of Washington, the Central and Eastern Districts of California, the District of New Jersey, Russia and elsewhere, IVANOV, Gorshkov, other individuals associated with the entity known as tech.net.ru, and other persons and entities were employed by and associated with the enterprise above. This enterprise engaged in activities which affected interstate and foreign commerce, including mail, wire and access device fraud; extortion and money laundering. As members of this enterprise, IVANOV, Gorshkov and other persons knowingly and intentionally combined, conspired, confederated, and agreed with each other to (1) conduct and participate, directly and indirectly, in the conduct of the affairs of the enterprise through a pattern of racketeering activity through the commission of a pattern of racketeering acts, including the acts identified below, and (2) to commit offenses against the United States, including violations of 18 U.S.C. §§1030 (computer intrusion, fraud and extortion), 1029 (fraud in connection with access devices), 1341 (mail fraud), 1343 (wire fraud), 1951 (interference in commerce by extortion), and 1956 (money laundering)

It was a part of the enterprise and conspiracy that IVANOV, Gorshkov and the other conspirators used computer systems located in Russia, the United States and elsewhere

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 13

**FILED UNDER SEAL**

(including the tech.net.ru computer systems) to conduct searches and scans on the Internet in order to identify victim computer systems vulnerable to attack and unauthorized access; to store computer intrusion and "hacking" tools and programs; to transmit computer intrusion and "hacking" tools, programs, and other data to other computer systems; and to execute these computer intrusion and "hacking" tools and programs. Using these computer systems IVANOV, Gorshkov and others exploited vulnerabilities in these computer systems, which were used in interstate and foreign commerce and communication and by financial institutions, in order to obtain unauthorized access and access in excess of authorization to those systems. They stole information and data from these systems, including confidential user accounts, password files, systems files, credit card, merchant and bank account numbers, storing it on computers in Russia and elsewhere, including the systems of tech.net.ru and IVANOV's laptop computer. They exchanged this information with each other and used it to purchase funds and merchandise for their own use, and for use in the criminal enterprise and conspiracy. IVANOV, Gorshkov and others contacted and communicated with the victims whose computers they had accessed and compromised, for the purpose of extorting money from those victims, by threatening to damage their computer systems and to take and publish confidential financial and other data from those systems obtained through unauthorized access. They used e-mail accounts obtained from certain Internet Service providers (ISPs) and Internet Relay Chat (IRC) protocols to communicate extortion demands to victims and to fraudulently obtain funds and merchandise.

#### Specific Conduct

*Beginning in the fall of 1999, a number of Internet-related businesses in the United States including but not limited to those identified below, suffered computer intrusions, or "hacks," into their computer systems that originated from Russia, intrusions that were executed and assisted by IVANOV, Gorshkov and their coconspirators, who were members of the enterprise identified above. These individuals gained control of the victims' computers and, among other things: (1) accessed, copied and stole private, confidential data that included computer system account and password data and merchant, credit card and bank account information, and/or (2) used these systems to scan and gain unauthorized access to other victim systems. In several instances, they used this stolen information to extort the victims by demonstrating their control over the victims' computer systems and information. They threatened to publish and use the stolen data and information, and to inflict damage on the computer systems unless the victim paid money or gave the hacker a job. In addition, they used the stolen financial information to make fraudulent purchases of goods and services from sellers in the United States and elsewhere.*

#### Unauthorized Access and Use of Internet Service Providers

In the fall of 1999, IVANOV, Gorshkov and their conspirators obtained unauthorized access into the computer systems of several Internet service providers ("ISPs"), including Vero, which is headquartered in Englewood, Colorado; Channel 1 Communications, which is located in Cambridge, Massachusetts; Lightrealm Communications (now known as Hostpro) in Kirkland,

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 14

**FILED UNDER SEAL**

Washington; and CTS Network Services, in San Diego, California. IVANOV, Gorshkov and others stole confidential data from these systems, including passwords and access devices, including credit card and merchant account numbers, and they exchanged this information with each other. For example, IVANOV initially used a stolen credit card number to open an Internet account with CTS and thereafter used the account to obtain unauthorized access into CTS computer systems. IVANOV, Gorshkov and their coconspirators provided each other with unauthorized access to and use of such computer systems, including the systems of Lightrealm and CTS. They used these computer systems as a "proxy" or base of operations for further unauthorized intrusions into and connections to other victim computer systems in the United States and elsewhere. These proxy systems concealed their use of computer systems in Russia, including those of tech.net.ru, and made it appear that the unauthorized intrusions and connections were coming from the United States.

Some of the ISPs detected these unauthorized intrusions, including Lightrealm and CTS. These ISPs gave IVANOV an account on their systems and made payments to him by transferring funds to Russia. In other instances, such as with Channel 1 Communications, IVANOV contacted the ISP after he had gained unauthorized access and stolen credit card account numbers, shared the access with his coconspirators and collected funds from Channel 1 which he shared with one of his coconspirators.

Unbeknownst to these ISPs, IVANOV and his coconspirators took advantage of their authorized and unauthorized access to the computer systems of these ISPs to steal databases that contained passwords and credit card and other financial information, to search for and scan victim systems, to gain unauthorized access into victim systems, to steal confidential data, including access devices and other financial data from victim systems, and to send extortionate communications to victim computer systems in an effort to obtain money and work from the victims. Much of the information stolen from these ISPs was stored on the computer systems of tech.net.ru. IVANOV stole credit card account numbers from Lightrealm customer Pluscellular, which he, Gorshkov and other conspirators used to fraudulently obtain funds and merchandise.

#### Speakeasy Network

Another of these victims was Speakeasy, an ISP located in Seattle, Washington. IVANOV and his coconspirators obtained unauthorized access to Speakeasy's computer network from computer systems located in Russia, at the end of November 1999. They were able to obtain unauthorized access to the system administrator's account – the account known as "root" or the "superuser" – on several Speakeasy computers. They also obtained credit card account numbers and several password files from Speakeasy systems, several of which were transferred to and stored on the systems of tech.net.ru.

On November 29, 1999, IVANOV, using the screen name "\_subb\_", engaged a Speakeasy employee in an IRC chat session. During the chat session, IVANOV stated that he



C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 15

**FILED UNDER SEAL**

had found holes in Speakeasy's network security, that he wanted a job and \$1,000 - \$1,500 per month, and that he would not tell Speakeasy about the security holes until he got a job. IVANOV stated that he had 2000 user passwords from Speakeasy, as well as credit cards. IVANOV also told Speakeasy representatives that he lived in Russia and that he could not be prosecuted in Russia because Russia did not have strong computer-crime laws.

After a brief hiatus, IVANOV again contacted Speakeasy, just before December 24, 1999. He again demanded a job and money, stating that it would be better for Speakeasy to give him a job than for Speakeasy to get hacked, have all of its files deleted, and have its customers' credit cards used. He demonstrated that he had credit card information by posting it on a web site that Speakeasy hosted. Since Speakeasy refused to pay any money to IVANOV or give him a job, IVANOV deleted files on one of Speakeasy's main computers and on one of its customer's computers, causing over \$5,000 in damage to those computers.

#### VPM Internet Services

VPM Internet Services LLC ("VPM"), was an Internet Service Provider located in Folsom, California. Between approximately December 1999 and February 2000, IVANOV and a coconspirator conducted a series of unauthorized intrusions into the computer network of VPM. On or about December 9, 1999, they scanned the network of VPM to obtain an Internet Protocol map of the network and to identify vulnerable network services. After mapping the VPM network, on or about December 10, 1999, and again from on or about January 10, 2000 through January 19, 2000, they installed a sniffer on the VPM network and thereby obtained log-in and password information from the VPM system. They also installed back doors so they could access the system if security measures were imposed. On or about December 10, 1999, they obtained password files from four separate VPM computers, several of which were transferred to and stored on the computer systems of tech net ru.

In or about December 1999, defendant IVANOV and another coconspirator obtained root-level or administrator-level access to VPM computers which provided them with full control of the computers from a remote location. After root-level access was obtained, they set up two Internet Relay Chat channels to contact and communicate with VPM representatives. During these communications, they demanded money from VPM and threatened to destroy data on VPM systems. They also prepared and sent an extortion communication to an officer of VPM.

During this period, IVANOV and a coconspirator deleted log files, inserted surreptitious programs, changed system files, and installed hacker tools on the VPM computer systems. On or about December 24, 1999, they changed .rhost files on a VPM computer which controlled user access to the VPM computer. These unauthorized intrusions resulted in losses to VPM totaling over \$5,000. VPM's system is a protected computer used in interstate and foreign commerce and communication.

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq  
July 31, 2002  
Page 16

**FILED UNDER SEAL**

As with the ISPs identified above, IVANOV and at least one other coconspirator also used their unauthorized access to the network of VPM to make further unauthorized access and intrusions to the networks of other victims. In this manner, they used VPM computer systems as a proxy system for further unauthorized intrusions into and connections to protected computers in order to conceal their use of computer systems in Russia and to make it appear that the unauthorized intrusions and connections were coming from the United States. Some of the computer systems accessed in this manner included the computer systems of the following United States companies: Commuter Communication Systems Incorporated on or about December 23 through 25, 1999; Eicon Networks on or about December 19, 20 and 24, 1999; OneNet Communications on or about December 21 through December 24, 1999; Anythinking net on or about December 24, 1999; and Signio.com on or about December 24, 1999. Data taken from some of these computer systems, including password files, was stored on the tech.net.ru computer systems.

#### Goodnews Internet Service

Goodnews Internet Service ("Goodnews"), located in Cincinnati, Ohio and was an Internet Service Provider ("ISP") engaged in providing interstate and foreign Internet communications service in interstate and foreign commerce.

From in or before January 23, 2000, and continuing through at least February 7, 2000, IVANOV, using the computer systems at tech.net.ru, and at least one coconspirator obtained unauthorized access to the computer systems of Goodnews and stole the password file from one of the Goodnews computer systems. IVANOV stored one of these password files and other data from Goodnews on the tech.net.ru computer systems. Both attempted to extort the ISP. The coconspirator sent e-mail messages to representatives of Goodnews indicating that he had obtained root access to one of the Goodnews systems and that he had decided not to inflict damage, but instead offered to exchange information regarding the vulnerabilities for payment. Soon thereafter IVANOV sent e-mails to representatives of Goodnews stating that he was a security engineer of Lightrealm, Inc. and offering to check the computer systems. IVANOV offered in one e-mail that if he found no vulnerabilities Goodnews would owe him nothing, but that if he found vulnerabilities, Goodnews would owe him \$9999. In fact, and as IVANOV knew, he was not a Lightrealm engineer and he had concealed from Goodnews representatives that he already had gained access to Goodnews systems and had already obtained information on its vulnerabilities.

#### Online Information Bureau

Online Information Bureau, Inc. ("OIB"), located in Vernon, Connecticut, was a financial transaction clearinghouse that assisted in the processing of merchant credit card and financial transactions. In December of 1999, IVANOV and his coconspirators used a number of computer systems in Russia, including those of tech.net.ru, to obtain unauthorized access into the computer

C. Thomas Furniss, Esq  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 17

**FILED UNDER SEAL**

systems of OIB. They accessed and stole confidential data from the systems, including passwords and credit card account numbers. They stored a significant portion of this data on their computer systems in Russia, including the systems of tech.net.ru.

From on or about January 29, 2000, and continuing until on or about February 3, 2000, IVANOV sent e-mail messages to representatives of OIB, Inc. seeking payment and employment in exchange for providing computer security services. Despite requests by OIB representatives that IVANOV stop his solicitation, IVANOV continued to send e-mail messages. In these e-mail messages, IVANOV demonstrated that he had obtained the root passwords to and control of a number of the OIB computer systems. He also sent an e-mail message that contained threats to cause damage to OIB and OIB's computers by taking confidential merchant account information from OIB computer systems and posting it on the Internet, and by destroying all of the data on certain OIB computer systems. These communications prompted the administrator of the OIB systems to immediately disconnect the OIB systems from the Internet, in order to avoid such damage.

IVANOV and his conspirators also shared information about OIB computer systems and how to access them. In March 2000, they used OIB's computer systems as a proxy system to search for and scan additional victims, and to transfer the information gathered to a number of computer systems in Russia. They also used the systems to send an e-mail communication to representatives of another victim, Financial Services Incorporated, outlined below

#### J2Global Communications (JFAX)

J2 Global Communications ("JFAX") was an ISP located in Hollywood, California. In or about January or March 2000, IVANOV obtained unauthorized access into the computer systems of JFAX.. Using this unauthorized access, IVANOV accessed and downloaded a significant amount of credit card numbers on several occasions. He stored these account numbers on the tech.net.ru computer systems and used them to defraud United States merchants by obtaining merchandise and other things of value.

#### Sterling Microsystems

Sterling Microsystems, ("Sterling") located in Anaheim, California, was a computer hardware and Internet service company that provided credit card processing services for on-line retailers, including credit card merchant accounts and electronic mail services, through its website "DEXIS.NET" Sterling maintained financial information and other data regarding its customers on the DEXIS.NET computer systems

In or about February 2000, IVANOV and a coconspirator gained unauthorized access to the computer system of Sterling, using a vulnerability on the DEXIS.NET webserver to gain access to Sterling's credit card database and other data. After gaining unauthorized access to

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 18

**FILED UNDER SEAL**

Sterling's computer system, IVANOV transferred credit card databases, user names, passwords and other data from Sterling's computer system to the computer system at CTS for the purpose of executing the fraudulent scheme. Specifically, on February 18, 2000 IVANOV transmitted a File Transfer Protocol command from Chelyabinsk, Russia to the computer systems of Sterling to transfer the credit card database to the CTS computer system

IVANOV unauthorized access to Sterling's computer systems caused the impairment of the integrity of the data contained on the systems and resulted in more than \$5,000 in loss to Sterling within a one-year period.

#### Financial Services Incorporated

Financial Services, Inc. ("FSI") was an Internet web hosting and electronic banking processing company located in Glen Rock, New Jersey. One of the computers on the FSI system, identified by the company as "Ralph", was one of several computers on which were stored employee passwords for the FSI computer network. Another computer on this network, a machine in Glen Rock identified by the company as "Trixie", was the primary computer used by employees of FSI for storing customer credit card numbers and related customer data

On or about March 22, 2000, IVANOV and a coconspirator, via an Internet connection from Russia, accessed the Ralph machine and the Trixie machine at FSI without authorization and downloaded: (a) eleven passwords used by FSI employees to access the FSI computer network; and (b) a text file containing approximately 3,500 credit card numbers and associated card holder information for FSI customers. IVANOV shared this information with his coconspirators, knowing that his coconspirators would use this information to defraud or extort FSI. In or about April 2000, IVANOV transferred the stolen FSI passwords to a file named "PASS\_FSI" on his laptop computer to facilitate future unauthorized access into the FSI computer network.

On or about March 29, 2000, one of IVANOV's coconspirators, using the aliases "Alexander" and "Grisha," sent an e-mail message from Russia to an employee of FSI in Glen Rock, New Jersey, in which he stated that he was part of a group of computer hackers who had accessed the FSI computer system without authorization and had stolen customer credit card numbers and associated card holder information for FSI customers. In the e-mail message, the coconspirator threatened to publicly release this stolen credit card information unless FSI paid him \$3,000. When the FSI employee failed to immediately agree to pay him \$3,000, this coconspirator sent this same FSI employee an electronic message via the Internet from Russia using the alias "Jimbo" in which he doubled his extortion demand to \$6,000. After further communications with the FSI employee, this coconspirator agreed to settle for an extortion payment of \$5,000 from FSI

C. Thomas Furniss, Esq.  
 Morgan P Rueckert, Esq.  
 July 31, 2002  
 Page 19

**FILED UNDER SEAL**

On or about March 30, 2000, this coconspirator of IVANOV sent an e-mail message to this same FSI employee in which he threatened that he would again access the FSI computer network and cause damage to this network if FSI failed to immediately agree to his demand for an extortion payment of \$5,000. On or about the following dates, as a result of these communications, this coconspirator of defendant ALEXEI V. IVANOV caused FSI to wire a total of \$5,000 to a bank account at Alfabank in Moscow, Russia, as follows:

Date	Amount
April 5, 2000	\$1,000
April 17, 2000	\$2,000
May 2, 2000	\$2,000

#### Nara Bank

Nara Bank is a financial institution whose computer systems and headquarters were located in California, and whose deposits were insured by the Federal Deposit Insurance Corporation. Between approximately March and April 2000, IVANOV and a coconspirator gained unauthorized access into the Nara Bank computer systems and from approximately March through April stole confidential financial and account information from the bank's computer systems. Files containing several thousand bank accounts numbers and other stolen data were stored on the tech.net.ru computer systems.

Between approximately April and October 2000, IVANOV and Gorshkov prepared and sent an e-mail communication to a number of Nara Bank officials revealing that they had access to Nara Bank systems and data, and which was intended to obtain funds and work through the use of fear and threat of economic damage. They also used their unauthorized access to the Nara Bank computer system and bank accounts to further the Paypal fraud scheme, outlined below. IVANOV, Gorshkov and their conspirators used the account data and access to Nara Bank systems to accomplish, at least temporarily, actual transfers of funds from some of its customer accounts to PayPal accounts.

#### Casinovega

Casinovega is a foreign entity that offered gambling through its web site over the Internet. In March 2000 IVANOV and a conspirator obtained unauthorized access to its computer system and confidential financial data and credit card accounts stored on the system. Casinovega representatives then contacted IVANOV. After IVANOV demonstrated his access and control of the Casinovega system, Casinovega officials paid IVANOV a total of \$4000 out of fear that IVANOV would damage the Casinovega system. He also stole confidential and financial data from these systems, which he stored on the tech.net.ru computer systems.

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 20

**FILED UNDER SEAL**

Electronic Data Enterprises, Inc.

Electronic Data Enterprises, Inc. ("E-Money") located in Maryland and Virginia, was a financial transaction clearinghouse that assisted in the processing of merchant credit card and financial transactions in interstate and foreign commerce. Between approximately May and July 2000, IVANOV and a coconspirator gained unauthorized access to the computer systems of E-Money using computer systems in Russia, including those of tech.net.ru. IVANOV stole a credit card account database from E-Money and stored it on the CTS computer systems.

Additional Victims

In the year 2000, ALEXEI IVANOV, Gorshkov and their coconspirators continued their unauthorized access of computer systems in the United States from Russia, including the following. In approximately August, they obtained unauthorized access Central National Bank (CNB) in Waco, Texas and American Bank ("AmBank") in Pennsylvania, the deposits of which were insured by the Federal Deposit Insurance Corporation. Credit card and merchant account numbers were taken from the AmBank computer systems and stored on the tech.net.ru computer systems. They also compromised the computer network of the St. Clair County Intermediate School District in Michigan, using it as a proxy for several illegal purposes.

The PayPal Scheme

An additional number of other computer programs or PERL "scripts" located in Gorshkov's "kvakin" home accounts implemented a fraud scheme against the online auction company E-Bay and the online credit card payment company PayPal. Gorshkov's scripts generated thousands of e-mail addresses at web sites offering free e-mail accounts, opened corresponding accounts at PayPal with stolen credit cards, generated fraudulent or "virtual" auctions at E-Bay, and initiated payments from one PayPal account to another using the stolen credit cards.

IVANOV, Gorshkov, and their coconspirators opened hundreds of accounts at PayPal from several IP addresses, principally 216.122.89.110, which resolved to www.lightrealm.com, in Kirkland, Washington, and 133.78.216.28, registered to Musashi Technical Institute in Japan. Other IP addresses from which PayPal had been defrauded included 212.57.129.2, resolving to www.surnet.ru, located in Moscow, Russia; 140.239.225.222, registered to popstick at Harvardnet, 63.70.149.190, registered to the St. Clair County, Michigan, Intermediate School; 202.155 \* \*, IP addresses registered to an Internet Service Provider located in Jakarta, Indonesia, and others. Additionally, the accounts were opened minutes apart by an automated process. Many of the fraudulent accounts used variants of the names "Greg Stivenson" and "Murat Nasirov "

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq  
July 31, 2002  
Page 21

**FILED UNDER SEAL**

Examination of the data downloaded from the tech.net.ru computer systems, tech.net.ru and freebsd.tech.net.ru, found over 50,000 access devices that had been stolen from various online merchants and banks in the United States, including several of the victims identified above. PayPal determined that thousands of those stolen credit cards had been used at PayPal by the person or persons who had opened the accounts discussed above. While PayPal managed to block many of the transactions, it has suffered a monetary loss due to the conspirators' activities that included charge backs from the card issuing banks.

In addition, personnel from several of the systems that were identified with the transactions at PayPal – including Lightrealm and the St. Clair County Intermediate School District – determined that their computers had been hacked from IP address 195.128.157.66, registered to tech.net.ru. The intruders had taken over their systems and used them as proxies to make other connections to the Internet. As to other compromised systems, the government's examination of evidence found on the tech.net computers established that the IP addresses registered to the Musashi Technical Institute and others also belonged to systems that the defendants had compromised.

IVANOV, Gorshkov and other conspirators solicited sellers of computer parts and other goods, convincing some of these merchants to sell the parts and ship them to Kazakhstan, which is not far from Chelyabinsk. Payment was made to the merchants' PayPal accounts with stolen credit cards

#### The Invita Scheme

In June 2000, IVANOV was contacted by representatives of Invita Computer Security, Inc. ("Invita") an undercover operation conducted by the Federal Bureau of Investigation that was based in Seattle, Washington. Throughout the next several months, representatives of Invita discussed working with IVANOV, Gorshkov and tech.net.ru, the Russian company which they managed in Russia and which, they stated, conducted computer security work. IVANOV and Gorshkov agreed to travel to Seattle, Washington, to meet with Invita personnel. Prior to traveling to the United States, IVANOV and Gorshkov offered to demonstrate their hacking skills on Invita's own computers. An Invita network was set up for that purpose, and IVANOV and Gorshkov successfully hacked into it using many of the same tools they had used to hack the victims above. On November 10, 2000, IVANOV and Gorshkov flew from Russia to Seattle, Washington in order to discuss doing business with Invita.

Upon arriving in Seattle, they met with Invita officials. In an effort to again demonstrate their hacking ability, IVANOV and Gorshkov sat down at computers located in the Invita office, and logged on to outside computer systems. IVANOV and Gorshkov also discussed the illegal hacking activity they conducted from tech.net.ru in Russia. They stated that they had hacked a number of American businesses and had obtained money from some of them. They created some of their own hacking tools, and recently had to "hijack" their system in order to hack systems that

C. Thomas Furniss, Esq  
Morgan P Rueckert, Esq.  
July 31, 2002  
Page 22

**FILED UNDER SEAL**

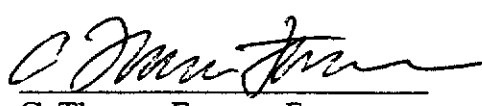
could trace them They explained that they hacked companies first, then approached them to offer security services, not telling the companies that their systems were already compromised IVANOV explained that in one instance the company paid him \$4000 because the company did not trust him and believed that he could damage them. IVANOV and Gorshkov indicated they would be willing to discuss stolen credit cards with Invita personnel, but only when they were in Russia.

At the end of the meeting IVANOV and Gorshkov were arrested.

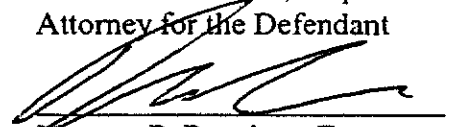
The written stipulation above is incorporated into the preceding plea agreement. It is understood, however, that the defendant and the Government reserve their right to present additional relevant offense conduct to the attention of the Court in connection with sentencing.

  
\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

  
\_\_\_\_\_  
Mark G Califano  
Shawn J. Chen  
Assistant United States Attorneys

  
\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
\_\_\_\_\_  
Mark G Califano  
Assistant United States Attorney

  
\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
\_\_\_\_\_  
Stephen C. Schroeder  
Floyd Short  
Assistant United States Attorneys

\_\_\_\_\_  
Arif Alikhan  
Assistant United States Attorney

\_\_\_\_\_  
Scott S. Christie  
Assistant United States Attorney

\_\_\_\_\_  
Mark L. Krotoski  
Assistant United States Attorney



C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
August 1, 2002  
Page 22

**UNDER SEAL**

could trace them. They explained that they hacked companies first, then approached them to offer security services, not telling the companies that their systems were already compromised. IVANOV explained that in one instance the company paid him \$4000 because the company did not trust him and believed that he could damage them. IVANOV and Gorshkov indicated they would be willing to discuss stolen credit cards with Invita personnel, but only when they were in Russia.

At the end of the meeting IVANOV and Gorshkov were arrested.

The written stipulation above is incorporated into the preceding plea agreement. It is understood, however, that the defendant and the Government reserve their right to present additional relevant offense conduct to the attention of the Court in connection with sentencing.

\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

\_\_\_\_\_  
Mark G. Califano  
Shawn J. Chen  
Assistant United States Attorneys

\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Mark G. Califano  
Assistant United States Attorney

\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Stephen C. Schroeder  
Floyd Short  
Assistant United States Attorneys

\_\_\_\_\_  
Arif Alikahn  
Assistant United States Attorney

  
\_\_\_\_\_  
Scott S. Christie  
Assistant United States Attorney

\_\_\_\_\_  
Mark L. Krotoski  
Assistant United States Attorney

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
August 1, 2002  
Page 22

**UNDER SEAL**

could trace them. They explained that they hacked companies first, then approached them to offer security services, not telling the companies that their systems were already compromised. IVANOV explained that in one instance the company paid him \$4000 because the company did not trust him and believed that he could damage them. IVANOV and Gorshkov indicated they would be willing to discuss stolen credit cards with Invita personnel, but only when they were in Russia.

At the end of the meeting IVANOV and Gorshkov were arrested.

The written stipulation above is incorporated into the preceding plea agreement. It is understood, however, that the defendant and the Government reserve their right to present additional relevant offense conduct to the attention of the Court in connection with sentencing.

---

Alexey V. Ivanov  
The Defendant

---

Mark G. Califano  
Shawn J. Chen  
Assistant United States Attorneys

---

C. Thomas Furniss, Esq.  
Attorney for the Defendant

---

Mark G. Califano  
Assistant United States Attorney

---

Morgan P. Rueckert, Esq.  
Attorney for the Defendant

---

Stephen C. Schroeder  
Floyd Short  
Assistant United States Attorneys

---

Arif Alikahn  
Assistant United States Attorney

---

Scott S. Christie  
Assistant United States Attorney

---



---

Mark E. Krotoski  
Assistant United States Attorney

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 22

UNDER S

could trace them. They explained that they hacked companies first, then approached them to security services, not telling the companies that their systems were already compromised. IVANOV explained that in one instance the company paid him \$4000 because the company did not trust him and believed that he could damage them. IVANOV and Gorshkov indicated they would be willing to discuss stolen credit cards with Invita personnel, but only when they were in Russia.

At the end of the meeting IVANOV and Gorshkov were arrested.

The written stipulation above is incorporated into the preceding plea agreement. It is understood, however, that the defendant and the Government reserve their right to present additional relevant offense conduct to the attention of the Court in connection with sentencing.

\_\_\_\_\_  
Alexey V. Ivanov  
The Defendant

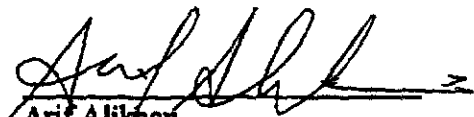
\_\_\_\_\_  
Mark G. Califano  
Shawn J. Chen  
Assistant United States Attorneys

\_\_\_\_\_  
C. Thomas Furniss, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Mark G. Califano  
Assistant United States Attorney

\_\_\_\_\_  
Morgan P. Rueckert, Esq.  
Attorney for the Defendant

\_\_\_\_\_  
Stephen C. Schroeder  
Floyd Short  
Assistant United States Attorneys

  
\_\_\_\_\_  
Arif Ali Khan  
Assistant United States Attorney

\_\_\_\_\_  
Scott S. Christie  
Assistant United States Attorney

\_\_\_\_\_  
Mark L. Krotoski  
Assistant United States Attorney

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 22

UNDER SEAL

could trace them. They explained that they hacked companies first, then approached them to offer security services, not telling the companies that their systems were already compromised. IVANOV explained that in one instance the company paid him \$4000 because the company did not trust him and believed that he could damage them. IVANOV and Gorshkov indicated they would be willing to discuss stolen credit cards with Invita personnel, but only when they were in Russia.

At the end of the meeting IVANOV and Gorshkov were arrested.

The written stipulation above is incorporated into the preceding plea agreement. It is understood, however, that the defendant and the Government reserve their right to present additional relevant offense conduct to the attention of the Court in connection with sentencing.

---

Alexey V. Ivanov  
The Defendant

---

Mark G. Califano  
Shawn J. Chen  
Assistant United States Attorneys

---

C. Thomas Furniss, Esq.  
Attorney for the Defendant

---

Mark G. Califano  
Assistant United States Attorney

---

Morgan P. Rueckert, Esq.  
Attorney for the Defendant

---

  
Stephen C. Schroeder  
Floyd Short  
Assistant United States Attorneys

---

Arif Alikahn  
Assistant United States Attorney

---

Scott S. Christie  
Assistant United States Attorney

---

Mark L. Krotoski  
Assistant United States Attorney

C. Thomas Furniss, Esq.  
Morgan P. Rueckert, Esq.  
July 31, 2002  
Page 23

**FILED UNDER SEAL**

RIDER CONCERNING RESTITUTION

The Court shall order that the defendant make restitution under 18 U.S.C. § 3663A. The order of restitution may include:

1. If the offense resulted in damage to or loss or destruction of property of a victim of the offense, the order of restitution shall require the defendant to:

A. Return the property to the owner of the property or someone designated by the owner; or

B. If return of the property is impossible, impracticable, or inadequate, pay an amount equal to:

The greater of -

(I) the value of the property on the date of the damage, loss, or destruction; or

(II) the value of the property on the date of sentencing, less the value as of the date the property is returned

2. In any case, reimburse the victim for lost income and necessary child care, transportation, and other expenses incurred during participation in the investigation or prosecution of the offense or attendance at proceedings related to the offense.

The order of restitution shall be a condition of probation or supervised release. Failure to make restitution as ordered may result in a revocation of probation, or a modification of the conditions of supervised release, or in the defendant being held in contempt under 18 U.S.C. § 3583(e). Failure to pay restitution may also result in the defendant's resentencing to any sentence which might originally have been imposed by the Court. See 18 U.S.C. § 3614. The Court may also order that the defendant give notice to any victim(s) of his offense under 18 U.S.C. § 3555. Finally, the order of restitution has the effect of a civil judgment against the defendant.

**EXHIBIT B**



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES DISTRICT COURT  
DISTRICT OF CONNECTICUT

-----\*

UNITED STATES OF AMERICA,  
Plaintiff,

vs.

ALEXEY IVANOV,  
Defendant.

3:00CR183 (AWT)  
AUGUST 2, 2002  
HARTFORD, CONNECTICUT

COPY

-----\*

BEFORE:  
HON. ALVIN W. THOMPSON, U.S.D.J.

SEALED UNTIL FURTHER ORDER OF THE COURT

APPEARANCES:

FOR THE PLAINTIFF:

OFFICE OF THE UNITED STATES ATTORNEY  
BY: MARK CALIFANO, ESQUIRE  
Assistant United States Attorney  
915 Lafayette Boulevard  
Bridgeport, Connecticut 06604

FOR THE DEFENDANT:

FURNISS & QUINN  
BY: THOMAS FURNISS, ESQUIRE  
248 Hudson Street  
Hartford, Connecticut 06106

SHIPMAN & GOODWIN  
BY: MORGAN P. RUECKERT, ESQUIRE  
One Landmark Square  
Stamford, Connecticut 06901-2676

.. Corinna F. Thompson, RPR  
Official Court Reporter

1 to hear them from Mr. Ivanov. The first one, the extortion,  
2 is the probably the toughest one we have psychologically,  
3 if you will.

4 So if we can go to the western district of  
5 Washington, which is a general conspiracy, and we've talked  
6 with Mr. Califano at some length, Mr. Ivanov will try to  
7 explain in a general way what the conspiracy was, the types  
8 of coconspirators, the objects of the conspiracy, Alexey,  
9 because there were more than one, some of the methods.  
10 Okay? Some of the victims. Shall we proceed that way?  
11 Okay. Go ahead.

12 THE DEFENDANT: Well, what happened is me and  
13 Mr. Gorshkov, defendant in Seattle case, we were agreed to  
14 do some kind of fraud, scheme, to obtain money, to obtain  
15 eventually money by defrauding victims on auctions, in  
16 addition defrauding online shop.

17 MR. FURNISS: Auctions like EBay?

18 THE DEFENDANT: EBay, yes. Online shops like  
19 Amazon and Barnes & Noble. We developed scripts which  
20 significantly automated process more.

21 MR. CALIFANO: Mr. Ivanov, the process you're  
22 talking about is getting goods by fraud?

23 THE DEFENDANT: Yes.

24 MR. CALIFANO: And what did you -- I'm sorry.

25 THE DEFENDANT: There was also a number of



1 people who were working in this scheme. For example--

2 MR. FURNISS: "Scheme" are you saying?

3 THE DEFENDANT: Scheme.

4 MR. FURNISS: Scheme.

5 THE DEFENDANT: For example, goods were  
6 delivered to people in different countries, Kazakhstan,  
7 because nobody wants to send goods to Russia. They were  
8 obtained either by me or Vasily Gorshkov from these drops.

9 We also had -- then it was myself. We also  
10 had a number of people who were working on these programs,  
11 scripts. I was involved in obtaining credit card  
12 information which would use as payment for goods.

13 MR. CALIFANO: May I inquire, Your Honor?

14 THE COURT: You may.

15 MR. CALIFANO: Mr. Ivanov, were these -- whose  
16 credit cards were these? .

17 THE DEFENDANT: Well, not ours definitely.

18 MR. CALIFANO: And was one of the places that  
19 you used, that you obtained credit cards located in the  
20 state of Washington, at Lightrealm?

21 THE DEFENDANT: Yes.

22 MR. CALIFANO: Was one of these known as Plus  
23 Cellular?

24 THE DEFENDANT: Well, it wasn't actually  
25 Lightrealm's credit card. Lightrealm is a company who

1 provides services to another company. They provide hosting.  
2 And credit card from company which was just mentioned by  
3 Mr. Califano, Plus Cellular, it was a customer of  
4 Lightrealm's. It wasn't the Lightrealm's credit card but  
5 it was customers of customers of Lightrealm.

6 MR. CALIFANO: And what would you do once you  
7 got those credit cards?

8 THE DEFENDANT: We used them in our scripts to  
9 defraud and put them in database and this database was used  
10 by scripts to defraud.

11 MR. CALIFANO: I think, Your Honor, that that  
12 would be enough to satisfy the conspiracy.

13 THE COURT: And then we have Count 4.

14 MR. CALIFANO: Yes, Your Honor.

15 THE COURT: Do you want to cover both  
16 together?

17 MR. CALIFANO: I can cover both together. That  
18 may be easier. As I understand it, Count 4 deals with the  
19 unauthorized access and intentional destruction of data at  
20 Speakeasy.

21 THE COURT: Yes.

22 MR. FURNISS: Alexey, tell His Honor what you  
23 did with Speakeasy and which of your coconspirators and how  
24 you did it.

25 THE DEFENDANT: Well, me and part of a

1 different conspiracy. I was involved in different--

2 MR. FURNISS: Different people?

3 THE DEFENDANT: Well, at the same time but it  
4 was different groups of people so it was a different  
5 conspiracy. This count alleged the different conspiracy.

6 So me and another coconspirator, his name  
7 Vladimir Kozhevnikov, K-o-z-h-e-v-n-i-k-o-v, we were get  
8 access unauthorized to Speakeasy, this company in  
9 Washington state.

10 MR. FURNISS: It's an ISP?

11 THE DEFENDANT: Yes. It's actually an ISP  
12 similar to Lightrealm. It provides hosting services to  
13 their customers.

14 Eventually we obtain unauthorized access  
15 to their credit card and we were involved in communications  
16 with representatives from this company and eventually some  
17 kind of destruction of the data took place and they --

18 MR. CALIFANO: May I inquire, Your Honor?

19 THE COURT: You may.

20 MR. CALIFANO: Mr. Ivanov, in getting access to  
21 this Speakeasy computer system, did you have authorization  
22 to get access?

23 THE DEFENDANT: No. I said it wasn't  
24 authorized.

25 MR. FURNISS: He said unauthorized.

1 MR. CALIFANO: Where were you operating from  
2 when you got access to Speakeasy? What computer system  
3 were you using?

4 THE DEFENDANT: Well, originally I was in  
5 Russia.

6 MR. CALIFANO: Was it the tech.net.ru computer  
7 system?

8 THE DEFENDANT: Tech.net.ru didn't exist at  
9 this time. It was a computer which was later was used at  
10 tech.net.ru.

11 MR. CALIFANO: Did you continue to store some  
12 Speakeasy data on the tech.net.ru computer?

13 THE DEFENDANT: Yes.

14 MR. CALIFANO: With respect to your  
15 communications with Speakeasy, in communicating with  
16 Speakeasy did you indicate to them that you actually had  
17 access to their computers?

18 THE DEFENDANT: Yes.

19 MR. CALIFANO: Did you also indicate to them  
20 that you had obtained data from their computers?

21 THE DEFENDANT: Yes.

22 MR. CALIFANO: And did you -- and did they  
23 agree as a result of that, in part you indicating to them,  
24 did they agree to pay you?

25 THE DEFENDANT: Yes.

1 MR. CALIFANO: And did they pay you?

2 THE DEFENDANT: No.

3 MR. CALIFANO: And when they didn't pay you,  
4 what did you do?

5 THE DEFENDANT: Well, it's like I said, some  
6 kind of destruction took place.

7 MR. CALIFANO: What did you do?

8 THE DEFENDANT: Well, me and my coconspirator,  
9 Vladimir Kozhevnikov, we were agreed to destroy data on  
10 their computer.

11 MR. CALIFANO: And did you, in fact, do that?

12 THE DEFENDANT: Yes.

13 MR. CALIFANO: Your Honor, I want to ask one  
14 question.

15 Mr. Ivanov, did you review the Stipulation  
16 of Offense Conduct that's attached to the end of the plea  
17 agreement?

18 THE DEFENDANT: Yes.

19 MR. CALIFANO: And do you believe it's an  
20 accurate statement of the events that occurred?

21 THE DEFENDANT: Yes.

22 MR. CALIFANO: Okay. By the way, with respect  
23 not only to Speakeasy but to the other things we talked  
24 about with respect to OIB--

25 THE DEFENDANT: Yes.

1 MR. CALIFANO: -- and to the extent that you  
2 thought it needed to be changed, did you communicate that  
3 to your attorneys and was that changed throughout? In other  
4 words, when you had changes to make, did your attorney --  
5 were those changes made before you signed it?

6 THE DEFENDANT: I don't think I had any  
7 significant changes about OIB.

8 MR. CALIFANO: But to the extent that you had  
9 changes in any of the offense conduct, you asked that they  
10 be made and they were made, at least to your satisfaction,  
11 before you signed it in order to make it accurate; is that  
12 correct?

13 THE DEFENDANT: Yes.

14 MR. CALIFANO: Your Honor.

15 THE COURT: Let me just -- are you ready to  
16 summarize the government's evidence at this time, Mr.  
17 Califano?

18 MR. CALIFANO: Yes.

19 THE COURT: You understand how this works. I'm  
20 going to ask you to listen carefully and if there is  
21 anything with which you disagree, I want you to tell me.

22 THE DEFENDANT: All right.

23 THE COURT: Mr. Califano.

24 MR. CALIFANO: Mr. Ivanov, Mr. Gorshkov and  
25 other persons conspired to conduct a number of things,

1 including access to computers without authorization and  
2 steal credit cards. We would present evidence that as part  
3 of that conspiracy, Mr. Ivanov accessed computers in a  
4 number of different Internet service providers, including  
5 an Internet service known as Lightrealm, including an  
6 Internet service provider VPM and a third known as CTS,  
7 which is located in California. Lightrealm is located in  
8 Seattle, Washington --

9 MR. FURNISS: Kirkland.

10 MR. CALIFANO: Excuse me. Kirkland,  
11 Washington. And VPM is located in the eastern district of  
12 California.

13 In the course of those intrusions and in  
14 furtherance of the conspiracy in particular, the government  
15 would present evidence that Mr. Ivanov obtained credit  
16 cards from the Plus Cellular database on the Lightrealm  
17 servers and Plus Cellular -- we would show from testimony  
18 from Plus Cellular that he conducted transactions on those  
19 computer systems of Lightrealm that resulted in credit card  
20 data of its customers being put on that system.

21 The evidence we would present would show  
22 that Mr. Ivanov took credit cards from that as well as a  
23 number of other Internet-based companies around the country  
24 and used them along with Mr. Gorshkov to do a number of  
25 things in an entity they called tech.net.ru.

1 Tech.net.ru was formed with Mr. Gorshkov.  
2 The evidence would show that there was a set of servers  
3 operated by Gorshkov and Mr. Ivanov which were based in  
4 Chelyabinsk, Russia. We would produce data he received,  
5 along with coconspirators, set of confiscated computer  
6 scripts also known as programs. Those programs were  
7 designed to take stolen "credit card information to open  
8 credit card accounts or accounts on Internet payment  
9 systems known as PayPals and to use those systems to  
10 generate funds in the PayPal accounts and purchase  
11 merchandise, including computers.

12 In addition, the scripts were also  
13 designed to open up accounts on EBay, which is a large  
14 auction-based communication -- payment system on the  
15 Internet -- it's operated in California -- in order to  
16 conduct phony auctions and also to induce people to bid on  
17 auctions that they initiated. That was in order to  
18 generate yet additional funds out of those auctions. That  
19 part of the system was not completely executed because they  
20 were arrested in Seattle when that occurred.

21 Finally, we would present evidence that  
22 Mr. Ivanov, Mr. Gorshkov communicated with a group of  
23 individuals they believed to be a security company in  
24 Seattle, Washington known as Invita, and in the course of  
25 that communication, Mr. Ivanov and Mr. Gorshkov agreed to



1 meet and to discuss doing further business, including the  
2 solicitation of security from various Internet companies  
3 after they already gained unauthorized access to those  
4 companies.

5 Those discussions occurred after Mr.  
6 Gorshkov and Mr. Ivanov had traveled to Seattle and then  
7 met with the undercover members of the Invita group, which  
8 were actually undercover F.B.I. agents and other  
9 individuals.

10 THE COURT: Thank you.

11 Mr. Ivanov, do you agree with the  
12 prosecutor's summary of what you did?

13 THE DEFENDANT: Well, just a little  
14 clarification. My agreement with Mr. Gorshkov was before  
15 it took place and I don't believe I can be conspirators  
16 with the government agents.

17 MR. CALIFANO: Your Honor, I think that -- if I  
18 may ask a question?

19 THE COURT: You may.

20 MR. CALIFANO: Mr. Ivanov, if the agreement  
21 began before, did it continue through the time that you  
22 were working?

23 THE DEFENDANT: Yes.

24 THE COURT: Anything else that you wanted to  
25 clarify?

...

1 THE DEFENDANT: No.

2 THE COURT: I think we will now go to the  
3 district of New Jersey.

4 THE DEFENDANT: Well, what happened is at  
5 first, like I told you, this is a little bit -- a little  
6 just short stories of mine so I can talk.

7 I am originally from Chelyabinsk and I was  
8 invited [REDACTED] by different group of people which I  
9 connected to Vladimir Kozhevnikov. The purpose of this  
10 visit was to do something illegal, to break into companies,  
11 obtain credit cards and make some kind of frauds to obtain  
12 money.

13 During at the time [REDACTED] FSI  
14 company was and I hacked and I got access to this company.  
15 Password files and credit card files was downloaded. All  
16 people who were involved in this had possession of this  
17 information. It was, as far as I remember, it was also  
18 understanding to send something to this company about  
19 asking them for permission for security services similar to  
20 OIB.

21 At the time [REDACTED] in  
22 early March and by the time--

23 MR. FURNISS: Of 2000?

24 THE DEFENDANT: 2000. Yes. [REDACTED] two  
25 weeks later in the middle of March and later some kind of

1 district of Washington, we'll go back and we'll pick up --  
2 we've done the district of Connecticut. We will start with  
3 the western district of Washington, do the remaining four  
4 cases and just so people can follow along, the clerk is  
5 going to read the docket number from Washington or the  
6 other jurisdiction and the number that's been assigned here  
7 in the district of Connecticut also.

8 MR. FURNISS: I'm may be extra work and she's  
9 going to make me pay.

10 THE CLERK: United States District Court,  
11 Western District of Washington at Seattle. United States  
12 of America versus Alexey Vladimirovich Ivanov, a/k/a Alexey  
13 Ivanov, a/k/a Subbsta. Number CR00-550C, Chief Judge  
14 Coughenour. Number here assigned in Connecticut is  
15 3:02CR216(AWT). Superseding indictment.

16 Count 1: The defendant is in violation of  
17 Title 18 United States Code Section 371.

18 To Count 1, how do you plead?

19 THE DEFENDANT: Guilty.

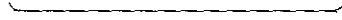
20 THE CLERK: Guilty, Your Honor.

21 Count 4: The defendant is in violation of  
22 Title 18 United States Code Sections 1030(a)(5)(A) and  
23 (c)(3)(A) and Section 2.

24 To Count 4, how do you plead?

25 THE DEFENDANT: Guilty.

**EXHIBIT C1**



1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

IN THE UNITED STATES DISTRICT COURT FOR  
THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	Case No. CR00-550C
Plaintiff,	)	
	)	Seattle, Washington
v.	)	October 4, 2001
	)	
VASILIIY VYACHESLAVOVICH	)	VOLUME 10
GORSHKOV, a/k/a VASSILI GORCHKOV,	)	
a/k/a "kvakin,"	)	
	)	
Defendant.	)	
	)	
	)	

TRANSCRIPT OF PROCEEDINGS  
BEFORE THE HONORABLE JOHN C. COUGHENOUR  
UNITED STATES DISTRICT JUDGE

For the Plaintiff:	Stephen C. Schroeder
	Floyd G. Short
	Assistant U.S. Attorneys
	601 Union Street, Suite 5100
	Seattle, Washington 98101-3903
For the Defendant:	Kenneth E. Kanev
	Attorney at Law
	1001 Fourth Avenue Plaza, Suite 2120
	Seattle, Washington 98154-1109
	Robert S. Apgood
	Attorney at Law
	500 Union Street, Suite 510
	Seattle, Washington 98101

Joseph F. Roth  
Official Court Reporter  
600 U.S. Courthouse  
Seattle, Washington 98104  
(206) 553-1899

Proceedings recorded by computer-aided stenography.

1 Q What was your response when Alexey said, well, you know,  
2 tell them that we're big and we've got 20 people working and --  
3 you ended up telling that to the Invita person?

4 A Yes.

5 Q What was your response, though, when he asked you to do  
6 that?

7 A My response was I was angry at him, that why should I tell  
8 to some people -- and if these people want to do business with  
9 me, why should I tell them what is not true? It's not a good  
10 idea to begin business with.

11 And I was mad at him that he called me partner. We are not  
12 partners and we are not going to be partners. But he persuade  
13 me that, look, if we are going to do this business with this  
14 guy, I'm going to manage the security part of your business, and  
15 we can hire 20 people easy.

16 And finally I agree with him, that if we can work with this  
17 guys in the United States -- and everybody knows that guys from  
18 the United States got some money -- we can handle it. We can  
19 hire all these people.

20 MR. KANEV: Madam Clerk, could you hand the witness  
21 Exhibit 3a, please.

22 Q 3a is the transcript of the phone conversation that we  
23 listened to you. I'm going to ask you not what's in the  
24 transcript, but you can use the transcript to refresh your  
25 recollection regarding the phone conversation. Pages 5 through

1 systems, roughly what time period are you talking about, what  
2 month or months?

3 A It's late September, probably it's October, probably it's  
4 October, October.

5 Q Let me drop back a little to the summer and also into  
6 September. This is -- we've heard evidence of a second server,  
7 the freebsd server, at your firm. When did that server come  
8 into existence and what was its purpose?

9 A The purpose of freebsd server was to -- to pick up -- one of  
10 the purpose was to pick up technical server. Second was because  
11 of the difference between this operational systems, it's a UNIX  
12 operational system but there is difference between UNIX and  
13 freebsd.

14 And my guys, who was working on the project, like on Linux  
15 operational system, they say that probably it's not a bad idea  
16 to check it on both -- both operational systems, and probably  
17 even more than two, just to check whether it's working properly  
18 on Linux, freebsd and possibly on all other UNIX operational  
19 system.

20 Q And as far as the personnel at your firm, did it change in  
21 any way from, I guess -- well, during the summer months, from  
22 May to September?

23 A From May to September -- in the beginning of May, maybe it's  
24 into -- I fired this Andrei Popov and Uri. Later I hired  
25 another guy -- guys. And at the middle of summer, middle of

1 July, I fired Karpych.

2 Q What happened between Karpych and you that led to his  
3 firing?

4 A At that time I received complaint from my provider, from my  
5 internet provider, when I was paying them, that they received  
6 complaint that there was scanning that was originated from my  
7 system, and I asked -- I asked Karpych to handle the situation,  
8 to figure out what happened and how it happened.

9 Q Why did you ask Karpych to handle it?

10 A Because he was system administrator.

11 Q And did he handle the situation?

12 A He -- he react the way that it's not a problem at all, and  
13 meaning it's not a problem to handle situation, but the scanning  
14 is not a problem at all.

15 Q And how did you respond to that?

16 A I was angry with him, because I'm giving him orders and he  
17 don't do it.

18 Q And as a result what happened?

19 A As a result he got fired.

20 Q Did you do any investigation on your own on this reported  
21 complaint about scanning coming from your internet provider?

22 A I didn't do it on my own. I asked Deniz to check, was it  
23 all right, was everything fine.

24 Q Now, Deniz, did -- who took over, if there was someone to  
25 take over from Karpych, as system administrator?



1 A It was Deniz, but it wasn't like system administrator.  
2 He -- first of all, when Karpych get fired, I consult with Deniz  
3 whether we need another administrator or Deniz can handle the  
4 situation, and Deniz persuade me that Karpych installed  
5 everything, and once system is installed, possibly nothing --  
6 there's nothing to do with this. It must work properly all the  
7 time.

8 Q Okay. And were there any other personnel changes during the  
9 summer, up until you were devoting some time to security  
10 research?

11 A At the end of the summer, but it would be September. When I  
12 was researching all the security stuff, I found out that a lot  
13 of machines on the internet, like on this Alta Vista and all  
14 this stuff, percentage of machines on internet, and I found out  
15 a big amount of machines is NT and Windows NT. So I hired Maxim  
16 Semenov.

17 Q Okay. And anyone else?

18 A No.

19 Q Okay. Roughly, then, September, October, how many people  
20 were working at your firm?

21 A It was six people.

22 Q And at that time -- and I think you left it where Invita had  
23 asked for passport information, according to Ivanov -- what was  
24 your view as far as Invita's business was concerned? Did you  
25 understand that they were a legitimate or an illegitimate

1 business in Seattle?

2 A I didn't even question it, because for me it was absolutely  
3 legitimate guys. I didn't even think about it.

4 Q Was there anything illegal suggested to you in the one and  
5 only phone conversation?

6 A No, no.

7 Q Was there anything that Ivanov said to you that raised any  
8 questions in your mind? '

9 A No.

10 Q When did you find out that a trip to Seattle would be  
11 worthwhile and that Invita was serious about talking to Ivanov  
12 and you in Seattle?

13 A When?

14 Q Yes.

15 A It was some day in August, some day in August.

16 Q Okay. And did it take awhile then before you were ready to  
17 actually leave? And, if so, what was the reason that there was  
18 that delay, as you understood it?

19 A Alexey complained to me that these guys a little slow in  
20 response. He said there is big delays between his e-mail and  
21 us, and he couldn't handle it. And for me it was I didn't -- I  
22 wasn't in a hurry, so I could wait.

23 Q And what about a test hack that Ivanov was given to do by  
24 Invita? Did you ever learn about that?

25 A At the end of October; maybe even beginning of November,

1 right before flight, one, maybe two weeks, he says that Invita  
2 provided finally this test -- test computer, and he did hack his  
3 computer.

4 Q And did you think there was anything unusual about that?

5 A It was unusual from my conversation when I was asking for  
6 this -- for some specific task, and until this hack or this  
7 test, it was several months.

8 Q Just the delay you found unusual?

9 A Just delay, yes.

10 Q And what was your understanding as far as whether that hack  
11 was with permission?

12 A For me it was apparent that it was with permission.

13 Q Now, before you left Chelyabinsk did you learn anything more  
14 about Invita from Mr. Ivanov?

15 A Before I left Chelyabinsk, no, nothing, not about -- no.

16 Q Okay. And the trip to Seattle, you spent 30 hours getting  
17 from Chelyabinsk to Moscow to Seattle, correct, or thereabouts?

18 A Even more, even more, about 34, 35.

19 Q And during that trip did the topic of Invita and this  
20 business meeting that he had arranged, did it come up?

21 A Yes, of course we talk about it.

22 Q And could you tell the jury, as best you recall, in sequence  
23 what all was discussed?

24 A In the plane, in the plane -- in the plane from Moscow to  
25 Seattle there was a big talk, and I was very upset about this

1 talk. Alexey explained to me, he said basically --

2 MR. SCHROEDER: I'm going to object, Your Honor. I  
3 believe this is all hearsay, Alexey's side of the conversation.  
4 He's not here to be cross-examined.

5 MR. KANEV: There are legal issues. Maybe --

6 THE COURT: All right. Why don't you step upstairs,  
7 folks, and you'll be up there at least 15 minutes.

8 (Jury retires to the jury room.)

9 MR. KANEV: Your Honor, there are a number of  
10 discussions that I would propose to go into with the witness as  
11 far as what Ivanov said to him prior to the meeting at Invita.  
12 Our argument is that these are not -- this is not hearsay, that  
13 it would qualify under 801(d)(2)(e), which is admission by a  
14 party opponent, and it's the co-conspirator in furtherance of  
15 the conspiracy statement. The rule does provide for admission  
16 if it's a, quote, party opponent.

17 I have not found any definitive case law out of the Ninth  
18 Circuit on whether in the context of where you have two parties,  
19 both named alleged co-conspirators, Ivanov and Gorshkov in this  
20 case, whether one of those parties, if the defenses are  
21 antagonistic, as they clearly are here, whether the second party  
22 defendant then becomes party opponent under the language of  
23 801(d)(2)(e).

24 I would argue that there's no reason why that exception  
25 should not apply, and it would take it out of being hearsay,

1 because 801 talks in terms --

2 THE COURT: Come up with another argument, Mr. Kanev.  
3 You're not getting very far with that one.

4 MR. KANEV: Well, the second argument is it goes to --  
5 it's circumstantial evidence explaining what the listener of the  
6 conversation did, in this case not only what he did, but what he  
7 said, at the Invita meeting. It's not introduced for the truth  
8 of it, and only then as --

9 THE COURT: What is he going to testify that Ivanov  
10 said?

11 MR. KANEV: Well, Ivanov said a number of things to  
12 him, and essentially convinced him that he had to play the role  
13 of hacker, meaning criminal hacker, in the Invita meeting if he  
14 wanted -- if he, Mr. Gorshkov, wanted to get legitimate web  
15 site, web design business out of the thing.

16 And the testimony will be that Mr. Gorshkov wasn't -- well,  
17 he was upset, as I think has already come out, and that there  
18 were further discussions, and then Ivanov filled him in on a  
19 number of things, including CTS, Lightrealm, which was all news  
20 to my client, which then came out at the discussion with the  
21 Invita people.

22 So on the second theory of admissibility --

23 THE COURT: That's a pretty tough sell, Mr. Kanev.  
24 Well, I'm going to let you make the argument, and I'm going to  
25 admit it for state of mind purposes.

1 MR. SCHROEDER: You're going to admit it, Your Honor?

2 THE COURT: Yes.

3 MR. KANEV: And that is the argument. Does Your Honor  
4 want to hear further on that?

5 THE COURT: No.

6 MR. SCHROEDER: Well, of course, we don't want it  
7 admitted, but Your Honor has ruled. But will the jury be  
8 instructed that --

9 THE COURT: It comes in only for state of mind  
10 purposes.

11 MR. SCHROEDER: Cannot be considered for the truth of  
12 the matter.

13 THE COURT: That is asserted in the contents of the  
14 statement.

15 MR. SCHROEDER: Well, the problem is it's a terrible  
16 bootstrap, because they're going to argue that he -- that the  
17 information that he relates to this undercover was received from  
18 Ivanov, which, frankly, is -- and that he then entered into the  
19 role, which is frankly an admission of joining a conspiracy, and  
20 yet they want to bootstrap it in a way they want their cake and  
21 eat it, too, and I think it's a really an unfair way for this  
22 evidence to come in.

23 THE COURT: I'm going to let it in. All right. We'll  
24 take 15 minutes. Before we go, have you given thought to what  
25 we talked about before lunch?

1 earlier version?

2 A Yes.

3 Q Thank you. And the last --

4 A The last one is a marriage agency.

5 Q A marriage agency?

6 A Yes.

7 Q Was your business -- your firm involved in working up the  
8 concept of a web site for that type of agency?

9 A Yes, but it wasn't ordered from -- from some company in  
10 Chelyabinsk that wants to make a set, it was --

11 Q How was it that you started working on it if you didn't  
12 actually have an order for it?

13 A I was -- in the summer of 2000 I was looking for project to  
14 develop, and I was looking again through internet sites, it's  
15 got a lot of customers, so whatever, and I was finding the sites  
16 by marriage agents, shops, job seekers, search -- search  
17 engines.

18 MR. KANEV: I'd move the admission of A-6 through -9

19 MR. SCHROEDER: No objection.

20 THE COURT: They'll be admitted.

21 (Defense Exs. Nos. A-6 through A-9 admitted.)

22 Q (By Mr. Kanev) Now, Mr. Gorshkov, back to the trip from  
23 Chelyabinsk to Seattle, I think you were at the point where  
24 there were discussions between you and Mr. Ivanov, is that  
25 correct?

1 A Yes.

2 Q What was discussed between you two on your flight to  
3 Seattle?

4 MR. SCHROEDER: Your Honor, this was the point I  
5 objected, and Your Honor indicated there would be a limiting  
6 instruction.

7 THE COURT: Yes. Ladies and gentlemen, Mr. Ivanov, of  
8 course, is not here to testify and is not subject to  
9 cross-examination. His statements are not being admitted for  
10 the truth of the contents of the statement, but only to assist  
11 you in evaluating the defendant's state of mind. Okay?

12 MR. KANEV: Thank you.

13 Q (By Mr. Kanev) Could you in sequence, if you can, tell us  
14 what was discussed, what did he say and what was your response?

15 A I was told that we supposed to be -- to get this job, to get  
16 this contract to this business partnership, these guys wants  
17 hackers on their jobs, the guys who already did a lot of the  
18 stuff they supposed to fight with. They work -- they want some  
19 guys who got experience, who knows -- who has knowledge how to  
20 hack, how to penetrate, how to, how to -- who know -- who got  
21 knowledge about systems, who know how to hack, who knows how to  
22 protect and how to hack, who got experience.

23 Q And when you're using the term "hack" -- and this is --  
24 that's the word in Russian, I take it, that Ivanov used in  
25 telling you this? ``



1 A Yes, but it was different than this.

2 Q But when he used the word "hack," what did you understand  
3 him to mean, that these guys, the Invita guys, wanted hackers?

4 A I understood that these guy want hackers who -- who did it  
5 before, and that means that -- not just knowledge about how to  
6 do it, not just knowledge -- not just knowledge of the systems,  
7 not just knowledge of the security of the system, but who got  
8 advantage of the system without permission of the owners of the  
9 company.

10 Q And how did you respond to that?

11 A I was upset. I was angry. I was -- I don't know. It  
12 was -- we were already on this plane, and we couldn't  
13 develop this -- I can't talk to these guys before about this.  
14 If I did get this information before, probably I would try to  
15 talk to these guys to get from this -- from another site, not  
16 just from Alexey, this information.

17 Q I'm sorry, you would try to get from --

18 A To get -- to talk to Invita guys to get this information,  
19 how -- what do they need, and why they look for us at this  
20 point.

21 Q Why would you want to, in that situation, have spoken to the  
22 Invita people, rather than Ivanov?

23 A Because I would try to get information from them that we're  
24 not engaged in anything illegal, that these guys got legitimate  
25 business and they want to develop this business with Russian,

1 Russian guys, because Russian programmers and people who knows  
2 the security, they just easy to find, and less to pay.

3 Q How long did you talk to Ivanov about this in terms of  
4 minutes or hours?

5 A Probably it was half of our flight to Seattle.

6 Q And was this all at one time, or were there numerous  
7 conversations?

8 A It was one conversation's, it was -- sometimes just end to  
9 nothing, and later, 20 minutes, half an hour, we begin to start  
10 to talk again about the same.

11 Q Did he tell you anything else, as far as what he had done,  
12 activities in the past?

13 MR. SCHROEDER: Your Honor, at this point I don't see  
14 how the details of exploits --

15 THE COURT: I'm going to sustain that objection.

16 Q (By Mr. Kanev) Was there any other conversation  
17 regarding -- oh, from Ivanov, regarding what you should do, or  
18 what you should say when you met with the Invita people?

19 A Basically Ivanov persuaded me that I should act like -- like  
20 I got a lot of experiences and stuff, like I know how to do it,  
21 I've done it before, and I can do it at any time. And he  
22 persuaded me. He told me that it's normal, everybody do it,  
23 and it's okay. I got the job at Lightrealm this way. I got the  
24 job at CTS this way. And --

25 MR. SCHROEDER: Objection, Your Honor. The details, I

1 don't --

2 THE COURT: He's answered the question. Ask another  
3 question.

4 Q (By Mr. Kanev) We've learned he's 19. And you were 25 at  
5 the time?

6 A Yes.

7 Q How was it that he was able to persuade you?

8 A Basically it was my ideas that he going to manage this part  
9 of business with this Invita guys at the end if we got this  
10 contract, and I can get -- and I can develop my -- my major  
11 idea, my idea of this international joint venture, where jobs  
12 and the contracts in the United States and people in Russia.

13 Q And when you arrived in Seattle, were you met by the Invita  
14 people?

15 A Yes.

16 Q And we heard testimony as far as travel from the airport up  
17 to the Invita office. There was conversation in the car, is  
18 that correct?

19 A Yes.

20 Q And do you recall what was discussed in the car?

21 A Yes, I do.

22 Q And did you at times in the car and also at the meeting act  
23 as interpreter for Ivanov?

24 A Yes, I had to do it.

25 Q And why was that? ..

1 indicates a time of roughly 4:56, what does the log and his  
2 movement indicate to you? The video screen, of course, says  
3 five o'clock. But what does that indicate to you, if anything?

4 A He runs this SuperScan program. And, by the way, when we  
5 were at meeting, sometimes when -- I asked him what are you  
6 doing, and he said that this guy wanted me to check -- to check  
7 the network again.

8 Q To check what, sir?

9 A Network, network, this test computer.

10 Q Now, during the course of the Invita meeting you said a  
11 number of things. And were most of the things that you said  
12 true or not true?

13 A Basically everything what I was saying, not everything, but  
14 most of the -- part of it, it wasn't true.

15 Q And why were you saying things that were not true in the  
16 Invita undercover meeting?

17 A The major reason because I was stupid to agree with Alexey  
18 to play this role of hacker.

19 Q Is there any other reason?

20 A And I wanted to get this job for my web development to  
21 get -- to develop this partnership with guys I don't really  
22 know.

23 Q And the web development job that you wanted to get, was  
24 that, in your mind, a legal job or an illegal job?

25 A Of course it's legal. "

1 Q Why do you say, "of course"?

2 A Because I didn't do illegal.

3 Q Your web design was legal activity?

4 A Yes.

5 Q At some point in the conversation there was mention of  
6 Microsoft software being sold in Moscow, I think.

7 A Not only Moscow, in Chelyabinsk, everywhere.

8 Q And I think you indicated that they have difficulty broke --  
9 to broke the sale of pirated software, is that what you were  
10 saying?

11 A Yes.

12 Q Did you use the word "broke"?

13 A Yes.

14 Q What did you mean that word to mean in that context?

15 A In that context I meant to stop, to prevent.

16 Q To prevent --

17 A Yes.

18 Q -- the sale of pirated software?

19 A Yes.

20 Q Now, you scanned the local network, is that correct, for  
21 Invita when you got there?

22 A It can be called scanned.

23 Q And did you believe that you had permission from Invita to  
24 do what you were doing?

25 A That's what I thought at that moment.

1 Q And was there a time that you asked someone with Invita,  
2 perhaps Agent Mallon, the woman FBI agent who we have heard  
3 from, for permission to do more than just the local area?

4 A I asked them whether I scanned, because they ask me to do --  
5 because in the car and in this room they're saying that they  
6 made it more secure and you probably will get troubles to  
7 penetrate into our system.

8 And I scanned the system and I could see that it's unsecure.  
9 And so I ask her whether I can get access to -- to computers,  
10 not just get information about computers, as it were, but get  
11 access to computers.

12 Q Okay. And was the access granted?

13 A No.

14 Q There was discussion, and I think you mentioned, they asked  
15 you -- and Mr. Pace was pressing, have you ever hacked. Give us  
16 an example of whether you've hacked. Were you able to get an  
17 example to Mr. Pace?

18 A Basically I was trying to bring something, and I did  
19 remember one example of Verio stuff.

20 Q Verio stuff?

21 A Yes.

22 Q What example do you remember of Verio stuff that you were  
23 talking about?

24 A Because I couldn't from my experience pick up any hack, so I  
25 came up with this Verio stuff, which difficult to call hack,

1 because it was an open directory, they store all information of  
2 full users.

3 Q So your conversation about a Webcom.com hack, can you  
4 explain to the jury what you meant in that meeting?

5 A I was trying to -- to give these guys -- I was playing this  
6 role of this hacker, experienced hacker, and because this guy  
7 were pushing show -- was always doing show us something, show us  
8 something, but I couldn't come up with any example, but -- with  
9 examples that -- not even hacked, but I called hacked, and I  
10 didn't -- I didn't want to further elaborate this explanation,  
11 because, in my mind, if they -- if they at that time would find  
12 out what was that, they would never call this hack.

13 Q And what was it that you were calling a hack that you were  
14 telling them about regarding Webcom.com?

15 A It was in the Verio system, in the open area, in the gmp  
16 directory, was stored information about accounts of the people  
17 who open accounts in this -- in this company.

18 Q And was it -- was there testimony in the trial about this  
19 hole, I guess?

20 A Yes.

21 Q And was that from the Verio person --

22 A Yes.

23 Q -- the other day? Did you ever tell anyone at your firm  
24 about the hole in Verio when you found it, or at any time after  
25 you found it?

1 A I did tell it to -- to Alexey, but it was before firm, it  
2 was before firm appeared.

3 Q And so what did you tell Alexey before the firm? Could you  
4 put a date on it, or an approximate date?

5 A It was fall of 1999, when I first met Alexey.

6 Q Okay. And what was the discussion that you told Alexey  
7 about?

8 A We -- we discussed that I wanted to open a company that web  
9 design, web -- web development company, and I did tell him that  
10 I doing research and, by accident, what I found. I didn't show  
11 him what I found. I just tell him that I found that -- a GMP  
12 directory at Verio that says store and open -- open password,  
13 open information of the people who open accounts in this  
14 company.

15 Q There was conversation about credit cards at the Invita  
16 meeting. Do you recall that?

17 A It was several times. It's not very much.

18 Q Okay. And you said something that you would not talk about  
19 credit cards in America or in Seattle. Do you recall that being  
20 discussed in the meeting?

21 A Yes.

22 Q Can you tell the jury what that context was and what you  
23 were saying?

24 A I don't remember exactly what -- when it was first time.  
25 First time, when we begin to discuss all this stuff, I was



1 surprised that they go somewhere not in the direction that I  
2 expect these guys to go, because I didn't want to -- I really  
3 didn't want to discuss and go that far. I didn't -- I wasn't  
4 happy with my role of hacker, or some guy who knows a lot, and I  
5 really don't know nothing about this stuff.

6 And I was trying to play on this crowd. And when they asked  
7 about -- about credit cards -- first time they ask about credit  
8 cards, I was thinking maybe they trying to check me, maybe they  
9 trying to -- to -- to check me, whether they can do business  
10 with me or not. Whether if we get to do this development and  
11 security job, whether at the first opportunity we will sell  
12 these credit cards all around the world.

13 Q They were trying to check you on that?

14 A Yes.

15 Q Why did you -- what was your response to that? You said  
16 that was your first response.

17 A I said to them that, look, it's -- I don't want to discuss  
18 it, this question, but to discuss in Russia. Meaning that if we  
19 got this deal and if we want to award this out, I will not work  
20 on this anyway, it's not my job, it's Alexey -- Alexey's job and  
21 Alexey will handle this stuff.

22 And basically --

23 Q Now, after the Invita meeting you were questioned by Agent  
24 Schuler and Agent Prewett that first evening, is that correct?

25 A Yes.

**EXHIBIT C2**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

IN THE UNITED STATES DISTRICT COURT FOR  
THE WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA,	)	
	)	Case No. CR00-550C
Plaintiff,	)	
	)	Seattle, Washington
v.	)	October 5, 2001
	)	
VASILII VYACHESLAVOVICH	)	VOLUME 11
GORSHKOV, a/k/a VASSILI GORCHKOV,	)	
a/k/a "kvakin,"	)	
	)	
Defendant.	)	
	)	
	)	

TRANSCRIPT OF PROCEEDINGS  
BEFORE THE HONORABLE JOHN C. COUGHENOUR  
UNITED STATES DISTRICT JUDGE

For the Plaintiff:	Stephen C. Schroeder
	Floyd G. Short
	Assistant U.S. Attorneys
	601 Union Street, Suite 5100
	Seattle, Washington 98101-3903
For the Defendant:	Kenneth E. Kanev
	Attorney at Law
	1001 Fourth Avenue Plaza, Suite 2120
	Seattle, Washington 98154-1109
	Robert S. Apgood
	Attorney at Law
	500 Union Street, Suite 510
	Seattle, Washington 98101
Joseph F. Roth	
Official Court Reporter	
600 U.S. Courthouse	
Seattle, Washington 98104	
(206) 553-1899	

Proceedings recorded by computer-aided stenography.

1 site was finished. They placed it somewhere. It wasn't my  
2 problem to place it somewhere, for example, who wrote for the --

3 Q Well, how about the Formula One site, did you pay for name  
4 service for that site?

5 A No, I didn't pay for that site.

6 Q Did you think that was unusual that you weren't getting  
7 bills for name service?

8 A I found -- I found out that -- I found out that my name  
9 com.ru is a free name. You can release it. I found it in  
10 internet. That's why I order it -- that to release it. ru just  
11 meant ru. Like Uralton.ru, it's a paying domain. You have to  
12 pay for it. For com.ru, net.ru, all this second -- org.ru, what  
13 else, all those domains, you can release it for free.

14 Q Did you ever go to the public registration sites and see  
15 where the name service for your web sites were actually located?

16 A No, never.

17 Q You never -- you never looked them up?

18 A Never looked them up. And even if I did, I would -- I would  
19 did, I would never understand whether it's proper or not.

20 Q You wouldn't have understood that they were being hosted at  
21 a school in Michigan in the United States?

22 A I wouldn't understand. For me, it's just like -- I don't  
23 know. For me, all the numbers were -- and still I don't know,  
24 what does it mean, where --

25 Q You were the manager, weren't you, sir?

1 A Yes.

2 Q You were responsible for the bills?

3 A Yes.

4 Q You were responsible for providing service to your  
5 customers?

6 A Yes.

7 Q Now, when your ISP complained that it was getting scanned  
8 from tech.net, did you look into that?

9 A I ordered my employee to look into it.

10 Q Was that Deniz?

11 A No, it was Karpych, and he didn't comply with my order.  
12 That was our problem, and I solved this problem.

13 Q Well, didn't you testify that you asked Deniz, your new  
14 employee, to check out the complaints from the ISP?

15 A At that time he was a new employee, but, yes, after Karpych  
16 was fired, I asked Deniz to review all this stuff.

17 Q But you didn't follow up on that yourself?

18 A How could I?

19 Q Now, you received a call on July 14th, or perhaps 15th, in  
20 Russia from the United States, didn't you, sir?

21 A Yes, I did.

22 Q And when you answered the phone, isn't it true that you  
23 spoke for Alexey?

24 A No, it's not true. I spoke for myself.

25 Q Didn't Mr. Michael Patterson ask you twice if you were

1 web site?

2 A It wasn't purchases over web site, it was orders that could  
3 be covered and later Formula One will deliver the stuff, or  
4 people who wants to buy something will go to the shops to get  
5 the stuff. Just orders to go.

6 Q Would customers be using their credit cards over those web  
7 pages?

8 A No.

9 Q No?

10 A No.

11 Q If you were unaware of the plan to collaborate with the  
12 American company in hacking, why did you tell them on July 14th  
13 that you had three or four hackers working for you?

14 A I was aware about collaborating with American company, and I  
15 was aware that they want to hire guys from Russia who know  
16 something about security, and I said to them that, look, we can  
17 hire -- that we already got people who know the stuff, hackers,  
18 you can call hackers.

19 Q Hacking, breaking into systems, right, sir?

20 A Hacking meaning knowing the system.

21 Q Hacking what?

22 A Knowing, to know system.

23 Q Well, in the undercover meeting when you said, page 113,  
24 "You know, in Russia we, ah, can broke or hack into a system --"

25 A Can I get the transcript?

1 Q "-- but when we're here, we don't want to."

2 THE COURT: Page number of the transcript.

3 MR. SCHROEDER: 113.

4 THE WITNESS: I don't know. I don't get the  
5 transcript. I don't know. It's phone conversation. I got  
6 phone conversation. I don't have Invita.

7 THE COURT: Yes. What's the exhibit number?

8 MR. KANEV: 1c.

9 MR. SCHROEDER: 1c. This is the one in front of the  
10 jury.

11 MR. KANEV: Is that the final version, counsel?

12 MR. SCHROEDER: Yes.

13 A What page?

14 Q (By Mr. Schroeder) Page 113, sir.

15 A Mm-hmm.

16 Q Now, when you said, "You know, in Russia we can, ah, broke  
17 or hack into a system, but when we're here, we don't want to,"  
18 in what sense were you meaning that word, sir?

19 A And what -- exactly what, hack? I was saying that here --  
20 basically I was saying to them, look, we don't want to spend  
21 time here on this -- showing these problems. We can do it. We  
22 can manage this work. But right now really -- and one of the  
23 reasons I was saying this, because if this guy were still  
24 pushing to do something, I just wasn't able to do it.

25 Q In fact, weren't you worried about the FBI in the United

1 States if you did hacking here?

2 A About FBI here, when it was conversation in Invita, Alexey  
3 bring this word FBI, and I just pick up this word and we use it  
4 in all -- all the conversation.

5 Q All right, sir. Then on page 139, when you say, "I can tell  
6 you. We, ah, try to rake it, you can say, from companies. A  
7 few months ago we tried, but we found it's not, um, profitable.  
8 It's better to hack, hack, 'hack." In what sense were you using  
9 the word then, sir?

10 A I was telling these guys -- I was playing this stupid role  
11 of the hacker, and basically everyone knows this word "rake," I  
12 still don't use it and still don't know. I don't know how it  
13 come up in my conversation, but --

14 Q But didn't you review the transcript, sir?

15 A I reviewed it, and it's exactly right. And it sounds  
16 like --

17 Q You didn't make a change on that one, did you, sir?

18 A I didn't change, because it sounds like "rake." Maybe I  
19 said it. I don't know where -- I still don't use this word, and  
20 I still don't know exact meaning of this word.

21 But here I was still playing this role, this role of hacker,  
22 that we got -- that we've done that, we've done this, and we  
23 know everything, how to do it, we've got lots of experience.  
24 But right now we don't do it, because -- we don't do it, because  
25 it's not that profitable. -- That's what I said.



1 Q That's not what you said. The transcript reflects what you  
2 actually said?

3 A Yes, it says, "but we found it's not such profitable."

4 MR. SCHROEDER: May I have just a moment, Your Honor,  
5 please?

6 THE COURT: Yes.

7 (Brief Pause.)

8 MR. SCHROEDER: Mr. Gorshkov, I won't trouble you with  
9 any more questions at this time. Mr. Short --

10 MR. KANEV: I object to the form of the question.

11 THE COURT: Overruled.

12 CROSS-EXAMINATION

13 BY MR. SHORT:

14 Q Mr. Gorshkov, your user name on these computers that we've  
15 been talking about, tech.net and freebsd, was kvakin?

16 A Yes.

17 Q And your password on those accounts was c-f-v-l-e-v-f-q?

18 A I don't remember how -- how you spell it, but it's Russian  
19 word, so I do remember it. Probably you're right, probably  
20 absolutely right.

21 Q Why don't you take a look at Exhibit 12. If we could have  
22 that. And why don't we take a look at page 10. Yeah, that  
23 would be good to start with that section. On page on 10, at the  
24 top there, it indicates you putting in your user name kvakin and  
25 then the password that I just read, is that right?

**EXHIBIT D**

---

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT SEATTLE

UNITED STATES OF AMERICA, )  
 )  
Plaintiff, )  
 )  
vs. " )  
 )  
VASILIY V. GORSHKOV, )  
A/k/a VASSILI GORCHKOV, )  
a/k/a "kvakin," )  
 )  
Defendant. )  
\_\_\_\_\_ )

Case CR00-550C  
October 1, 2001  
9:30 a.m.

**COPY**

TRANSCRIPT OF PROCEEDINGS - VOLUME VII  
BEFORE THE HONORABLE JOHN C. COUGHENOUR  
UNITED STATES DISTRICT JUDGE

APPEARANCES:

On Behalf of the United States: FLOYD G. SHORT  
STEPHEN C. SCHROEDER  
Attorneys at Law  
  
On Behalf of the Defendant: KENNETH E. KANEV  
ROBERT APGOOD  
Attorneys at Law  
  
Also Present: Linda Noble  
Official Interpreter

Caroline R. Castle  
Official Court Reporter  
(206) 553-1899

Proceedings recorded by mechanical stenography; transcript  
produced by computer. ...

## Attfield-Direct (Continued)

1 A Partly by interview with Agent Schuler, and the other  
2 aspect is that in that the files were transferred, as  
3 Agent Schuler was logged into the kvakin account, with FTP. He  
4 had to have a read access to the files to obtain them. As  
5 well, there's a history file. And that is reflected in the  
6 commands, that that's where the file came from.

7 Q So based on the logs of the downloading process and the  
8 activity of Agent Schuler, you're able to say those were in  
9 kvakin's account?

10 A Yes, I am.

11 Q All right. Let's talk about data from these two machines  
12 that simply wasn't obtained at all. In the course of  
13 reconstructing these file systems, did you learn about some  
14 files like that, files that existed on the system but simply  
15 weren't copied?

16 A Yes.

17 Q What can you tell us about those?

18 A There are great volumes of system files that weren't picked  
19 up. There are data files, there are account files belonging to  
20 other users that could not be picked up and were not picked up  
21 due to permissions issues. There were other files that weren't  
22 known at the time of the download that weren't picked up that  
23 we learned about subsequently on analyzing the downloaded  
24 data.

25 Q Okay. How about encrypted material? Was there some of

## Attfield-Direct (Continued)

1 that?

2 A Yes. There was one entire subtree of encrypted  
3 information, and we weren't able to make anything of it.

4 Q Now, you also mentioned an incomplete transfer of a file.  
5 Tell us about that.

6 A There's a file that was used--there was a file that  
7 contained the contents of the kvakin\_nt directory and files and  
8 subdirectories from the freebsd system. And this file should  
9 have been, I believe the number was, approximately  
10 320 megabytes in length. And only 240 megabytes were  
11 transferred.

12 Q So what are the implications of that?

13 A The implications are that the remaining 80 megabytes were  
14 not transferred.

15 Q What about the material that did arrive?

16 A Because of the way that a tar file is created, all of the  
17 information that was received was received intact. All of the  
18 information that wasn't received wasn't received. And what  
19 we'd be left with at the very end of this file is at most one  
20 file that would have been truncated or damaged.

21 Q Okay. Can you explain that by way of some analogy? Is  
22 there some real-world analogy you can use to describe how that  
23 tar transmission process works?

24 A Yeah. Think about it as a truck pulls up to a loading  
25 dock, and the people on the truck are now unloading boxes. And

Attfield-Direct (Continued)

1 you get 50 boxes off the truck and there's 20 more to go, and  
2 the truck all of a sudden abruptly pulls away. And the  
3 person's about to hand you the last box, and it falls on the  
4 ground and breaks open. You get some of the contents intact,  
5 but everything unloaded you received intact. What was on the  
6 truck when it drove away you just didn't receive it all.

7 Q And does the fact that not everything was obtained in that  
8 tar file, does that affect the reliability of the data  
9 received?

10 A No, it doesn't.

11 Q You mentioned that there were some files that you didn't  
12 learn about until later that were on the system and not  
13 obtained. Are you referring to some databases?

14 A Yes. When analyzing--there are several scripts on the  
15 system. When analyzing those, we found evidence indicating the  
16 presence of two databases and a variety of tables. And then  
17 databases were identified as mm and mm1.

18 And going back to the download logs, was able to locate the  
19 presence of database software and the location where these  
20 files would normally have lived on the system. And, indeed,  
21 the files couldn't be downloaded because those areas were  
22 protected from the regular users.

23 Q You mentioned some scripts. Do the scripts actually have a  
24 mechanism for accessing the database?

25 A Yes, they do. Scripts actually reference that they should

## Attfield-Direct (Continued)

1 connect to the local computer often on Port 3306. They would  
2 connect as root. And the scripts also had embedded within them  
3 the password to connect.

4 Q So anyone who had the script could run it and get access to  
5 the database?

6 A That's correct.

7 Q Let's talk about these two Russian computers. And, in  
8 fact, let's talk about the network they were on. Were you able  
9 to determine how many computers were actually networked  
10 together with the tech.net and freebsd computers?

11 A On the basis of looking at the W-temp file and the  
12 information we have, we're aware of tech.net.ru and  
13 freebsd.tech.net.ru. The W-temp files also indicate  
14 approximately eight other PCs. Those would be PCs that were  
15 probably running Windows or Windows NT.

16 Q Are there logs that also tell you about the hardware of  
17 these computers?

18 A Yes, there are. On each system--whenever a Unix system  
19 starts, it writes startup messages to a log file. These are  
20 typically retained for diagnostic purposes. Each system  
21 creates a file that contains the information that describes the  
22 operating system, the hardware on the system, the layout of the  
23 hard disk, the date the operating system was built, as well as  
24 the boot time.

25 Q Why don't we start with the tech.net computer. Can I ask

Attfield-Direct (Continued)

1 A That matches what we saw in the portion of the script that  
2 fed the password field.

3 Q If we could scan across there. How about that birth date?

4 A 10/10/69.

5 Q And does this indicate that these were established at least  
6 the first portion here--in August, August 23rd of 2000?

7 A Yes, it does.

8 Q How about this IP? If we could go up just a touch. Date  
9 established IP. Does that IP--is that familiar to you?

10 A 133.78? Yes it is. That's for a computer named Pony at  
11 the Musashi Institute of Technology in Tokyo, Japan.

12 Q Is that IP address familiar to you?

13 A Yes.

14 Q What do you know about that?

15 A The computer was likely compromised and was used as a proxy  
16 or redirect server in targeting other information.

17 Q And you saw, then--in the tech.net and freebsd systems, you  
18 saw programs that then used that computer?

19 A Yes. The name was referenced in those scripts.

20 Q How about this 195.128.157.67?

21 A I believe that's the tech.net.ru computer.

22 Q All right. Let's turn to scripts that relate to E-bay.

23 And if I could have you now switch over to the freebsd system  
24 and Exhibit 216. Have you got 216 there?

25 A Yes, I do.



Attfield-Direct (Continued)

1 Q What is this?

2 A This is a listing of the contents of the E-bay directory of  
3 the kvakin account on the freebsd computer.

4 Q Now, we've got quite a few files on here. There are three  
5 files that are actually scripts or programs. Is that right?

6 A Yes.

7 A There's solded, randinfo.pl, func.pl. Those are the most  
8 interesting.

9 Q Those are the primary scripts?

10 A Yes.

11 Q Do some of these other files relate to input and output for  
12 those?

13 A Yes.

14 Q What's the primary script here? What's the one that is  
15 sort of the main program?

16 A The top level is solded.

17 Q Let's take a look at that. Exhibit 219. This is another  
18 PERL script?

19 A Yes, it is.

20 Q Okay. Again, I don't want to go into great detail of all  
21 the specific parts of this. How long is this?

22 A This is quite a lengthy script. This one is 22 pages. And  
23 it's actually--the main level alone is 22 pages, but the whole  
24 composite is quite a bit larger.

25 Q Okay. Now, in a moment I want to turn to a portion of this

## Attfield-Direct (Continued)

1 that actually sort of lays out what the script does. But  
2 before I do that, I notice at the bottom of the screen here we  
3 have something that says: Require/func.pl and  
4 require/randinfo/pl. What does that mean?

5 A That's the way that solded tells PERL that it needs to have  
6 the functions or the--part of the program available in func.pl  
7 made available for its use. It's basically saying: I need  
8 stuff in another file. Please give it to me. So it's asking  
9 for it.

10 Q If we could go down a little further. We have something  
11 here that says REDIR-HOST and PROXY.

12 A Yes.

13 Q What is that?

14 A What it's doing is assigning the--it's assigning a value to  
15 a couple of variables. It will use www.epsa.org as a redirect  
16 host. And it's assigning the value PROXY of REDIR-HOST at  
17 17492, which is a high port. The script is basically saying it  
18 wants to communicate with some remote machine, but it's going  
19 to go through another machine in the middle so the traffic will  
20 appear to have come from somewhere else, not where the script  
21 was actually run.

22 Q So this machine is a compromised machine?

23 A In all likelihood, yes.

24 Q Let's turn to page 15 of this program. Is there a--as I  
25 mentioned, sort of a summary of what this does? If we could

## Attfield-Direct (Continued)

1 scroll down to the lower half of this, starting where it says:  
2 Commands.

3 A Yes. What it's doing is showing--this would display the  
4 commands available for this script if you ran it. So, for  
5 example, nua means create random users.

6 Q And what does the script actually do? What does that  
7 mean: Create random users?

8 A It's actually creating random user accounts. So it's  
9 essentially establishing identities and doing them at random.

10 Q Okay. What else does this program do?

11 A It's capable of building auctions and manipulating auctions  
12 at E-Bay.

13 Q So when it indicates--so here it indicates EY registration,  
14 does that command actually register?

15 A Yes. That pertains to registration at E-bay.

16 Q How about this portion here that says: add cc?

17 A Add cc allows it to associate a randomly chosen credit card  
18 number with one of its randomly created identities.

19 Q Randomly chosen credit card from where?

20 A There is a database. One of the tables in mm or mm1 is  
21 called credit cards. And it chooses credit card and  
22 information relating to the card number out of the database at  
23 random.

24 Q And then what does it do with that randomly chosen credit  
25 card?

Attfield-Direct (Continued)

1 A It then associates that with a user, with a randomly  
2 generated user.

3 Q We also have down here several commands or functions that  
4 relate to auctions.

5 A Yes.

6 Q What do those do?

7 A Those are capable of manipulating the auctions at E-Bay.  
8 For example, overbid. It's capable of going in and reviewing  
9 an auction and adjusting its own bids, bids it has control  
10 over.

11 Q What would be the purpose for that?

12 A Drive the price up.

13 Q Does it allow you to control the bidding? In other words,  
14 to somehow ensure that you're going to be the winner?

15 A Yes. If you're able to track the auction and you know who  
16 all the participants are, if you have control over five  
17 identities and a sixth one appears, then you're able to take  
18 one of your five identities and make sure that the sixth is  
19 always outbid.

20 Q And as part of this lengthy script and its creation of  
21 users, is it creating people who can both buy and sell?

22 A Yes, it is. Those are both contained within the seller's  
23 table of the database.

24 Q Let's take a look at those two files that the solded script  
25 uses, the func.pl and randinfo. Let's start with the 217.

## Attfield-Direct (Continued)

1 A The first portion of that are names that were formed by  
2 choosing a random first name and a random last name and  
3 truncating them and putting an underscore in the middle. So  
4 OSC is the beginning of a name, perhaps Oscar. BL could be  
5 something like Black. It's combined the two together to form  
6 osc\_bl and then appended a random number, in this case  
7 217. So it created the e-mail number osc\_bl217 at insurer.com.

8 Q So this pattern exactly reflects that script and how it  
9 generates random names?

10 A Yes, it does.

11 Q And it's done this on both ends of the auction, the seller  
12 and buyer?

13 A Yes.

14 Q Let me have you turn to Exhibit 222, also in that kvakin  
15 account. This file is entitled feedbacks.

16 A That's correct.

17 Q What does feedback mean in the context of an E-bay  
18 auction?

19 A In an E-bay auction, buyers and sellers have a rating  
20 mechanism for each other where they submit feedback regarding  
21 their business experience. And you basically give negative or  
22 positive feedback on the basis of your satisfaction with the  
23 transaction or with the person with whom you're doing  
24 business.

25 Q Okay. Now, this file is yet another long file, is it not?

Attfield-Direct (Continued)

1 A Yes, it is.

2 Q Couple hundred pages?

3 A Uh-huh.

4 Q And is it safe to describe it as a list of different types  
5 of feedback?

6 A Yes. It's actually a dump of a table in a database that  
7 contains feedback.

8 Q When you say a dump of a table in a database, what do you  
9 mean by that?

10 A Normally, you can't read the context of a database written  
11 on a page like this. It's encoded in a form that the database  
12 software understands. But by dumping it out, you can dump it  
13 into a form that's readable. And then you can also manipulate  
14 it with other tools--for example, a text editor--and reimport  
15 it.

16 Q So this is actually just a portion of the database?

17 A This is the--this is one part of the database. There's  
18 much more to it than this.

19 Q Okay. And this indicates that the database on the system  
20 is fuckebay?

21 A That's the name.

22 Q And could we skip down to where the list of actual  
23 feedbacks begins? You may need to back out just a little to be  
24 able to read those and shift over.

25 So when we see, for example, this kind of language--very

Attfield-Direct (Continued)

1 satisfied, thank you, or smooth transaction, good  
2 communication, excellent E-bayer, A-plus-plus-plus--these are  
3 feedbacks that could be sent back to E-bay? Is that right?

4 A Yes. That's correct.

5 Q And then that would--what result would that have for the  
6 credibility of sellers on the auction?

7 A If you did--if something like this were used, you could  
8 completely skew the rating mechanism in your favor. So in  
9 other words, somebody who is--you wouldn't want to do business  
10 with, if--you could use this to skew the rating system.

11 Q And these 200-and-some pages are essentially variations on  
12 good transaction, good person to deal with?

13 A They're all very positive.

14 Q That type of thing.

15 A Yeah.

16 Q Did you find the database that's referred to here on the  
17 system?

18 A In the original form we know of its existence, but we don't  
19 have the database itself.

20 Q How is it that you know of its existence?

21 A Through reference in the download logs, you can see where  
22 the configuration files in the areas were that were used by the  
23 my.sql database. At the time of the download, we don't know it  
24 existed because we don't know it was there. And we also didn't  
25 have the permissions required to download the database.

## Attfield-Direct (Continued)

1 Q But in this case, it just so happened in kvakin's account  
2 there was the dump, as you described it, of a portion of the  
3 database?

4 A That's correct.

5 Q Do we know what else was in the database?

6 A Again, tables of credit card information, random credit  
7 cards complete with names," addresses, expiration dates, tables  
8 of first and last names, tables of e-mail identities that were  
9 used in a variety of situations.

10 Q Now, all of this relates to those three main E-bay scripts  
11 you talked about. Right? The solded, the func and the  
12 randinfo?

13 A Yes.

14 Q Were those scripts also found in kvakin's account on the  
15 other computer, the tech.net.ru computer?

16 A Yes, they were. They were also found in an E-bay  
17 directory. However, the files had much earlier time stamps and  
18 were much smaller. And reviewing the solded script, it also  
19 had less functionality.

20 So this indicates an evolution in the development of the  
21 script.

22 Q Now I'd like to turn to a different category of scripts,  
23 scripts that relate to PayPal.

24 How does PayPal work with E-bay? What's the relationship?

25 A PayPal is a mechanism that allows a payment to take place.



Attfield-Direct (Continued)

1 Say, for example, I put an item up for auction and several  
2 people bid on it--

3 MR. APGOOD: Objection, Your Honor. How is this  
4 witness qualified to discuss how PayPal works?

5 THE COURT: Overruled. Counsel, one lawyer, one  
6 witness. Mr. Kanev made objections earlier.

7 MR. KANEV: I'm sorry, Your Honor. That was a general  
8 objection. Mr. Apgood--

9 THE COURT: Nobody should be making objections as to  
10 any witness except the lawyer who will cross-examine the  
11 witness.

12 MR. KANEV: Thank you, Your Honor.

13 Q (BY MR. SHORT) The relationship between PayPal and E-Bay.

14 A Right. Basically, at the outcome of an auction you need a  
15 mechanism to transfer the payment from the buyer to the  
16 seller. And PayPal is a mechanism that can employ bank  
17 accounts or credit cards to cause a transaction like this to  
18 take place.

19 Q And can I have you take a look now at Exhibit 121.

20 Mr. Attfield, is this an exhibit that was in the kvakin  
21 account on tech.net.ru?

22 A Yes, it was.

23 Q And it's called gethttps.

24 A That's correct.

25 Q Essentially, what does this script do?

## Attfield-Direct (Continued)

1 A This script is capable of creating accounts at PayPal and  
2 managing them, and also assigning credit card information to  
3 them and triggering transactions.

4 Q Now, do we have a similar--at the beginning here, does it  
5 identify the database that's being used?

6 A Yes. It's working this time in the mm database. And  
7 again, we have root and the password.

8 Q And that's the same mm database you referred to earlier?

9 A If they were on the same machine, it would be the same  
10 database. Yes.

11 Q Now, if we could go to the bottom of that page. Now, what  
12 does this portion of the script do?

13 A Right at the very bottom, it obtains a random e-mail  
14 address, and it retains random credit card info that locates a  
15 full name for the credit card. And it does a sign-in to attach  
16 the credit card to the e-mail address.

17 Q Okay. So is it going into the database to get that random  
18 e-mail name and random credit card information?

19 A Yes. Those are being like pulled from a hat in the  
20 database, if you want to call it, to pick one at random. And  
21 then it's using those in the credit card function.

22 Q On the portion that if signed in, it's actually signed in  
23 to PayPal and creates an account?

24 A It will be connecting to the machine as if a normal user  
25 did that with a web browser.

Attfield-Direct (Resumed)

1 Q All right. In connection with the Memphis computer, you  
2 also mentioned that it was used to send large quantities of  
3 e-mail.

4 A That's correct.

5 Q And I think you mentioned the name Greg Stivenson involved  
6 in that?

7 A That's correct. "

8 Q Have you seen any similar e-mails in the data that you've  
9 reviewed on the two Russian computers that relate to the same  
10 type of solicitation?

11 A Yes, I have.

12 Q What have you found?

13 A On freebsd.tech.net.ru, there was the 111.dbf and 111.dbt  
14 files that contained similar solicitations for parts. And  
15 there were other messages that mentioned the name greg\_stiv at  
16 a variety of domain names. As an example, in the emails.my  
17 file.

18 Q Let's take a look at that 111 file you mentioned,  
19 Exhibit 261. Does this reflect the type of e-mail relating to  
20 the sale of computer parts you were referring to?

21 A Yes, it does.

22 Q And this file--again, this is a long one, isn't it?

23 A Certainly is.

24 Q Couple hundred pages?

25 A Yes, several hundred.

## Attfield-Direct (Resumed)

1 Q Are these all e-mails essentially listed one after the  
2 other?

3 A Yes. The contents of that file.

4 Q Let's take a look at the first one here. We have the  
5 indication about a quarter of the way down: Original Message.  
6 And if we could scroll up, just so we can see that message.  
7 The other direction. There we go.

8 So this message is coming from--

9 A The identity that sent it was Murat Nasirov at Yahoo.com.

10 Q And in the text it indicates: We're a firm in Khazakstan,  
11 and we want to buy processors.

12 A That's correct.

13 Q And this one is signed: Murat Nasirov, executive manager.

14 A That's correct.

15 Q And if you go throughout these e-mails, are there  
16 variations of that name as part of the e-mail address?

17 A Yes, there are.

18 Q And you mentioned that you had seen the Greg Stivenson  
19 ones. Are they of a similar character involving the sale of  
20 computer parts to a firm in Khazakstan?

21 A Yeah. It's a similar type of request.

22 Q Can I have you now look at Exhibit 259, which I believe is  
23 the other file you mentioned, the emails.my. What type of file  
24 is that?

25 A This is--it's a plain text file that contains a list of

Attfield-Direct (Resumed)

1 e-mail addresses, e-mail identities.

2 Q Can I scroll just a bit on those? Are these essentially  
3 just variations on that Murat Nasirov name?

4 A Yes. Because each name has to be unique for a given  
5 domain. You would just--by creating a variant, you can have  
6 multiples provided at the same e-mail provider.

7 Q And the domain name here is Yahoo.com?

8 A That's correct.

9 Q Do we also see that password we saw before in some of those  
10 scripts in the kvakin account?

11 A Yes.

12 Q Q1w2e3r4?

13 A That's correct.

14 Q Does there appear to be some relationship between this file  
15 and the one we just looked at?

16 A The addresses are similar.

17 Q On this Memphis computer, you also mentioned it was used as  
18 a relay or a proxy.

19 A Yes.

20 Q Did you find evidence of specific computers being used as a  
21 proxy, including Memphis?

22 A Yes, I did.

23 Q May I ask you to look at Exhibit 136. Okay. This file, is  
24 this from the kvakin account again?

25 A I believe so. I'm just going to flip back to the

Attfield-Direct (Resumed)

1 directory. Yes, it is.

2 Q Okay. And if we could scroll it just a bit. This is  
3 another PERL script, is it?

4 A Yes, it is.

5 Q Does this indicate a proxy that's being used as part of  
6 this script?

7 A Yes, it does. "

8 Q And what is it?

9 A Memphis.k12.mi.us.

10 Q What does this script do using that proxy?

11 A It establishes a connection to a remote\_host using that as  
12 its intermediate.

13 Q So if you're on that remote computer and traffic comes  
14 through this, where does it appear it's coming from?

15 A It will appear to have come from memphis.k12.mi.us.

16 Q If you could flip in the same notebook there to 157. This  
17 file, squid.conf, what does that mean?

18 A Squid is a--again, another software package. And Squid  
19 offers a cacheing or proxying mechanism for connecting to web  
20 sites. This is a configuration file for it.

21 Q This file will actually indicate the computers to be used  
22 as proxies?

23 A Yes. Or addition of computers to be used.

24 Q Can we turn to page 3 of that exhibit about halfway down?

25 Does that indicate the computers that are being used as proxies

Attfield-Direct (Resumed)

1 by this file?

2 A It indicates the use of computers as cache peers.

3 Basically, their IP identities and the port numbers.

4 Q So that indicates Memphis is one of them?

5 A That's correct.

6 Q And these other computers like merisel.uct.ru?

7 A Merisel has appeared earlier in the material we've  
8 reviewed.

9 Q As something that was used as a proxy?

10 A As a likely compromised system.

11 Q And then the Musashi computer, the Japanese computer you  
12 referred to earlier, did you also find evidence of that being  
13 used as a proxy?

14 A Yes. That was referenced in several of the PERL scripts.

15 Q If I could ask you to look at Exhibit 133. What is this?

16 A This establishes a connection to a web site through an  
17 intermediate and requests a page.

18 Q And what is the intermediate?

19 A The intermediate in this case is:  
20 pony.cms.ie.musashi-tech.ac.jp.

21 Q That's indicated there?

22 A That's correct.

23 Q Does this number at the end--does that indicate a  
24 particular port on that machine?

25 A Yes. That was the same port we found in the configuration

Attfield-Direct (Resumed)

1 files.

2 Q Is there some other evidence or additional evidence in  
3 kvakin's account as to how all of these different proxy  
4 computers might be kept track of or maintained?

5 A There is a script in the home directory on tech.net.ru  
6 called add\_proxy, which would be used to add the name and  
7 address, port number, of a computer to a database of computers  
8 available for that function.

9 Q Can I ask you to look at Exhibit 114? Should be in  
10 Volume 4.

11 Now, you indicated that this file was located in the home  
12 directory?

13 A Yes. That's correct.

14 Q Do you mean /home/kvakin?

15 A /home/kvakin.

16 Q And it's called add\_proxy.

17 A That's correct.

18 Q So what does this program do?

19 A This little--this script connects to the mm database and  
20 inserts a record into the database where you say--it says:  
21 Insert into proxies, that's referring to the table, host,aim.  
22 It's substituting values that were passed in on the command  
23 line to the script.

24 Q So this is the same mm database you've testified about  
25 before?



Attfield-Direct (Resumed)

1 A Yes, or another instance of it.

2 Q And is this a way, then, that you can simply type in the  
3 compromised system and it will add on to your database?

4 A Yes.

5 Q I'd like now to turn to another computer system of Nara  
6 Bank called hankook. Did you review data from that server?

7 A Yes, I did.

8 Q And did you work with Norm Sanders in getting access to  
9 that data?

10 A Yes, I did.

11 Q What were you able to determine about the Nara Bank  
12 server?

13 A The Nara computer had been compromised. We were able to  
14 determine computers that had been in communications with it and  
15 changes that had been made to the web site that was served at  
16 that computer.

17 Q What type of changes to the web site?

18 A There was a page that had been added to the web site that  
19 was not put there--was not put there by the people that managed  
20 the site.

21 Q Do you remember the name of that?

22 A I believe it was paypal.asp.

23 Q Can I ask you to look at Exhibit 451? Is this the file  
24 paypal.asp that you referred to?

25 A Yes, it is.

Attfield-Direct (Resumed)

1 hankook server.

2 MR. APGOOD: No objection.

3 THE COURT: It will be admitted.

4 Q (BY MR. SHORT) Mr. Attfield, this is the list?

5 A Yes, it is.

6 Q From six computers, we had access to that paypal.asp file?

7 A That's correct.

8 Q And you've already identified the first two there as

9 Musashi--

10 A I recognize the school at the bottom. I believe that's

11 63.70.

12 Q And that was Musashi?

13 A That's correct.

14 Q And tech.net?

15 A Is 157.67.

16 Q Do you recognize any of these others?

17 A I think one of them is surnet, if I'm not mistaken. I

18 would need to look at the directory to verify.

19 Q Are these IP numbers that are all reflected in that  
20 exhibit, 15, the directory that shows IP numbers and domain  
21 names that's been admitted?

22 A Yes, they are.

23 Q All right. The last topic I'd like to ask you about is  
24 credit cards.

25 Did you do a search of all of the data from tech.net.ru and

Attfield-Direct (Resumed)

1 freebsd.tech.net.ru to try to determine how many unique credit  
2 cards were located?

3 A Yes, I did.

4 Q How did you do the search?

5 A I constructed a script that went through and looked for  
6 patterns of numbers that met the criteria for appearing to be a  
7 credit card. For example, a Visa card has a 16-digit number  
8 that begins with 4. The first four digits correspond to an  
9 issuer. That's known as the BIN number, the bank ID number.  
10 So searched through and extracted those numbers out.

11 Q Okay. And you're aware of these patterns of credit cards,  
12 based on personal experience?

13 A I have previous experience working for a company where we  
14 had a web site and had to deal with credit card transaction  
15 processing.

16 Q Now, the number that you came up with, would that not count  
17 credit cards that were, for example, in some of the databases  
18 you've been testifying about?

19 A The databases may very well have been larger, but we don't  
20 have them.

21 Q So based on the data that you did have in tech.net.ru and  
22 freebsd, how many unique credit cards did you find?

23 A I think the number was around 56,000.

24 MR. SHORT: No further questions for Mr. Attfield.

25 THE COURT: You folks can stretch, if you'd like.

**EXHIBIT E**

---

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 113

GORSHKOV: (In Russian) (Unintelligible) at home?  
(Unintelligible).  
(Unintelligible). Whatever...(unintelligible).  
(Simultaneous conversations)

CW: Oh the, the network (unintelligible).  
(Simultaneous conversations)

GORSHKOV: Whatever is set (unintelligible).

IVANOV: (Unintelligible) address...(unintelligible).

CW: Oh the, the network (unintelligible).  
(Simultaneous conversations)

MALLON: Yeah.

IVANOV: (Unintelligible). Let's, let's (simultaneous  
conversations).

LEETH: Is there others that, I mean it doesn't necessarily  
have to be that one. It could be something you  
guys have done in the past. I mean if you wanna go  
back to a, a system.

GORSHKOV: You know in Russia, we can, ah, broke or hack into  
a system, but when we're here, we don't want to  
(unintelligible)...

MALLON: (Unintelligible).

LEETH: (Unintelligible).

MALLON: Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 114

GORSHKOV: (Unintelligible) an address, an address, so...  
(Simultaneous conversations)  
(Unintelligible).

LEETH: Because I, again that's what I keep talkin' about.  
That's what we're gonna be doin'. That's our  
business. We want it where we can, ah, penetrate,  
find it and we'll (unintelligible).

GORSHKOV: (Unintelligible) system. We don't, we don't do not  
write down sometimes. We just, broke, use it.

CW: Oh?

GORSHKOV: You, ah, sometimes it's hard to explain, but one of  
third systems on Windows NT...easy to hack in.

CW: One-third?

GORSHKOV: We have, we did some (unintelligible) scanners.

LEETH: Well, what, have you guys made any other  
(unintelligible) any other intrusions other than, I  
mean Alexey was telling me about Lightrealm, the  
job you did there. Have you done any more?  
(In Russian) (Unintelligible).

GORSHKOV: (Unintelligible).

IVANOV: Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 115

GORSHKOV: (Unintelligible). You know, just, if you want I can show you a few, a few NT hacks. Just to show. It's not (unintelligible).

LEETH: No, but I mean have you, have you been able to, other than Light, Alexey said Lightrealm was one company that you (unintelligible).

GORSHKOV: Lightrealm is a big company. It's uh, and the, they used.

LEETH: Have you done any more type companies like that?

GORSHKOV: Ah, do you remember the company that is called webcom com, webcom com?

LEETH: Webcom?

GORSHKOV: Yes. It was, ah, last (unintelligible) company. They have about, ah, ten, maybe twenty thousand users (unintelligible).

LEETH: Oh.

GORSHKOV: Ah, I can show you. (Unintelligible). Especially, for example...  
(Brief pause.)

LEETH: Yeah. You know where the bathroom is right?  
(Unintelligible).  
(Brief pause.)  
(Unintelligible).

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 116

CW: Don't like the stick?

GORSHKOV: I don't use.  
(Laughter)

GORSHKOV: this kind of stick. I like this kind.

CW: Oh yeah, yeah. Yeah.

LEETH: What does this do, Vasiliy? What did you just, is it a P.C. also? I mean is it your...

GORSHKOV: Ah...

LEETH: ...do you actually...

GORSHKOV: I want to buy a network card for it and use it from

CW: (Unintelligible).

LEETH: Oh really? Okay.

GORSHKOV: (Unintelligible)...

LEETH: It's not too small?

GORSHKOV: Functional as P.C.?

LEETH: Yeah.

MALLON: (Unintelligible) P.C..

CW: Uh hum.

GORSHKOV: (Unintelligible).  
(Brief pause.)

GORSHKOV: It was a huge, I don't know, company but now they, I don't know where he is.

LEETH: Oh yeah he, he went to the bathroom.



FD-302a (Rev 10-6-95)

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 117

\* \* \* \* \*

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 118

TAPE #6

GORSHKOV: Ah, how to say it in English?

MALLON: Large thing?

GORSHKOV: No, ah, now (unintelligible) com on  
(unintelligible) when you type web com com, you go,  
you go to Verio (unintelligible).

CW: Oh, they bought'em out?

GORSHKOV: They bought'em.

CW: Okay. That's a redirect on the web page.

MALLON: Oh, okay.

GORSHKOV: And, ah, they (unintelligible) their own  
(unintelligible) language.

CW: Their own programming language?

GORSHKOV: No, ah, yes. So, and there was a big hole.

CW: Oh, okay. And you found the hole?

GORSHKOV: (Unintelligible).

MALLON: Uh hum.

GORSHKOV: Right now, they don't accept new users.

MALLON: They don't accept new users?

GORSHKOV: Because of that (unintelligible) Verio  
(unintelligible).

CW: Verio.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 119

GORSHKOV: Yes.

MALLON: (Unintelligible) Verio (unintelligible).

GORSHKOV: And Verio got it (unintelligible) and they a few months ago, they got (unintelligible) all account information was accessible to anyone.

MALLON: Wow.

GORSHKOV: All new account information, all new, ah, including passwords...

MALLON: Wow.

GORSHKOV: ...ah, passwords to cyberpage.

CW: And you found that hole?

GORSHKOV: And, ah, it was in the tempe (phonetic) directory.

CW: Oh, the temp directory. Okay. And you guys found this?

GORSHKOV: Yes.

CW: Oh cool.

GORSHKOV: Well it was easy actually 'cause...

LEETH: Well did you, did you guys contact them and see if they were interested...

GORSHKOV: No because, ah, when we found it we just, what can do, and (unintelligible) and they, they, ah, watch it, they, they watch our activities and close this hole.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 120

LEETH: Oh they did? Well, have you guys been able to find holes in a company, and this is what we're interested in.

GORSHKOV: Yeah.

LEETH: Finding holes in a company, uh, and then, you know, a week after (unintelligible)...

GORSHKOV: We can try. We can't, ah, we can't, ah, promise we, we'll find something. But who knows?

LEETH: Have you done any in the past though other than what Alexey said...

GORSHKOV: Yes. Well, uh, with webcom I worked, and it was, it wasn't, um, some sort of, ah, accident, accident.

MALLON: You were in their system a little bit and then they closed you out.

GORSHKOV: Ah...

MALLON: They closed, Verio closed you out after you found this temp?

GORSHKOV: I don't think so. I assume because the com script language was poor when (unintelligible).

MALLON: (Unintelligible) it was bad.

GORSHKOV: Not, ah, convenient to user. And they beginning lose users and they have to sell.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 121

CW: Oh, okay.

LEETH: Um have you been able to get any business though out of, out of companies as far as providing these holes? Showing, them the holes? Can you, I mean how much are they paying you?

GORSHKOV: You know, when you in Russia and when you try to contact some sort of company.

LEETH: Uh huh.

GORSHKOV: Ah, big companies.

LEETH: Right.

GORSHKOV: (Unintelligible) usually they got a lot of programmers. You even, ah, usually you can't even explain to anybody what happens. If you got a man that understands you...

LEETH: Uh huh. He can...

GORSHKOV: That man, very fast, will close this hole and will say to manager that he find the hole.

LEETH: Uh huh.

(Simultaneous conversations)

GORSHKOV: And, and it happens you cannot (unintelligible)...

LEETH: Take credit for it? He'll take credit for it?

GORSHKOV: Yes.

LEETH: Mmm.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 122

GORSHKOV: Especially when, ah, they will know that you're in Russia and...

LEETH: What about, what about here in the U.S. though?.

GORSHKOV: If, let's say, he (unintelligible) FBI (unintelligible) FBI.  
(In Russian)

IVANOV: (In Russian) But the fact is...

LEETH: I heard F.B.I. (Laughs)

IVANOV: But the fact is that if, let's say (in Russian) (unintelligible) FBI (in Russian) (unintelligible).

GORSHKOV: We don't think about the FBI at all. Because they can't get us in Russia.

LEETH: Right.

GORSHKOV: Your guys don't work in Russia.

LEETH: Absolutely.

GORSHKOV: Maybe they work, but they can't just can't come and say...

LEETH: Right, right.

GORSHKOV: "Let's go."

LEETH: What's your equivalent of the F.B.I. called?

GORSHKOV: Ah, F.S.B.

COONEY: F.S....

LEETH: F.S.B.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 123

(Unintelligible).

GORSHKOV: But they, they didn't have a good specialist. And their principle form is different from the FBI.

LEETH: Well since you're in Russia though, can you get companies in the United States?

IVANOV: Sure, yes.

GORSHKOV: Yes.

LEETH: You can?

GORSHKOV: Yes.

LEETH: See, that's maybe something that we, see, because we're talkin' about the same thing. We're here in the U.S., but if we can get you guys from Russia to get into American companies...

GORSHKOV: Ah, the fact is that, ah, programmers don't provide, ah, detailed information about them. Without it, they will not believe you. Ah, their system is, ah, (unintelligible).

CW: Can you take information and show it to them?

GORSHKOV: Ah, we tried but they, they, they have lost every, everything (unintelligible) beginning (unintelligible). When they found, they close, and give nothing to us. It is better just gather

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 124

information about it, when you find something big,  
ah bigger.

LEETH: Well how do you, how do you, I mean I'm asking you  
this as a businessman. How do you contact a  
company when you find a hole?

GORSHKOV: Call.

LEETH: Call?

GORSHKOV: Call. Ah, (unintelligible)...

IVANOV: (Unintelligible) and we try to first of all E-mail.

LEETH: Uh huh.

IVANOV: But usually it's not work because, ah, the system  
administrators, they not want, they hold.

GORSHKOV: (Simultaneous conversations)

LEETH: I hear you.

IVANOV: ...(Unintelligible) they call to managers.

LEETH: Right, right.

IVANOV: Because...

LEETH: Well, can you call management?

IVANOV: Ah, I try call managers (unintelligible).

GORSHKOV: They say that our administration, our, is the best  
in the world and...

IVANOV: Yes, and, ah...

GORSHKOV: ...you can't hack it.



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 125

(Laughter)

(Simultaneous conversations)

GORSHKOV: They have administration. You can contact about, they say no. And begin such call...

MALLON: Hmm.

GORSHKOV: And when, of course is, ah, lost, you can...

LEETH: Did they, is that what happened with Lightrealm?

IVANOV: And usually the administration (unintelligible)...

GORSHKOV: Lightrealm? Ah...

LEETH: 'Cause I know they got hacked. That's why I'm asking.

GORSHKOV: Because ah they (unintelligible). (Laughs)  
Actually, you can ask about Lightrealm Alexey. It his work.

LEETH: But it is...

GORSHKOV: He did it alone.

LEETH: He did it? Okay. That's what we're tryin' to do here. But we can't do it because of the F.B.I. Do you understand? (Unintelligible)...

GORSHKOV: He (unintelligible).

LEETH: (Unintelligible) you're in Russia...

GORSHKOV: Actually, we can do it because we can do, ah, such with, ah, all will be invisible or will, or will be

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 126

visible, but, ah, another (unintelligible) where we...

LEETH: Well, maybe if we could, ah, we could have you guys hack a place for us. You're over there, we're here. All right? We go to them and provide the service. We reach out and we pay you guys, you know, per hack or however you wanna do it.

GORSHKOV: It will be sensible but the fact, ah, (unintelligible)...

LEETH: Well, let me ask you what, what did Lightrealm pay? What, what did they pay you for that?

GORSHKOV: Ah, you see it's not a, a question of money. They pay only because right now they are friends and they didn't pay a price. Alexey found a hole.

LEETH: Oh they didn't?

GORSHKOV: The price of this hole is very big, but they pay, you know. (In Russian) I don't know how to say it.

COONEY: (Unintelligible) they may have just (unintelligible).

GORSHKOV: (Unintelligible).

LEETH: They paid pennies...but why?  
(Simultaneous conversations)

IVANOV: ...was about eighteen dollars ah per month.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 127

LEETH: Eighteen dollars a month?

GORSHKOV: Well that's why we do it and Lightrealm was a huge company.

LEETH: Right.

GORSHKOV: So they can pay real price, but they didn't pay what even asked about small company. They can pay too but they never pay.

LEETH: What about any other places in the U.S. Have you had any luck going, going to them?

GORSHKOV: Actually, ah, we stopped trying to contact with these people. Because we have some money. We did not (unintelligible)...

(In Russian) (Unintelligible) did not especially need (unintelligible).

COONEY: Ah they weren't in a hurry for money particularly so (unintelligible).

(Simultaneous conversations)

IVANOV: (Unintelligible).

GORSHKOV: (In Russian) And these negotiations were just empty chat.

COONEY: Ah, he said these negotiations were just a waste of time.

LEETH: Oh, really?

..

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 128

COONEY: (Unintelligible).

LEETH: They didn't wanna pay it? Oh. Because there's been in the last six months maybe a year there have been several hacks into companies here in the U.S. And I'm hearing that it, well some of the hacks have come from Russia. But some of the companies have paid. And that's what I want, that's what I wanna get into.

GORSHKOV: No, we don't, ah, we know, ah, some people that work for it. They ask for companies, but it's true it's very very difficult. You have to broke thousand hosts, but you'll be paid by one, maybe two.

LEETH: Yeah. Yeah.

GORSHKOV: It's true. It, it's very, you don't have to, ah,...

IVANOV: Spend time.

GORSHKOV: ...spend your time on hacking. You have to, ah, to spend your time on negotiating.

LEETH: Huh.

GORSHKOV: The fact ah, ah, we can try it and you'll see.

LEETH: Okay.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 129

GORSHKOV: We can write somebody and then you'll see what the, we can, ah, create a folder or create a file that, and write them, you have a faulty security or something. But, they say it's, ah, problem you will be contacted by FBI, never ask us about it.

IVANOV: Uh hum.

GORSHKOV: But in several days, maybe several months, they pay to a huge company that work on security and they'll fix this hole.

LEETH: Yeah.

GORSHKOV: But not pay to hack it.

LEETH: Well see, ah, that's what we were trying to do is we'll be the security company (unintelligible)...

GORSHKOV: And we, ah, we tried to negotiate, ah, beginning with work, we can help you with your security.

LEETH: Yeah.

GORSHKOV: But (unintelligible), we are from Russia, brought hacks with from Russia. You know Russia has a bad reputation about hacking and computer (unintelligible).

CW: And some good reputation for being good at it.

GORSHKOV: But reputation, and there's no laws that can't, hacking can be, ah...

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 130

LEETH: Exactly.

GORSHKOV: And we (unintelligible) so...

LEETH: What about, ah, credit cards? Credit card numbers? Anything like that?

GORSHKOV: What do you (unintelligible)...

(Laughter)

LEETH: It's always, ah, you know, if you've got access to credit card numbers that's, ah...

CW: Companies get really worried about (unintelligible)...

(Simultaneous conversations)

GORSHKOV: Actually, wait a minute, actually, we'll never, when we're here, we'll never say that we got access to credit card numbers.

(Laughter)

LEETH: I understand. I hear ya, I hear ya.

(Simultaneous conversations)

GORSHKOV: It's, ah, it's, ah, just security question.

LEETH: Right.

GORSHKOV: But when we are in Russia, we can (unintelligible).

LEETH: But you could, if you were over there you could get 'em for us? If we, you know, decided at some point...

..

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 131

GORSHKOV: The fact is that, that this kind of question is better discussed in Russia.

(Laughter)

GORSHKOV: Is true, yes, because now FBI is (unintelligible) stories about it.

LEETH: Yeah.

GORSHKOV: ... (unintelligible).

LEETH: It's all overblown. They think they're good. They're not. It's a myth. Don't worry about it. I mean (unintelligible)...

(Simultaneous conversations)

LEETH: ...I'd worry, I'd worry. Listen, and we're in this building. I feel comfortable in this building right? All right.

GORSHKOV: Okay...

LEETH: But, at the same time, you know I know we're in the U.S. and I know what you're saying. All right? But I, I...

GORSHKOV: I have never been in the U.S. Why do I need some problem?

LEETH: Yeah. These are...

GORSHKOV: (Unintelligible).

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 132

LEETH: ...these are things that, that we wanted to talk to you guys about okay? About what we can do to help you. What you can do to help us. And you guys being in Russia, can help us.

GORSHKOV: The fact is that ah our ah, I don't know how to say it's not a company. We've never called our firm "company." We call "Kontora".

LEETH: Office, an office.

GORSHKOV: (Unintelligible) You know Russian word "Kontora."  
(Unintelligible).  
(Simultaneous conversations)  
(Russian/Laughter)

COONEY: Okay, very specifically focused semi-official company but not a full blown company. We've never (unintelligible).

LEETH: Well are the fifteen or twenty people that're working for you guys are they, are they hacking also?

GORSHKOV: Um, actually, they, not all hackers.

LEETH: Uh huh.

GORSHKOV: About, ah, four maybe. All of them can be designers, programmers, and so on. About four of



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 133

them work only for designing, programming, web hosting...

LEETH:

Right.

GORSHKOV:

Others help us to create standard hacking tools...

LEETH:

Hacking tools?

GORSHKOV:

Yes.

CW:

Oh, okay.

GORSHKOV:

And they even...

(Simultaneous conversations)

IVANOV:

If we can't find some tools, ah, some tool in internet, we write (unintelligible)...

(Simultaneous conversations)

LEETH:

Now did you, did you guys write the tools that you used to hack into our system?

GORSHKOV:

Of course.

(Unintelligible).

LEETH:

Okay. All right.

GORSHKOV:

Actually, our firm is, initially, it was created as hackers club.

LEETH:

A hacker's club?

CW:

Oh.

GORSHKOV:

But there was a lot of misunderstanding with that. And we had to split...

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 134

IVANOV: Uh hum.

GORSHKOV: ...some of, some of, our club, go, go to nowhere.

LEETH: Yeah.

GORSHKOV: We know about that and we know, they, ah, work various way (unintelligible) American.

LEETH: Yeah.

GORSHKOV: But we didn't, ah, stop our club. We growing with five people.

LEETH: Uh hum.

GORSHKOV: (Unintelligible).

LEETH: How do you pay them though? How do you pay your people from w...where is the money coming in? You understand?

IVANOV: If money is not come in it is our mistake. But people work, and anyways, we pay the people.

LEETH: But I mean how do you guys get the money to pay them?

IVANOV: People come to us. It is our mistakes that money is not come to us.

LEETH: What do you, what...

IVANOV: But peoples...

(Simultaneous conversations)

LEETH: Well no no no.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 135

GORSHKOV: (Unintelligible).

COONEY: Ah yeah.

GORSHKOV: Well it, it's, ah, sort of personal question and here in America, (laughs) talk about it (unintelligible). (Unintelligible).

GORSHKOV: Don't ah, don't ah (unintelligible).

COONEY: Don't get offended if...

LEETH: No, no, I'm not.

GORSHKOV: (Unintelligible). (Simultaneous conversations)

GORSHKOV: There's no question...

LEETH: I'm not, I'm not asking for any secrets you understand. Okay. But, and I'm not, I'm just curious that...

GORSHKOV: I can explain, ah, to pay, ah, for, ah, for our people...

LEETH: Right.

GORSHKOV: ...peoples. Is an enough money, that pays, uh, for the host and, ah, web creation and so on. But it's not enough for growing for us for (unintelligible).

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 136

LEETH: Yeah. Well what I'm, what I'm trying to say is are the guys hacking, are you getting money that way.

GORSHKOV: No. They never, pay.

LEETH: They don't, they don't do that.

GORSHKOV: They, they, didn't pay. They only create tools for us.

COONEY: Aw. So you guys can do it. All right. Okay.

GORSHKOV: They help us to.

COONEY: And the, and the money that you get for that you pay these guys.

GORSHKOV: You can say...  
(Laughter)

GORSHKOV: ...you can say it.

LEETH: Okay.

GORSHKOV: (Unintelligible) not gonna say it.

LEETH: All right. All right. Understood. Because I mean that's, that's what we're trying to do here. You understand?

GORSHKOV: I understand.

LEETH: I know, I know the companies. I, I can sell, I can sell my business.

GORSHKOV: I know um...

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 137

LEETH: But the technical side, these guys, these guys  
can't do it from here.

GORSHKOV: I understand.

LEETH: For, for obvious reasons.

GORSHKOV: You know when, ah, it's, ah, a question of plan.  
(Unintelligible) here, maybe two, maybe three, and  
in (unintelligible) Russia, you know Putin he's  
K.G.B.

LEETH: Yeah.

GORSHKOV: Here right now I, I begin (unintelligible) because  
he begins from Moscow to take such hacker's slots,  
there are a lot of them, and they didn't go to jail  
but they bought, they everybody, um, will be a  
worried about how. You know, just they take  
control of, of it. But we can create same class in  
Kazakhstan (unintelligible). it's, ah, about two  
hun...two hundred kilometers from Chelyabinsk.

LEETH: Right. Right.

GORSHKOV: And there are a lot of more corruption.

LEETH: Yeah, yeah.

GORSHKOV: And we can pay and create everything there. If  
you've got money. You got everything there.

LEETH: Oh, right. Okay.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 138

GORSHKOV: So only question is, ah, we, you know, can be here or, ah, or, ah, we can be in Russia, but we can, ah, send some of our people there, and they will be hacking from...

LEETH: Right.

GORSHKOV: Kazakhstan, ah, Uzbekistan, so on.

LEETH: Right, right.

GORSHKOV: (Unintelligible).

LEETH: (Unintelligible) fly down, take your P.C.  
(Unintelligible).

GORSHKOV: They (unintelligible).

LEETH: Should be easy. Okay. All right. Just so I know you guys are as good as you, I think you are. How can I ask you this without, I don't want you to feel afraid but (unintelligible)...

(Simultaneous conversations)

LEETH: No, no, no, no, I understand. But I'm trying to find a way to see your work. I know of a lot of hacks that occurred here in the United States. And some of the companies paid out. Paid money. Without saying specifics, could that, any of that have been you guys?

GORSHKOV: Ah (unintelligible)...

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 139

(Simultaneous conversations)

GORSHKOV: I can tell you. We, ah, try to, to rake it, you can say, from, um, companies. A few months ago we tried, but we found it's not, um, such profitable.

CW: Uh hum.

LEETH: Yeah.

GORSHKOV: It's better to hack, hack, hack, and when you find something very interesting, all those hacks will be (unintelligible) and will do only that. But if you find something very interesting you, you can get such, ah, so many monies, so you don't need ever record from company that you hack.

MALLON: (Unintelligible). My dog needs to go for a walk. So (unintelligible).

LEETH: Huh.

GORSHKOV: So, ah, but anyway we try to create such companies as security consultant. We hack them, this security consultant, ah, give a call, ah to manager or director of the firm, we'll explain that they will be easy hacked. Let us try.

LEETH: Right.

GORSHKOV: We don't ask you to, ah, pay or some.... Let us try.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 140

LEETH: Uh huh.

GORSHKOV: ...already hacked company.

LEETH: Uh huh.

GORSHKOV: (Unintelligible),.

LEETH: Right. You've already hacked it though right?

GORSHKOV: Yes.

LEETH: Yeah.

GORSHKOV: And then we will show some hole...

LEETH: Uh huh.

GORSHKOV: ...a hole just to be sure they will pay.

LEETH: Right.

GORSHKOV: But you, ah, we didn't begin because of lack of time.

LEETH: Right.

GORSHKOV: We didn't have enough time. I sleep very, ah, I, I didn't, I sleep about seven years, ah, seven hours per day.

LEETH: Seven hours per day you said?

GORSHKOV: Yes.

LEETH: Yeah.

GORSHKOV: So I, I, I just, ah, don't have enough time.

LEETH: Yeah.



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 141

GORSHKOV: And, and I don't, ah, trusted people to create this company to, ah, to let them create this company.

LEETH: Uh huh.

GORSHKOV: Under my control.

LEETH: Right. It, it seems like that this is such a growing business so that, that, that...

GORSHKOV: Yes. It's very, very...

(Simultaneous conversations)

LEETH: ...companies are willing to pay lots of money to avoid getting hacked for security.

GORSHKOV: For security. Right.

LEETH: And, ah, I know some, I've been hearing. 'Cause I deal with a lot of security managers. I know some companies have paid out twenty twenty-five thousand dollars. You know, to hackers. You know, and that's...

GORSHKOV: Ah, you know, maybe somebody pays, but we never (unintelligible) ah, I know is, is a reasonable price.

LEETH: Yeah.

GORSHKOV: We, uh, protect some Russians from a big on-line shop, there are a lot of credit card information.

CW: Uh hum.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 142

GORSHKOV: And, I didn't feel safe, but we will, ah, we will have some, ah, accessible real, real big shops that (unintelligible) about twenty thousand credit cards from Russia. .

CW: And they, they need this to, to protect (unintelligible).  
(Simultaneous conversations)

GORSHKOV: To protect them. But is, ah, so, ah, unsecure.

LEETH: Yeah.

GORSHKOV: It is even funny.

LEETH: Let me ask you this. Is there a market in Russia for credit card numbers?

GORSHKOV: Ah, actually, yes, but we never sell it. And we never buy it.

LEETH: Okay.

GORSHKOV: We never sell it or buy.

CW: Uh hum.

LEETH: Right.

GORSHKOV: You can sell, you can buy it but, you know, a lot of peoples, they just take information and never pay and you need to find a trusted people.

LEETH: Right. (Unintelligible)...

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 143

GORSHKOV: But if you find a trusted people. (Unintelligible)  
I find trusted people, I never give them such  
information. I make them work, work for me.

LEETH: Right.

GORSHKOV: And this um, um (unintelligible).

LEETH: Okay. Well that's, that's basically what we're  
looking for from you guys over there is  
ah...(simultaneous conversations).

GORSHKOV: I understand, but, ah, how it's...you guys here  
don't quite understand what is happening in Russia.

LEETH: Uh huh.

GORSHKOV: Because in Russia there are a lot of, um, a lot of,  
powerful, powerful, ah, men of, ah no, ah services,  
not services, ah...

LEETH: Powerful...?

GORSHKOV: Like K.G.B., F.S.B. It is better to (simultaneous  
conversations).

LEETH: Okay, okay.

GORSHKOV: (Unintelligible)...

LEETH: Over there, there's a lot of powerful agen...  
agencies?

GORSHKOV: Agencies, yes.

LEETH: Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 144

GORSHKOV: Actually.

MALLON: Okay.

GORSHKOV: Ah, and if they, they got information, they never, ah, pay anybody. But if they get an order from hack agency.

LEETH: Yeah.

GORSHKOV: They'll take it and in one, two hours, it, it will be, ah, not like in the United States, it will be if they'll take you, it is not a matter you did it or you never did it. They can't prove or they can prove. Because if they take you, you'll go to jail.

LEETH: Yeah.

GORSHKOV: Or you'll work for them.  
(In Russian) (Unintelligible)

GORSHKOV: They even will not try to prove if they can prove it. They'll find something that, they can prove.  
(unintelligible)...

LEETH: Right, right.

COONEY: Right.

GORSHKOV: And they will find some...

LEETH: Well how could we communicate, ah, securely with you guys in Russia? Like if we found, I know that

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 145

you mentioned the C.T.S., I mean you guys still have a, an account with C.T.S.? You still own an account?

GORSHKOV: Ah, for C.T.S. all questions to. Yes. The account at C.T.S. but...

LEETH: I mean is it secure? Can we...

IVANOV: I opened an account with stolen credit card, into this and to try to hack it. I'm successful and, ah, after this they, I contact administas...ah, administrators and, ah, they open regular account for me.

LEETH: Oh, they did? Cool.

IVANOV: And they...

MALLON: (Unintelligible).

LEETH: And they paid you?

IVANOV: Yeah.

LEETH: Can we, can we use that account? I mean to communicate?

GORSHKOV: I think the best way is communicate is if, ah, if we will create something (unintelligible).

LEETH: Right.

GORSHKOV: Ah, the best way is to live here one month (unintelligible) I'll go back to Chelyabinsk.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 146

LEETH: Okay, okay.

GORSHKOV: And somebody.

LEETH: Come out when somebody else comes?

GORSHKOV: I think Alexey better anybody else. He'll come, he'll can do something from here.

LEETH: Yeah.

GORSHKOV: And since it's, ah, not, ah, dangerous or...

LEETH: Yeah. What, what did, what did ah C.T.S. pay you? Was it good?

GORSHKOV: No. No.

IVANOV: No. Payment is...

GORSHKOV: We never received good money from hack.

LEETH: Really?

GORSHKOV: Ah, from, ah, people who was, who was hacking.

IVANOV: Ah, the last, ah, money that was good.

LEETH: Uh huh.

IVANOV: It, ah, have been about ah one or two months ago.

LEETH: Yeah.

IVANOV: And, ah, it has been casino. I'm just (unintelligible) how to steal money from, from them. And, ah, after this, they paid me, and payment (unintelligible) for about ah four... (In Russian)

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 147

COONEY: Thousand.

IVANOV: Four, four thousand dollars.

LEETH: Four thousand?

IVANOV: And, ah, they pay to me every week, ah, in my and sent every, every week, ah, one thousand.

LEETH: Yeah.

IVANOV: And, ah, because it was, ah, not trust me and, ah, they think that I can, ah, do something bad for company.

LEETH: Right.

IVANOV: And, ah, because this, they sent, ah, packs of money to me.

LEETH: Right, right.

IVANOV: For trust.

LEETH: Right.

LEETH: How do they pay you? Do they wire it, ah, to Russia or...

IVANOV: Wire transfer.

LEETH: To, to Chelyabinsk?

IVANOV: To Chelyabinsk.

LEETH: Mmm that's, that's...

GORSHKOV: The best way to help, ah, is not to Russia.

LEETH: No. I was gonna say.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 148

IVANOV: (Unintelligible).

LEETH: It's usually better to go to a third country. Wire it. Yeah. And then wire it again. Yeah, that's something you guys mi...may wanna think about. 'Cause if you've got it goin' straight to Chelyabinsk, um, somebody could track it goin' out of here. Were they sending it from the states straight to Chelyabinsk?

GORSHKOV: No. Ah, I think it must be made such way. Ah, no way no pack will be directed to Chelyabinsk or here to Seattle.

LEETH: Right.

GORSHKOV: It must be in such ways that all monies to some off-shore firm.

LEETH: Yeah it's...

GORSHKOV: It's in, ah...

LEETH: Caribbean.

GORSHKOV: ...in, ah, third, ah third countries, like Kazakstan, Uzbekistan.

IVANOV: Kazakstan.

GORSHKOV: Ah, and so...

LEETH: Well how much would we have to pay officials in Kazakstan if we were wiring money back and forth?



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 149

Do you think they would be, you'd have to pay off a lot?

IVANOV: (Unintelligible).

GORSHKOV: Ah, I don't know actually but we can find out.

LEETH: Yeah.

IVANOV: (Unintelligible).

(Simultaneous conversations)

GORSHKOV: No, there are a lot of, ah, companies (unintelligible) of people in Russia that can help you to open any off-shore firm or...

LEETH: Yeah. Accounts.

GORSHKOV: Accounts. And it was thousand, maybe two (unintelligible).

(Simultaneous conversations)

LEETH: I know I've asked you this before and I don't mean to keep pushing you, but I'm trying to get an idea of what you're capable of doin'. All right? And I know that's, I don't wanna ask you.

GORSHKOV: The fact is...(unintelligible)...

LEETH: Tryin', tryin' to, we say in America establish your, your bona fides (unintelligible). You understand? Your...

GORSHKOV: Yeh, yeh, I understand.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 150

LEETH: And that first hack that you did on our system was very good. According to the people that, Michael said he was real good. Um, is there any other examples you can give me that I can research?

GORSHKOV: (Unintelligible). I can, ah, companies like Lightrealm (unintelligible).  
(Simultaneous conversations)

GORSHKOV: But we can do it a thousand per day. We got some scanners. We can run it, and we'll get a report on companies and it will be so many that...

LEETH: (Unintelligible), okay. You, you set up a scanner to run stuff through.

GORSHKOV: (Unintelligible) the scanners run and make all kinds because all holes that are well known.

LEETH: Okay.

GORSHKOV: So, ah, you can, ah, think about what, what is plan (unintelligible). But I think is right. Ah, the best way is not to try to create a firm if interesting yes, but in the (unintelligible) of the process you can get nothing, nothing, and you will, you will work about it a year or half year.

LEETH: Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 151

GORSHKOV: But you find a hole that is not give you full access. And if you, ah, run a scanner, you'll get full access to a thousand machines, everyday.

LEETH: Okay.

GORSHKOV: And...

LEETH: Well, what makes you decide to go after one specific company versus another?

GORSHKOV: (Unintelligible)...

LEETH: Once you get, I mean how much money they've got, ah...

GORSHKOV: No.

LEETH: No?

GORSHKOV: Actually, when we'll try (unintelligible) because they pay little money (unintelligible), you just take (unintelligible) I don't remember but there were ten of them.

LEETH: Ten companies that did pay?

GORSHKOV: No.

LEETH: No.

GORSHKOV: Nobody did pay. We just checked, ah, security (unintelligible).

LEETH: Okay.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 152

GORSHKOV: And every tenth, maybe tenth, or maybe fifth company of Windows machine was...

LEETH: Hackable (unintelligible).  
(Simultaneous conversations)

GORSHKOV: Hackable. Not hackable, ah, not hack, ah, not hackable. We don't hack any, any (unintelligible). We know how, ah, but, ah, we never did it because this, ah...

LEETH: ...not worth it...

GORSHKOV: ...(unintelligible) no we don't get enough time (unintelligible).

LEETH: Right, right. But I guess my question though is what, when you, when you get into a company what makes you wanna go to that company versus all the other ones that you've got out there that you could get into. What makes, you understand? Is it how many accounts they have or how much money?

GORSHKOV: Ah, the fact is that, ah, we're, a few days ago, we need some ISP's to steal ah, to hide our host.

LEETH: You needed what?

GORSHKOV: To hide our host, to

LEETH: hide your host?

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 153

GORSHKOV: ...to, to, ah we need some IPs to show, ah, to hack some systems that can trace to our host. We don't need some problems with our...

LEETH: Okay.

CW: Ah, (unintelligible).

LEETH: So you found other IP addresses and hosts...

GORSHKOV: IPs, IPs, and we found we just opened Yahoo or Alta Vista.

LEETH: Alta Vista?  
(Simultaneous conversations)

CW: (Unintelligible) exploits?

GORSHKOV: No, we don't touch exploits, we no exploit. We search for companies. We just run some...um, symbols, and it was random, and they found, uh, Alta Vista found...

LEETH. Hmm.

GORSHKOV: ...several hundreds of companies with that, this work, and we just scanned them. And we get fifty or twenty accounts and full accessible machines and we'll

CW: Use those.

GORSHKOV We need SMTP servers to send e-mail anonymous.  
Just got, uh, words from one of those machines with

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 154

very many E-mails and takes from there. Ah, addresses, SMTP services, and checks them off. It's a, it's a question of ah what do you need? If you need (unintelligible), you scan (unintelligible). If you need money, you scan banks.

CW: Banks?

LEETH: Yeah. Oh yeah.

GORSHKOV: So...

LEETH: Have you had any luck with those? Banks?

GORSHKOV: Banks? Actually, with banks, there are a lot of problems (unintelligible). Ah, we got some, we never, uh get any money from 'em.

LEETH: Yeah.

GORSHKOV: We take some control but you know with banks, they, they make the servers stand alone, only for internet and hope they (unintelligible).

(Simultaneous conversations)

LEETH: It's off line. Right. It's an In...Intranet.

(Simultaneous conversations)

GORSHKOV: Among banking, there are differences. They, maybe few, I don't know how it work. Maybe they make a (unintelligible), but when you come on-line banking

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 155

systems, they make their host, ah, on their machine, but when you work with account, it's , ah, (unintelligible) in one or one, ah, IP or on one, ah, net and this net is fully security. (Unintelligible) wasting time on it. Just not profitable.

CW: So you never found any holes on on-line banking?

GORSHKOV: Ah yes, we found some but we didn't receive anything.

CW: Oh you didn't tell the bank about the holes?

GORSHKOV: Ah, I tried to (unintelligible).

IVANOV: It is very difficult to find person, ah, who can really help, ah, security (unintelligible).  
(Phone rings)

IVANOV: Because too many, too many managers and, ah, (unintelligible).

LEETH: (On telephone) John...Yeah...Uh huh...Yeah...  
Right...

IVANOV: Very difficult.

MALLON: (Unintelligible) on-line banking.

IVANOV: (Unintelligible).

CW: (Unintelligible) banks would want to close their holes 'cause if their customers find out, they'll

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 156

take their money out of the bank and the bank will go out of business.

GORSHKOV: No, we don't take, ah, (unintelligible) make quick money.

LEETH: ...Uh huh...

GORSHKOV: With twenty or fifty thousand dollars. We want to make (unintelligible).

LEETH: ...Okay. All right...

GORSHKOV: (Unintelligible) so we just gather information. We take it...

LEETH: (on telephone) That's it? That's all he can pay?

GORSHKOV: (Unintelligible) money for today, for tomorrow. You just need, um, (unintelligible) a target to work with.

CW: Right. Well banks are good customers for us because, you know, we do a, test their networks and...

GORSHKOV: I understand. Yes, but ah, then (unintelligible).

LEETH: (on telephone)...Okay...All right...All right. Just let me know...Yeah bye. (End of telephone conversation)



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 157

GORSHKOV: (Unintelligible). And you can put there the information that don't, ah, put money in this bank on people. You can do it.

CW: Right.

MALLON: (Unintelligible).

GORSHKOV: It's easy. It's easy (unintelligible). Actually, there are a lot of such banks but the real money, you...

CW: I would think the banks would be afraid (unintelligible) you doing that.

GORSHKOV: Maybe they're afraid, but we never contact with them due to lack of time.

CW: Oh.

MALLON: Are they hiring more people to work with you in Russia?

GORSHKOV: You know, ah, the human factor is that, uh... (unintelligible).

MALLON: (Unintelligible)...

GORSHKOV: ...it is so hard to find, ah, good people that we'll never, ah...

MALLON: Good, good people you can trust or just.

GORSHKOV: Ah, trust and work.

(Simultaneous conversations)

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 158

GORSHKOV: Trust and work. I can find people I can trust, but I cannot find (unintelligible). (Laughs)

MALLON: Okay. Is your company gettin' well known in Russia or...

GORSHKOV: No.

MALLON: ... (unintelligible).

GORSHKOV: You know, well known company like ours...

MALLON: You say (unintelligible).

GORSHKOV: ... (Unintelligible) if you, ah, it, it is to be in official capacity, if you, if you will be well known as a web hosting company, or well known as a web design company (unintelligible).

MALLON: You're not known as like technet?

GORSHKOV: But if you well known as hacker, or (unintelligible).

CW: (Unintelligible) agencies.

GORSHKOV: You agencies.

MALLON: Oh, I gotcha. But are you, is your company name Tech-Net?

GORSHKOV: Tech-Net ru (phonetic).

MALLON: Or is that your, just your web site?

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 159

GORSHKOV: It's just web site. And our company's called  
technet ru. It's just, ah, ah, how do you say  
(unintelligible).

COONEY: (In Russian) What?

GORSHKOV: (Unintelligible).

COONEY: Ah, top of the, ah, top of the heap?

GORSHKOV: (in Russian) (Unintelligible). It's just to let  
people know we exist. If they ask, we can send  
them something (unintelligible).

COONEY: Uh huh. It's simply a, a means for people to know  
that they exist. It's not a big...

MALLON: Gotcha. Gotcha.

LEETH: So there's no, there's not a formal name to it? I  
mean there's not a real...

GORSHKOV: It's, ah, it's, ah, just official name we can  
change it.  
(Laughter)

GORSHKOV: We don't (unintelligible).

LEETH: But that's Tech Control you told me? Or Tech...

GORSHKOV: You know, Tech, (in Russian), Tech-Ne Tru  
(phonetic) means "We don't rub them, we rub these"

COONEY: Ah, uh huh.

COONEY: Uh huh.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 160

GORSHKOV: This is (unintelligible). It's a play on words.

COONEY: Aw.

GORSHKOV: (Unintelligible).

MALLON: Uh hum.

GORSHKOV: (Unintelligible).

COONEY: (Unintelligible). Tech-Ne-Tru.

GORSHKOV: (Unintelligible). Tech-Ne-Tru. I rub others.

COONEY: That's fine.

LEETH: (Unintelligible).

GORSHKOV: It's, ah, a play on words.

IVANOV: I like, ah, words play.

GORSHKOV: I like Tech-Ne-Tru, why not, why not its like technical (unintelligible). But...

LEETH: Are all these people that, that work for you are they, that make the tools are they in Chelyabinsk?.

GORSHKOV: They work for Tech-Ne-Tru.

LEETH: Are they in Chelyabinsk or are they spread out all over Russia.

GORSHKOV: They're in Chelyabinsk.

LEETH: Are they? Okay.

GORSHKOV: It's ah very difficult to work with people that are (unintelligible).

LEETH: Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 161

GORSHKOV: They can work for you, but (unintelligible).

LEETH: Exactly. So they, that, that picture that you sent, ah, is that your office, office space?

IVANOV: (Unintelligible).

GORSHKOV: (In Russian) (Unintelligible) Here, take this (unintelligible).

MALLON: Did you want to finish this tonight?

LEETH: Do you, do you guys want to, ah, we can, you wanna work on this later? I mean I think we've got enough information, ah, Ray's gotta leave out tonight.

MALLON: I need to walk my dog.

LEETH: We can, we can work on this this weekend. I mean if you don't wanna...

GORSHKOV: Ah...

\* \* \* \* \*

TAPE #7

GORSHKOV: ...actually, information...what kind of information do you want? We can give you some (unintelligible). You can (unintelligible). It will be a real big (unintelligible).

LEETH: Mmm.

GORSHKOV: ...just company, just the companies.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 162

LEETH: Yeah.

GORSHKOV: Ah, is, ah, ah, you can just to show what we can you can (unintelligible) and show, ah, web hosting companies (unintelligible) and tomorrow, what we'll (unintelligible).

LEETH: Okay. All right. That's fine. I know you guys are tired.

GORSHKOV: Actually...

LEETH: So you guys got, you, you set up your own account in, in C.T.S. I mean you set, set up your own?

IVANOV: Hmm?

LEETH: Got your own account in C.T.S.? Ah C.T.S. the company you were talking about earlier?

IVANOV: (In Russian) I don't understand.

IVANOV: (Unintelligible) C.T.S.

GORSHKOV: (In Russian) (Unintelligible) account in C.T.S.

IVANOV: (In Russian) (Unintelligible).

GORSHKOV: If you got, ah, ah, stolen credit card, you can open an account there.

LEETH: Yeah. But I mean you gotta, you got a sole account. Yeah.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 163

GORSHKOV: We got this account by stolen credit card, but only for hacking purposes.

COONEY: Purposes.

GORSHKOV: ...purposes.

LEETH: Yeah, yeah.

GORSHKOV: And once you find the holes there (unintelligible).

LEETH: But when you set up an account like at C.T.S. were you you the, I mean do, are you the only one that's using it or do you, you let other people, other people use it or, how does that work?

GORSHKOV: Ah, this account only, ah, for the work of Alexey, he opened it and he, I don't need it. But no, actually, ah, I don't, ah, I can't call me hacker. I never was a hacker and never will be hacker...

LEETH: Okay.

GORSHKOV: (Unintelligible) but, you know, it's not, ah, hacking actually, a part of business.

LEETH: Yeah exactly.

CW: Uh, huh. Yeah.

LEETH: That's why we're here.

GORSHKOV: Hacker is, ah, hacker will broke the system, that is powerful and secure businessman (unintelligible).

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 164

CW: Security consultant.

GORSHKOV: No. I don't...  
(Laughter)

GORSHKOV: ...I, I (Unintelligible).

COONEY: (Unintelligible).

GORSHKOV: (Unintelligible) consult (unintelligible).  
(Laughter)

GORSHKOV: It's not (Unintelligible). I prefer to work with  
it. (Unintelligible).

LEETH: Uh hum. It's a business.

GORSHKOV: (Unintelligible) occupation.

LEETH: It's a business. You bet. And it's growing.

GORSHKOV: Yes.

LEETH: It's growing.

GORSHKOV: Very very (unintelligible).

COONEY: How many firms like yours, or Konteras, are there  
like yours?

GORSHKOV: I don't know, actually. I think in Chelyabinsk,  
it's the only one. (Unintelligible) in Moscow  
there are several. But I don't know what they do.

LEETH: In Ch...

GORSHKOV: (Unintelligible).

COONEY: ...in Chelyabinsk, there's only one?



288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 165

GORSHKOV: Yes.

COONEY: You guys?

GORSHKOV: In Chelyabinsk, I think, in...ah, yes, ah big, ah, big city, Petersburg. It's, ah, (unintelligible). I think there are no such (unintelligible). In Moscow, there are. Definitely, there are. I don't know how they work or what they know, but they're, ah, some of them. In Vladivostok, I know there's...they, ah, do something (unintelligible).

COONEY: Tough business.

LEETH: There's a lot of, lot of people in it though. That's the problem. That's one of the problems. There's a lot of knowledgeable folks.

GORSHKOV: Ah there are a lot of but, ah, the problem of these people is they are not, how do you say (unintelligible). (In Russian)

COONEY: There's no union or organization, associations.

GORSHKOV: They do not...There are no organization of most of them.

COONEY: Yeah.

GORSHKOV: Because of, ah, hackers (unintelligible).

COONEY: (Unintelligible).

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 166

GORSHKOV: They work a lot.

LEETH: Uh huh.

GORSHKOV: You can give, ah, (unintelligible) such a  
(unintelligible).

CW: Is this one, one of your tools?

MALLON: Super Scan?

IVANOV: (Unintelligible). (Simultaneous conversations)

GORSHKOV: It's simple for a scanner, it's beautiful, but....

MALLON: (Unintelligible).

IVANOV: First of all, I must to know what (unintelligible).

CW: Uh hum.

MALLON: Right, right.

GORSHKOV: (Unintelligible).

IVANOV: (In Russian) Well, yes (unintelligible).

MALLON: Oh.

LEETH: You guys have any more questions for these guys?

CW: You guys, that, is that the scanner you use a lot  
or different software is that your favorite?

GORSHKOV: No, it's, ah, (unintelligible).

IVANOV: (Simultaneous conversations) (Unintelligible).

GORSHKOV: There are a lot of such scanners.

CW: In-Map is the one we usually use.

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 167

GORSHKOV: And we don't like such scanners because we don't need such scanners.

CW: Right, right.

GORSHKOV: We can easily take it from the net. Why (unintelligible).

CW: Right, right.

IVANOV: If we can, ah, if we can find something why we must develop it.

CW: Exactly. Why reinvent the wheel?

LEETH: All right. You guys tired?

GORSHKOV: No. When we work, we (unintelligible)... (Laughter)

GORSHKOV: Because we work by night. (Unintelligible).

GORSHKOV: ...(unintelligible), ah, condition.

LEETH: Yeah, yeah.

GORSHKOV: Can I say condition?

CW: Uh hum.

MALLON: Uh hum. (Unintelligible).

IVANOV: (Unintelligible) condition (unintelligible).

GORSHKOV: (Unintelligible). Especially if you got a new project and you have to learn

FD-302a (Rev 10-6-95)

288A-SE-84302-ELIB

Continuation of FD-302 of Tape #4, On 11/10/2000, Page 168

LEETH: Right.

GORSHKOV: quickly..

LEETH: Right.

GORSHKOV: You work, work, work. In the U.S., peoples work...

COONEY: You'll sleep well tonight.

(Laughter)

LEETH: Have one shot of Vodka and...

(Laughter)

LEETH: ...you sleep well. You guys wanna head over?

IVANOV: You really not drink. We drink because ah don't, don't have something to do at airport.

LEETH: Uh huh.

(Simultaneous conversations)

GORSHKOV: So nothing to do. Absolutely.

LEETH: Yeah.

GORSHKOV: We are know every...

IVANOV: And nothing to do in the airplane.

GORSHKOV: ... corner of airport, and just walk there, back there...

(Laughter)

LEETH: Yeah.

GORSHKOV: And just (unintelligible).