

IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL SEGAL,

Defendant.

03 JUN 10 PM 6:00

U.S. DISTRICT COURT

DOCKETED

JUN 16 2003

No. 02 CR 0112

Judge Ruben Castillo

FILED

JUN 10 2003

MICHAEL W. DOBBINS  
CLERK, U. S. DISTRICT COURT

NOTICE OF MOTION

TO: Dean Polales, Esq.  
Virginia Kendall, Esq.  
William Hogan, Esq.  
Assistant U.S. Attorney  
219 South Dearborn Street, Suite 500  
Chicago, Illinois 60604

PLEASE TAKE NOTICE that on Friday, June 13, 2003, at 9:30 a.m., we shall appear before the Honorable Judge Ruben Castillo, or any judge sitting in his stead, in the Dirksen Federal Building, 219 S. Dearborn Street, Chicago, Illinois 60604, and then and there present the attached Defendant's Motion for an Evidentiary Hearing, a copy of which is hereby served upon you.

Dated: June 10, 2003

  
Daniel E. Reidy

Thomas P. McNulty

Jeremy P. Cole

JONES DAY

77 West Wacker Drive, Suite 3500

Chicago, Illinois 60601-1692

(312) 782-3939

Attorneys for Defendant

MICHAEL SEGAL

IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL SEGAL,

Defendant.

03 JUN 10 PM 6:00

U.S. DISTRICT COURT

No. 02 CR 0112

Judge Ruben Castillo

FILED

JUN 10 2003

MICHAEL W. DOBBINS  
CLERK, U. S. DISTRICT COURT

DEFENDANT'S MOTION FOR AN EVIDENTIARY HEARING

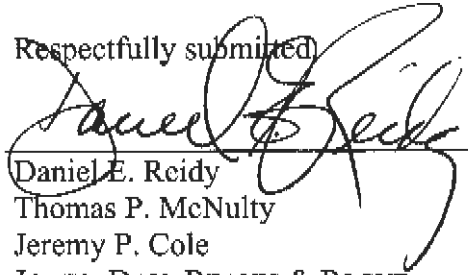
Defendant, Michael Segal ("Mr. Segal"), by his undersigned counsel, moves this Court to grant him an evidentiary hearing to establish whether government witnesses were acting as agents of the government, and therefore in violation of the Fourth Amendment, when they procured information that a confessed computer hacker had stolen from Mr. Segal and his insurance brokerage firm, Near North Insurance Brokerage, Inc., during an extensive eight-month hacking spree that began several months before Mr. Segal's arrest.

In support of this motion, Mr. Segal submits the accompanying Memorandum of Law in Support of His Motion for an Evidentiary Hearing, and Appendix of Exhibits in Support of Defendant's Motion for an Evidentiary Hearing.

WHEREFORE, defendant Michael Segal respectfully requests that this Court grant his motion for an evidentiary hearing to determine whether Mr. Segal's constitutional rights have been violated.

Dated: June 10, 2003

Respectfully submitted



---

Daniel E. Reidy  
Thomas P. McNulty  
Jeremy P. Cole  
JONES, DAY, REAVIS & POGUE  
77 West Wacker Drive, Suite 3500  
Chicago, Illinois 60601-1692  
(312) 782-3939

Attorneys for Defendant  
MICHAEL SEGAL

IN THE UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF ILLINOIS, EASTERN DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

MICHAEL SEGAL,

Defendant.

03 JUN 10 PM 6:00

U.S. DISTRICT COURT

No. 02 CR 0112

Judge Ruben Castillo

DOCKETED

JUN 16 2003

FILED

JUN 10 2003

MICHAEL W. DOBBINS  
CLERK, U. S. DISTRICT COURT

**DEFENDANT'S MEMORANDUM IN SUPPORT  
OF HIS MOTION FOR AN EVIDENTIARY HEARING**

Daniel E. Reidy  
Thomas P. McNulty  
Jeremy P. Cole  
JONES DAY  
77 West Wacker Drive, Suite 3500  
Chicago, Illinois 60601-1692  
(312) 782-3939

Counsel for Defendant  
MICHAEL SEGAL

June 10, 2003

97

## TABLE OF CONTENTS

	Page
I. INTRODUCTION .....	1
II. LEGAL FRAMEWORK FOR ANALYSIS.....	5
III. FACTUAL DISCUSSION.....	7
A. A Computer Hacker Repeatedly Stole Massive Amounts of Confidential, Privileged and Proprietary Information From Mr. Segal and Near North Before and During the Government's Investigation of Mr. Segal.....	7
B. The Government's Principal Cooperating Witnesses Solicited and Received Stolen Information from Mr. Cheley. ....	11
C. At Least One Government Witness Attempted to Cover Up His Solicitation And Review of Stolen Information. ....	15
D. Mr. Segal Needs an Evidentiary Hearing To Determine Whether Certain Witnesses Were Acting as Government Agents When They Solicited, Received, and Reviewed Material Stolen from Mr. Segal and Near North.....	16
1. Mr. Segal Needs an Evidentiary Hearing To Determine Whether the Government Knew, Should Have Known, or Acquiesced in Its Witnesses' Procurement of Stolen Information. ....	17
2. Mr. Segal Needs an Evidentiary Hearing To Determine Whether the Government's Witnesses Procured the Stolen Information To Assist the Government.....	21
IV. CONCLUSION.....	25

## **I. INTRODUCTION**

For more than eight months, defendant Michael Segal and his insurance brokerage firm, Near North Insurance Brokerage, Inc. ("Near North"), were the targets of a complex, intrusive, and focused computer hacking scheme by one of Near North's ex-employees. The hacker pilfered proprietary, confidential, and attorney-client privileged information from Near North's system on a routine basis, beginning at least four months before Mr. Segal's arrest in January 2002, and continuing until as late as April 2002, well after Mr. Segal's arrest.

At about the same time as the hacker began perusing and stealing copious amounts of this information from Mr. Segal and Near North, a number of other former Near North employees, who were now working for a rival insurance brokerage firm, began volunteering information to the federal government with the intention of destroying Mr. Segal and Near North. These former Near North employees sought to gain a competitive advantage over Mr. Segal and Near North for themselves and their new employer. As the discovery in this case has shown, these former employees became the government's key "confidential sources" and witnesses. The allegations made by these individuals were in fact the centerpiece of the affidavit used to support the search warrant and arrest warrant against Mr. Segal on January 26, 2002.

Despite the government's strident and unqualified denials of any connection between the hacker and its key witnesses, it is now clear beyond any doubt that the hacker repeatedly provided the government's principal cooperating witnesses with the most sensitive and critical of stolen and privileged information hacked from Near North's system. Recently uncovered proof conclusively shows that critical information stolen from Mr. Segal and Near North by the hacker was solicited and received by these witnesses. Forced to concede that his clients indeed received stolen information, the witnesses' private counsel explained to a court in related civil litigation

that his clients used the hacked materials solely "in connection with our cooperation with the government."<sup>1</sup>

Mr. Segal seeks an evidentiary hearing to determine whether, under the relevant case law, government witnesses were acting as agents of the government when they solicited and received confidential and privileged information that the confessed computer hacker had stolen from Mr. Segal and Near North during his extensive, eight-month hacking spree. As the case law discussed below makes clear, Mr. Segal need not show that the government explicitly directed its witnesses to obtain stolen information in order to invoke the protections guaranteed to him under the Fourth Amendment. Rather, an agency relationship between the government and a private party may be inferred for purposes of the Fourth Amendment if the government "blinks its eyes" at an illegal private search, and then reaps the benefits.

Based on controlling legal authority, a finding that there is an agency relationship between the government and its witnesses sufficient to implicate Fourth Amendment protections may be shown through various factors, including whether: (1) the government knew or should have known of the hacking activity based on its investigation and information supplied by its witnesses; (2) the government acquiesced in its witnesses' continued procurement of stolen information; and (3) the government's witnesses procured the hacked information to assist the government. The evidence currently available to Mr. Segal does much more than suggest that the answer to all of these factual issues is "yes," and he now seeks the help of this Court in the

---

<sup>1</sup> The related civil litigation is pending in the Circuit Court of Cook County, and is styled *Near North Insurance Brokerage, Inc. et al. v. AON Corporation et al.*, Case No. 02 CH 01595. Richard J. Prendergast is lead counsel for Near North in the action, and Craig D. Tobin represents Mr. Segal individually. Eric Brandfonbrener of Perkins Coie represents the government's cooperating witnesses in that litigation, and acknowledged that his clients used hacked material in their cooperation with the government in a hearing on April 18, 2003. (See Ex. 1, Transcript of April 18, 2003 hearing, at 76.)

form of an evidentiary hearing to establish that he has been deprived of critical constitutional protections.

Mr. Segal realizes that granting an evidentiary hearing places burdens on an already extremely busy court, and he does not ask for one lightly. Throughout the investigation and prosecution of Mr. Segal, the government repeatedly insisted, in conversations with counsel for Mr. Segal and with counsel for Near North, that its witnesses had no connection to the hacking activity. The government even took the position that, should Near North allege in related civil litigation that there was a conspiracy between the hacker and its witnesses, the government would view that allegation negatively and take it into account in deciding whether to identify Near North as a RICO enterprise in superseding charges against Mr. Segal, or whether to name Near North as a defendant.

Now, however, as a result of materials obtained in discovery in the civil litigation and in response to Rule 17(c) subpoenas in this case, Mr. Segal has gathered irrefutable proof that the government's insistence that there was no connection between the hacker and its witnesses was flat out wrong. Certain of the government's key witnesses, all of whom were former executives at Near North who left Near North to work for competitors, unquestionably solicited and received stolen information from the confessed hacker. The witnesses' knowledge that the information was hacked is demonstrated by a series of pre-arrest, pre-indictment e-mail communications between one key government witness and the hacker. In one of those communications, the hacker noted that the government witness must not be "happy" with Mr. Segal "based on what I've read," and that if the government witness was "interested in knowing what Segal's plans are[,] let me know a number to call." The witnesses' knowledge of the hacking is further demonstrated by multiple, transparent "cover-up" e-mails exchanged between



the same government witness and the hacker. In one such cover-up e-mail, the government witness pretended that the hacked information was "sent in error" and "deleted without any review," even though, just two hours earlier, the government witness had explicitly asked the hacker to "please resend" a large amount of stolen information. That witness then received an additional cache of stolen information from the hacker less than twenty-four hours later.

Moreover, the government acknowledged that it knew months before Mr. Segal's arrest that its witnesses were receiving confidential e-mails involving Near North and Segal from a purportedly "unknown" source. At least one hacked e-mail was forwarded by a government witness directly to an FBI agent's personal e-mail address shortly after Mr. Segal's arrest. It is clear that there were frequent communications between the witnesses and the FBI or other government personnel. It is equally clear that, despite the government's agreement to "open-file" discovery in this case, the defense has not been provided with contemporaneous memoranda of key communications between the FBI (or other government personnel) and the witnesses who were receiving the stolen information. Either there are no contemporaneous records by the government documenting what were clearly critical and highly confidential communications being sent to its witnesses, or those materials have been withheld from discovery to date. The defense has vigorously pursued this information in numerous discovery conferences, correspondence, and other exchanges with the government. In one instance, the Government supplied a recently-written 302 concerning a ten-month old key conversation between the government and one of its cooperating witnesses about the witness' supposed non-involvement with hacked materials. In other instances, the defense now has obtained evidence of communications between the government's witnesses and the FBI at times coinciding with the hacker's intrusions into files of Mr. Segal and Near North. In still another instance, the defense

gathered evidence from a third party reflecting the forwarding of hacked information from a government witness to the FBI via the agent's home e-mail, but the government has not yet produced any 302 or other contemporaneous memorialization of this communication. Based on this less-than-complete record of the government's communications with its witnesses, the defense cannot tell without a hearing how much additional hacked information the witnesses passed on to the government, and what level of knowledge the government possessed about the illicit nature of the material.

Consequently, Mr. Segal seeks the aid of this court in holding an evidentiary hearing to get at the truth regarding the nature and extent of the government's receipt and awareness of the stolen materials provided to it by its cooperating witnesses. For these and other reasons, described in more detail below, Mr. Segal respectfully asks that this Court hold an evidentiary hearing to determine whether the government's witnesses were acting as agents of the government when they solicited and received information that had been stolen from Mr. Segal and Near North, and to then fashion an appropriate remedy once Mr. Segal has established that his constitutional rights have been violated.

## **II. LEGAL FRAMEWORK FOR ANALYSIS**

The Fourth Amendment to the United States Constitution mandates that "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The Fourth Amendment applies not only to searches performed by government officials, but extends to searches by private parties if the private party is acting as an "instrument or agent" of the government. *See United States v. Crowley*, 285 F.3d 553, 558 (7th Cir. 2002); *United States v. Shahid*, 117 F.3d 322, 325 (7th Cir. 1997).

Two critical factors in determining whether a private party has acted as an "instrument or agent" of the government are: 1) whether the government knew of and acquiesced in the private

party's intrusive conduct; and 2) whether the private party's purpose for conducting the search was to assist law enforcement efforts or to further his or her own ends. *See Crowley*, 285 F.3d at 558; *Shahid*, 117 F.3d at 325; *United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987). The Court may also consider whether the private party acted at the request of the government and whether the government offered the private party a reward. *Shahid*, 117 F.3d at 325; *United States v. McAllister*, 18 F.3d 1412, 1417-18 (7th Cir. 1994). The analysis of whether a private party acted as an "instrument or agent" of the government is made on a case-by-case basis and in light of all the circumstances. *United States v. Koenig*, 856 F.2d 843, 847; *Feffer*, 831 F.2d at 739. The movant has the burden of proving by a preponderance of the evidence that the private party was acting as an instrument or agent of the government. *Shahid*, 117 F.3d at 325; *United States v. Feffer*, 831 F.2d 734, 739 (7th Cir. 1987).

The defendant need not prove that the government explicitly asked the private party to conduct a search on its behalf, nor must a defendant present "clear" evidence that the private party acted as an agent, or even that the government acted improperly. *United States v. Stein*, 322 F. Supp. 346, 348-49 (N.D. Ill. 1971)(despite no "clear" evidence that the private party acted as the government's agent and no finding that the government acted improperly, court granted defendant's motion to suppress documents allegedly stolen by a private party who shared the defendant's office; because the government displayed "a clear pattern . . . to procure the cooperation of [the private party]," the court had "ample reason to believe that [the private party] thought the government would reward him for turning over [the] records," and the government was not "totally divorced" from the gathering of the stolen information); *Knoll Assocs., Inc. v. Federal Trade Comm.*, 397 F.2d 530, 535 (7th Cir. 1968)(where evidence demonstrated that an employee stole documents from his employer, and that the FTC knew of the theft but nonetheless

accepted and used the documents against the defendant in an FTC hearing, court found that the FTC violated the Fourth Amendment and suppressed evidence). Nor can the government avoid the Fourth Amendment's reach by turning a blind eye to illegal private searches by cooperating witnesses. *See United States v. Mekjian*, 505 F.2d 1320, 1328 (5th Cir. 1975) ("If government officials were aware, or should have been aware, that [the witness] was removing and copying records for [the government's use], [the government] will not be permitted to stand by or blink [its] eyes and accept the benefit of her activities").

Where, as here, resolution of factual issues is necessary in deciding whether evidence was obtained in violation of the Fourth Amendment, courts should conduct an evidentiary hearing. *See United States v. Sims*, 879 F. Supp. 883, 888 (N.D. Ill. 1995) (quoting *Nechy v. United States*, 665 F.2d 775, 776 (7th Cir. 1981)). The party requesting the evidentiary hearing must show that there are disputed issues of material fact necessitating a hearing. *Sims*, 879 F. Supp. at 888. As long as the factual issues presented are "definite, specific, detailed, and nonconjectural," an evidentiary hearing is justified. *Id.* (quoting *United States v. Hamm*, 786 F.2d 804, 807 (7th Cir. 1986)). Based on the factual issues described in more detail in the following section, an evidentiary hearing should be granted here.

### III. FACTUAL DISCUSSION

#### A. **A Computer Hacker Repeatedly Stole Massive Amounts of Confidential, Privileged and Proprietary Information From Mr. Segal and Near North Before and During the Government's Investigation of Mr. Segal.**

David Cheley<sup>2</sup> worked at Near North at the same time that the government's key witnesses were high-level executives there. Mr. Cheley started at Near North as a contractor in 1999. He later became a Near North employee, and worked in the company's information

---

<sup>2</sup> Mr. Cheley is a named defendant in the related civil suit pending in Cook County Circuit Court, and has been publicly identified in various filings and articles relating to that action.

technology ("IT") department from approximately January 2001 until August 15, 2001, when Near North terminated his employment. Within a week, Mr. Cheley began working for an IT consulting company, and was quickly assigned to a major financial and insurance company with offices in suburban Chicago ("Company"). Mr. Cheley worked at Company from approximately August 20, 2001 until April 24, 2002, when he was discharged from his engagement as a result of Near North exposing his hacking activity.

In March of 2002, several weeks after Mr. Segal's arrest and amid a flurry of grand jury and government investigative activity, suspicion arose at Near North that someone was illegally accessing its computer network, including its e-mail. To confirm this suspicion, Near North developed a monitoring program that identified all unauthorized intrusions into its e-mail network, including the Internet Protocol (or "IP") address of the intruder. On April 17, 2002, Near North put the monitoring program into place. Within an hour of its installation, the monitoring program detected several intrusions. Near North traced these intrusions to a single IP address at Company, where Mr. Cheley was working as a consultant. Two days later, NNIB detected intrusions from a second IP address that Mr. Segal later determined to be Mr. Cheley's home internet connection.

Near North scheduled a meeting with Company, and on April 23, 2002, representatives of Near North and Company met to discuss the hacking activity. After some internal investigation, Company confirmed to Near North that Mr. Cheley had repeatedly accessed the Near North system through Company's network. Company's records indicated that, between March 12 and April 24 alone, Mr. Cheley recorded 14,500 "hits"<sup>3</sup> on the Near North network, including more

---

<sup>3</sup> As counsel understands it, a "hit" refers to any type of selection or "click" that Mr. Cheley made while within Near North's network. For example, while Mr. Cheley was invading Mr. Segal's e-mail in-box, a "hit" would be generated every time Mr. Cheley clicked on a particular e-mail to view the message. If Mr. Cheley then clicked the "Back" button to return to Mr. Segal's in-box, this would generate another "hit." Scrolling through a particular e-mail or copying and pasting a particular e-mail, however, typically does not generate a "hit."

than 10,000 hits from a laptop computer that Mr. Cheley maintained at Company. In addition to his laptop, which he used for 80% of the hacking activity, Mr. Cheley also used at least three Company desktop computers to hack into Near North. Although the three Company desktops comprised only approximately 20% of the hacking activity, computer forensic analysis indicated that the desktops contained over one thousand hacked e-mails, many of which contained Mr. Segal's attorney-client privileged communications and proprietary business information. To facilitate his hacking, Mr. Cheley used several unauthorized devices at Company, including his own laptop computer, a CD-ROM "burner," and an ethernet hub.<sup>4</sup> Mr. Cheley used four separate e-mail vendors and at least five different e-mail aliases to transmit the information he hacked from Mr. Segal and Near North to key government witnesses and others.<sup>5</sup>

On April 24, 2002, Company confronted Mr. Cheley about his hacking activity and terminated his engagement with Company. In a four-page handwritten confession, Mr. Cheley admitted to accessing Near North's network from Company. (Ex. 2.) Mr. Cheley told Company's investigators that he hacked into Near North's system "at least twice a day" during his eight months of employment at Company. (Ex. 2.) Based on Near North's internal investigation and evidence gathered pursuant to trial subpoenas, Mr. Cheley also repeatedly

---

<sup>4</sup> A CD ROM "burner" is the informal name for a recording device that can copy data onto a CD, or compact disc. By using a CD ROM "burner," one can copy extremely large amounts of information onto a CD, and then physically send the CD to another individual, without ever creating an electronic trail of transmitting the information to another individual. One CD-ROM can hold around 650 megabytes, or the equivalent of 450 floppy disks. An ethernet hub is a device that allows an individual to split his or her network connection among multiple computers. An ethernet hub allowed Mr. Cheley to have simultaneous access to Company's network from both his laptop computer and a desktop computer.

<sup>5</sup> When Mr. Cheley transmitted stolen information to government witnesses via e-mail, he used several "alias" internet e-mail addresses, most beginning with the name "Lisa." From October 1, 2001 until December 28, 2001, Mr. Cheley transmitted information under the pseudonym "Lisa Chen" and the internet e-mail address squid7811@yahoo.com. Between December 7, 2001 and February 8, 2002, Cheley used the name "Lisa Rasmussen" and the internet e-mail address lisa90111@excite.com to transmit stolen information. Between February 28, 2002 and March 20, 2002, Cheley sent hacked information under the alias "Lisa Fisher" and ih8sno18@hotmail.com. According to the internet usage activity data from the desktop hard drives that Mr. Cheley used at Company, Mr. Cheley used all of the above internet e-mail addresses, as well as 1971@license71.com, dcheley@earthlink.net, and dcheley@hotmail.com.

invaded Near North's network from an IP address traced to his home and his home telephone line. During many of his intrusions, Mr. Cheley had unfettered administrative access to Near North's network, including employees' e-mail, Near North's financial and accounting systems, customer files and correspondence, and Near North's file server. Mr. Cheley also used his administrative access to stay up-to-date on Near North's user password list, and he also had the ability to create, delete, and/or modify files. Indeed, as Cheley himself bragged to a former colleague shortly before Near North detected his hacking, "I can pretty much do anything on the [Near North] network."<sup>6</sup> (Ex. 3).

Following its meeting with Company on April 23, 2002, Near North requested that Company copy the hard drive in Mr. Cheley's laptop computer that was used for the majority of the hacking activity. Unfortunately, neither Company nor the government ever seized or replicated the laptop hard drive before Company terminated Mr. Cheley, thereby letting crucial forensic data get away.<sup>7</sup>

Although Mr. Cheley often forwarded stolen information electronically during his intrusions, he also appears to have printed hardcopies of the hacked material and maintained files for it. For instance, in the same e-mail referenced in footnote 6, Mr. Cheley notes to his former Near North colleague: "I have a large file of NNNG stuff that would surely cause major problems for the company . . . I'll scan this stuff in when I get some time and send it to you."

---

<sup>6</sup> To illustrate Mr. Cheley's focus on issues relevant to this case and the depth of his hacking, one need not look further than an e-mail sent by Cheley to a former Near North colleague. For instance, shortly after this former colleague was terminated by Near North in March 2002, Mr. Cheley e-mailed him, boasting about having accessed Near North's "financial records" and then explicitly referring to Near North's premium fund trust account, a regulatory issue that has long been the centerpiece of the government's case against Mr. Segal. (Ex. 4.)

<sup>7</sup> As explained more fully below, to the best of the defense's knowledge, the government did not seize Mr. Cheley's laptop until several weeks later in June 2002. Mr. Cheley recently admitted that by June of 2002, he had already erased the hard drive on his laptop, completely eliminating critical forensic data that would likely have revealed, among other things, what information Mr. Cheley reviewed on Near North's network; which documents or files he cut and pasted; to whom he forwarded that information; the date and time of forwarding; the location from which he forwarded the information, such as Company, his home, or from some other location; and whether he created, destroyed, or altered any documents, files, or financial records on Near North's system.

(Ex. 4.) Furthermore, Mr. Cheley also refers on more than one occasion to sending information to his former Near North colleague through the post office.

**B. The Government's Principal Cooperating Witnesses Solicited and Received Stolen Information from Mr. Cheley.**

---

As one might expect from the frequency and the focused nature of his hacking, Mr. Cheley was not simply hacking Mr. Segal's e-mail and Near North's records out of idle curiosity. Recent discovery obtained from AON (a rival insurance brokerage that hired many of Near North's former employees who became the government's witnesses) in related civil litigation has revealed that beginning as early as October 2001 and continuing at least until March of 2002, Mr. Cheley repeatedly forwarded confidential and privileged communications stolen from Near North's network to various individuals, including government witnesses Matt Walsh and Dana Berry, both of whom left Near North in the summer of 2001 to join AON. Moreover, the AON e-mails demonstrate that Messrs. Walsh and Berry were not the only government witnesses who received hacked information from Mr. Cheley. Indeed, in two separate e-mails to Mr. Walsh dated September 21, 2001, Mr. Cheley admits to having already transmitted information to Jeff Ludwig, another government witness and former Near North executive who, like Mr. Walsh and Mr. Berry, joined a competitor (not AON) immediately following his employment with Near North. (See Ex. 5.) (In late August 2001, Near North had voluntarily disclosed issues relating to its PFTA to the Illinois Department of Insurance. This self disclosure occurred more than four months before Mr. Segal's arrest, which was the first



overt indication of the federal government's investigation.<sup>8</sup>) Mr. Cheley advised Mr. Walsh that Mr. Ludwig "seemed to appreciate" the information that Mr. Cheley provided.<sup>9</sup>

In the days leading up to Mr. Cheley's transmission of stolen information to government witnesses, Mr. Cheley and Mr. Walsh had several communications by phone and by e-mail. These communications provide compelling evidence that Messrs. Walsh and Berry knew exactly how Mr. Cheley was obtaining confidential and privileged information about Mr. Segal and Near North. For instance, on September 21, 2001, at 12:56 p.m., Mr. Cheley e-mailed Mr. Walsh at his AON e-mail address, stating "I may have some information you might be interested in so please let me know if this is your e-mail address." (Ex. 5.) At 1:23 p.m., Mr. Walsh confirmed for Mr. Cheley that he had the correct AON e-mail address, and then made a joking reference to a technical computer program manual that Mr. Cheley and Mr. Walsh discussed while working at Near North.<sup>10</sup> (Ex. 6.) At 1:57 p.m., Mr. Cheley responded with the following:

I called Jeff [Ludwig, another government witness] a couple of weeks ago and passed some info to him and he was appreciative. I am guessing based on what I've read that you, Tim [Gallagher, another government witness], and Dana [Berry, another government witness] are not real happy with [Mr. Segal]. I am personally disgusted with what NN has done not only to me but to

---

<sup>8</sup> In Near North's forty-year history prior to its self-disclosure, no client or insurance company had ever filed a complaint against Near North with the Department of Insurance alleging unpaid premiums. Following Mr. Segal's arrest in January 2002, Near North instituted an independent five-member board of directors including, among others, Fred Foreman and Walter Stowe.

<sup>9</sup> Although the e-mails produced by AON demonstrate that the government witnesses solicited and received information that Cheley stole from Near North, those materials do not represent the entire universe of communications between Mr. Cheley and any government witnesses, or even the government witnesses employed at AON. In fact, analysis of the AON e-mails reveals that whatever source AON searched to produce the e-mails did not retain every e-mail communication between Mr. Cheley and Mr. Walsh's AON e-mail account. The forensic data contained on Mr. Cheley's laptop computer, which was apparently used to conduct 80% of his hacking activity, would have provided a more comprehensive picture of the communications between Mr. Cheley and the government witnesses. However, because that evidence was not promptly seized, Mr. Segal and Near North may never know the extent of communications hacked by Mr. Cheley, or to whom and when they were forwarded.

<sup>10</sup> The reference to the computer program manual demonstrates, at a minimum, that Mr. Walsh remembered at the time he received this e-mail that Mr. Cheley had been involved with the IT department at Near North.

the former management group.<sup>11</sup> Anyway, I don't want to go into details here as to what I have or can get and how I do it but if you're interested in knowing what Segal's plans are let me know a number to call." (Ex. 7.)

At 2:20 p.m. that same day, Mr. Walsh e-mailed his phone number to Mr. Cheley, indicating "I neglected to give you my phone number in the event you want to reach me." (Ex. 8.) Less than a half-hour later, according to Mr. Cheley's cell phone records, Mr. Cheley called Mr. Walsh's number at 2:44 p.m. and talked for thirteen minutes. Five days later, on September 26, 2001, Mr. Walsh e-mailed Mr. Cheley and provided him with work phone numbers for Mr. Berry and Tim Gallagher, who, like Messrs. Walsh and Berry, left Near North in the summer of 2001 to work at AON. (Ex. 9.) In his September 26 e-mail, Walsh explained to Mr. Cheley how he could reach Mr. Berry and Mr. Gallagher, including a fax machine that Mr. Berry had in his private office:

I forgot to let you know that we are not in the Aon Center. We are at Aon Corporation [provides address]. The digs are decent and Dana [Berry] actually has a fax in his office. He got here first so he got first choice. That number is [provides fax number]. He and Tim send their regards. Dana's number is [provides number] and Tim's is [provides number]." (Ex. 9.)

Seconds after sending this e-mail to Mr. Cheley, Mr. Walsh forwarded the same e-mail to Mr. Berry and Mr. Gallagher. (Ex. 10.)

With the groundwork in place, Mr. Cheley did not wait long before forwarding stolen information to Mr. Walsh. For instance, on October 1, 2001, at 1:07 p.m., Mr. Cheley e-mailed Mr. Walsh a "zip file"<sup>12</sup> containing a privileged communication from Mr. Segal to his in-house

---

<sup>11</sup> Messrs. Walsh, Berry, Gallagher and Ludwig were all part of the "former management group" at Near North before leaving to join competitors.

<sup>12</sup> A zip file uses electronic compression technology to allow a person to forward multiple electronic files or e-mails in a single file. Hence, various files or e-mails can be "zipped up" into one file. Moreover, when transmitted, a "zip file" appears as a single attachment and conceals the text of the underlying files, until, of course, the recipient opens the zip file by "clicking" on it.

counsel at Near North regarding litigation strategy in connection with Near North's plans to pursue claims against Walsh, Berry, and Gallagher for breach of fiduciary duty, among other claims. (Ex. 11.)<sup>13</sup> At 2:22 p.m., Mr. Walsh replied "I received your note but none of the attachments functioned." (Ex. 12.) The next day, at 9:17 a.m. on October 2, 2002, Mr. Walsh informed Mr. Cheley that "someone else" was able to open the attachment. (Ex. 13.) Mr. Cheley intended to send Mr. Walsh two zip files, one small and one "bigger." Apparently realizing that he had not received the larger zip file, Mr. Walsh e-mailed Mr. Cheley and stated ". . . please resend with the original larger file." (Ex. 14.)

Mr. Cheley quickly complied with Mr. Walsh's request. At 10:16 a.m., Mr. Cheley e-mailed Mr. Walsh the "larger" zip file, which contained several dozen privileged and confidential communications involving Mr. Segal and Near North. One particular communication included in the "larger" zip file was a four-page single-spaced e-mail from Mr. Segal to his wife, which was transcribed and given to Mr. Segal's former criminal defense counsel. The e-mail contained confidential details about, among other topics, "trust accounting background issues" and the roles that various Near North consultants played in addressing those issues. Six minutes after receiving the large zip file, Mr. Walsh forwarded it to Dana Berry.<sup>14</sup> Throughout the month of October 2001, Mr. Cheley proceeded to send Mr. Walsh three additional zip files, including one titled "news\_2.zip" consisting entirely of eight privileged e-mails involving Mr. Segal and in-house or outside counsel. (Ex. 16.) The AON records also

---

<sup>13</sup> To avoid any risk of waiving the attorney-client privilege, Mr. Segal has included in the accompanying Appendix only the transmittal e-mail from Mr. Cheley to the government witnesses, and not any of the hacked e-mails contained in the various "zip files," many of which are privileged. The defense, of course, is prepared to submit to the Court *in camera* the contents of the zip files and any other privileged e-mails hacked and forwarded by Mr. Cheley, if the Court would like to review them.

<sup>14</sup> There is no doubt that Mr. Berry knew as much as Mr. Walsh about the illegal source of these documents. In addition to the above instances where Mr. Walsh forwarded to Mr. Berry information about Mr. Cheley, Mr. Walsh also did a mass forwarding of his e-mail correspondence with Cheley to Mr. Berry on October 2, 2001 at 10:03 a.m., thirteen minutes before Mr. Cheley sent the "larger" zip file. (Ex. 15.)

reveal that Mr. Cheley forwarded hacked information to Mr. Walsh in December 2001 and February 2002. Although Mr. Segal's investigation is ongoing, it is virtually impossible without an evidentiary hearing to determine how much stolen information Mr. Cheley transmitted to the government's witnesses, including information transmitted by non-electronic means, such as telephone calls, in-person meetings, or the mail.

**C. At Least One Government Witness Attempted to Cover Up His Solicitation And Review of Stolen Information.**

---

Further demonstrating their knowledge that the hacked information had come from an illegal source, at least one government witness and Mr. Cheley exchanged multiple, transparent e-mail communications designed to "cover-up" their transmission and review of stolen information. For example, on October 2, 2001, after receiving two zip files from Mr. Cheley in the previous twenty-four hours and having just asked Mr. Cheley two hours earlier to "resend" a large zip file, Mr. Walsh disingenuously wrote the following to Mr. Cheley at 12:07 p.m.:

I did receive the instructions to delete the information sent, and will utilise [sic] it immediately. Thank you. **I recognise [sic] that these were sent in error and contain information that upon first glance I did not wish to receive and you did not intend to send. Hence, it has been deleted without any review.**

(Ex. 17.) Less than a day later, Mr. Cheley e-mailed Mr. Walsh another zip file containing privileged communications between Mr. Segal and Near North's in-house counsel. (Ex. 18.)

Another bogus cover-up effort is reflected in an e-mail dated February 9, 2002 from Mr. Cheley to Mr. Walsh. Since early October 2001, Mr. Cheley had been repeatedly forwarding zip files to Mr. Walsh containing privileged and confidential information about Near North and Mr. Segal. Mr. Cheley even forwarded such a zip file to Mr. Walsh on February 7, 2002. Then, two days later, Mr. Cheley e-mailed Mr. Walsh, and introduced himself as "Dave Cheley, formerly from NNNG," pretending as if they had not communicated in some time. (Ex. 19.) Based on

these two illustrations alone, any contention that the government's witnesses did not know that the information forwarded to them by Mr. Cheley had been stolen from Near North would defy belief.

Based on the witness statements produced by the government to date, the picture emerges that Mr. Cheley began supplying government witnesses with hacked information just before the witnesses began cooperating with the government against Mr. Segal. As stated above, Mr. Cheley and Mr. Walsh began corresponding via e-mail toward the end of September 2001, and, based on the evidence gathered to date, the first zip file that Mr. Cheley forwarded to Mr. Walsh at his AON e-mail address was dated October 1, 2001. (Ex. 11.) This corresponds closely with the date of the earliest witness statement produced by the government in this case: a 302 of an interview with "Source" (believed to be Matt Walsh) dated October 4, 2001. (Ex. 20.)

**D. Mr. Segal Needs an Evidentiary Hearing To Determine Whether Certain Witnesses Were Acting as Government Agents When They Solicited, Received, and Reviewed Material Stolen from Mr. Segal and Near North.**

As stated in Section II *supra*, to determine whether the government's witnesses were acting as agents of the government for purposes of the Fourth Amendment, this Court must consider, among other factors: (1) whether the government knew or should have known of the hacking activity based on its investigation and information supplied by its witnesses; (2) whether the government acquiesced in its witnesses' continued procurement of stolen information; and (3) whether the government's witnesses procured the hacked information to assist the government. Although resolution of these factual issues will require an evidentiary hearing and a fully developed factual record, Mr. Segal has ample reason to believe that, under this legal framework, the government's witnesses were indeed acting as government agents when they procured the stolen information.

**1. Mr. Segal Needs an Evidentiary Hearing To Determine Whether the Government Knew, Should Have Known, or Acquiesced in Its Witnesses' Procurement of Stolen Information.**

There can be no dispute that the government received at least certain pieces of stolen information from its witnesses. For instance, on February 8, 2002, shortly after Mr. Segal's arrest but before he faced any indictment, Walsh forwarded a hacked e-mail to the personal e-mail address of the lead FBI agent on Mr. Segal's case, [user name]@mindspring.com.<sup>15</sup> (Ex. 21.) In the e-mail, Matt Walsh wrote "as noted in the past, from time to time I receive these anonymously." *Id.* The text of Walsh's e-mail -- "as noted in the past" -- suggests that this was not the first time that Walsh told the government about receiving confidential or privileged e-mails from purportedly "anonymous" sources. (Of course, as explained above, the notion that the source of the stolen information was "anonymous" to Walsh is demonstrably false.) Moreover, the government has never produced to Mr. Segal's defense counsel the hacked communication that Walsh forwarded to the lead case agent on February 8, 2002, or any 302 memorializing Walsh's forwarding of that hacked information to the lead case agent, or any memorialization of Walsh's prior receipt of purportedly "anonymous" e-mails as Walsh claims to have "noted in the past."

In addition to the above e-mail, there are other instances tending to show that the government either knew or should have known that it was receiving stolen information from its witnesses. On September 17, 2002, approximately six weeks before the return of a superseding indictment in this case, outside criminal counsel for Near North (not Mr. Segal's personal counsel) met with the prosecution team in this case to discuss Near North's plan to file an

---

<sup>15</sup> To avoid public disclosure of the agent's personal e-mail account, the defense has redacted the user name portion of the e-mail address. In a recent discovery conference, the government has confirmed that the address to which Walsh directed his February 8, 2002 communication is indeed the personal e-mail address of the lead case agent in this investigation.

amended complaint in Cook County Circuit Court against various entities and individuals, including government witnesses Walsh, Berry, Gallagher, and Ludwig. The amended complaint added new allegations based on the hacking activity to existing allegations involving violations of employment contracts and breach of fiduciary duty. In an attempt to prevent any misconceptions about the suit, counsel for Near North gave the government a draft of the amended complaint before filing. At the meeting, the government voiced strong objections to Near North's allegation that the government's witnesses had conspired with Mr. Cheley to obtain stolen e-mails and other electronic information, and indicated that its own investigation had established no connection whatsoever between Mr. Cheley and the witnesses cooperating in the prosecution of Mr. Segal. (The government echoed these sentiments at a meeting with Mr. Segal's defense counsel approximately one month later.) The government further noted at the September 17 meeting that if Near North made allegations regarding a conspiracy between Cheley and the cooperating witnesses that the government believed to be false or without sufficient basis in fact, the government would take that into account in determining whether to name Near North as a RICO enterprise and whether to charge Near North in a superseding indictment.

On September 19, 2002, just two days after the aforementioned meeting with Near North's counsel, the lead case agent prepared a 302 of a conversation with Dana Berry. (Ex. 22.) The 302 indicates that Mr. Berry "advised that on or about March 4, 2002, he received an unsolicited e-mail from "Lisa Fisher" [as noted above, a David Cheley alias] that contained a privileged communication between Mr. Segal and Harvey Silets, Mr. Segal's criminal defense lawyer. March 4, 2002 was more than five weeks after Mr. Segal was arrested. According to the September 2002 302, Mr. Berry faxed to the lead case agent the e-mail from "Lisa Fisher," after

redacting the privileged communication between Mr. Segal and Mr. Silets. The unredacted portion of the e-mail states "here is another FYI on some of the plans . . . I have access to lots of interesting information and I want to make sure it gets to the right person." (Ex. 23.) While it appears, based on the date of the 302, that the lead case agent spoke to Mr. Berry about this stolen privileged document on September 19, 2002, it is not clear from the 302 whether the lead case agent also spoke to Mr. Berry at or around the time that Mr. Berry received the "unsolicited" e-mail on March 4, 2002, and if so, what protections the government put in place to prevent further intrusion into Mr. Segal's privileged communications with his criminal defense attorney. According to a filing in the related civil litigation, Mr. Berry's lawyer represented that Mr. Berry provided an allegedly redacted version of the March 4, 2002 e-mail "to the FBI upon its receipt." (Ex. 24, at 7.) Thus, based on this evidence and what the government has produced to Mr. Segal to date, Mr. Berry informed the government that he had received a plainly privileged e-mail between Mr. Segal and his criminal defense counsel and forwarded some version of the e-mail to the government upon receipt in March 2002, yet the government made no memorialization of this communication until more than six months later.

The lead case agent also wrote a 302 on January 6, 2003 based on a telephonic conversation with "Source," again believed to be Mr. Walsh. In this 302, the lead case agent stated that Mr. Walsh "*had previously related* that he had received unsolicited e-mails that contained what appeared to be e-mails of Michael Segal." (Ex. 25)(emphasis added). Again, the government has not produced any contemporaneous 302s or other memorialization of those instances where the witness "*had previously related*" that he received "unsolicited" e-mails. If confirmed at a hearing, the uncharacteristic lack of FBI contemporaneous documentation of



these discussions of stolen confidential and even privileged e-mails may well be probative of whether the FBI was aware that its witnesses were receiving stolen confidential information.<sup>16</sup>

In addition, back on October 31, 2001, another case agent, prepared a 302 memorializing a telephonic conversation with "Source" Matt Walsh.<sup>17</sup> (Ex. 26.) According to the 302, "Source" provided the government with a copy of an e-mail containing a message apparently sent to Near North employees generally "From the Desk of Mike Segal." (Ex. 27.) The e-mail was cut, pasted, and forwarded to at least two recipients. In the document obtained from Matt Walsh by another case agent, the names of the people who forwarded and received the e-mail are redacted, and the person who forwarded the message wrote: **"This fell off a truck into my e-mail."** The message that was stolen "From the Desk of Mike Segal" and obtained by the government is dated October 30, 2001, several months after Mr. Walsh left Near North, a fact well-known to the government by that time. Despite the obvious cause for suspicion, the 302 is silent as to how Mr. Walsh obtained the information, and the defense is unaware of any subsequent investigative reports detailing any government follow-up to its receipt of this apparently stolen e-mail.<sup>18</sup>

---

<sup>16</sup> As this motion and memorandum were being finalized for filing, the defense received additional information raising questions about whether the discovery provided to it pursuant to the represented "open file" is, in fact, complete, and whether FBI contacts with key witnesses were contemporaneously memorialized. The first 302 of ex-Near North employee and government witness Tim Gallagher which has been produced to the defense is dated July 12, 2002. This is more than five months after the searches at Mr. Segal's office and home, which occurred on the same day as Mr. Segal's arrest, January 26, 2002. Very recently, the defense has received phone records indicating that Mr. Gallagher's cell phone connected to the FBI main number or to what the defense believes to be an FBI agent's cell phone number approximately 66 times before July 12, 2002. The calls begin in September 2001, more than nine months before the first memorialization of contact with Gallagher, and approximately four months before the searches and arrest.

<sup>17</sup> Like the 302 dated October 4, 2001, this 302 again has the name "Matt" handwritten in the upper left-hand corner, referring to Matt Walsh.

<sup>18</sup> From the redacted/blacked-out version of the e-mail attached to the October 31, 2001 302, the defense is unable to determine whether the e-mail was hacked from Near North's system or forwarded by an employee who had legitimately received it, or whether it was transmitted by Mr. Cheley or some other person.

Finally, Mr. Segal has reason to believe that at least one other conversation took place between the lead case agent and Mr. Walsh regarding Mr. Walsh's receipt of "unsolicited" e-mails. After the aforementioned September 17, 2002 meeting between the government and counsel for Near North, the two sides attended a follow-up meeting on September 23, 2002 where they discussed whether witnesses cooperating in the investigation and prosecution of Mr. Segal had received any confidential or privileged communications regarding Mr. Segal or Near North-related entities from a third party. At the September 23, 2002 follow-up meeting, the lead case agent indicated to Near North's counsel that, in approximately October 2001, Mr. Walsh had called the lead case agent and said that Walsh had received an unsolicited e-mail from an unknown third party that contained confidential Near North information. The lead case agent indicated that he had told Mr. Walsh to call his civil attorney. Despite the obvious importance of such a conversation, the government has not produced any memorialization of the conversation, contemporaneous or otherwise, or any record of the government's direction to its witness "to call his civil attorney." Nor has the government provided any contemporaneous record evidencing that it admonished its witnesses not to procure, accept, or review stolen confidential or privileged material regarding Mr. Segal or Near North.

**2. Mr. Segal Needs an Evidentiary Hearing To Determine Whether the Government's Witnesses Procured the Stolen Information To Assist the Government.**

Mr. Segal has compelling evidence, including an open-court admission, to show that the government witnesses who solicited and received the hacked information did so to assist the government. Mr. Segal also has evidence showing that the government had reason to know that its witnesses stood to reap substantial commercial and personal benefit by cooperating with the government and by providing information to the government, especially if such action led to the destruction of Near North as a competitor.

First and foremost, cooperating witnesses Walsh, Berry, and Gallagher no longer contest that they received stolen Near North property from Cheley. Instead, they have resorted to a tellingly brazen “defense” in the civil case that is central to this motion in many respects. At a discovery conference in the civil case last month, the cooperating witnesses’ attorney, Eric Brandfonbrener, represented to the court: “We’re not using these e-mails except in connection with our cooperation with the government.” (Ex. 1.) Mr. Brandfonbrener further stated that “we’re not using these e-mails for any purpose, and . . . these e-mails are only going to the FBI.” *Id.* This admission, by itself, is enough to justify an evidentiary hearing.

The government’s defensive attitude toward the civil suit brought by Near North as a result of the hacking activity has also inured to the benefit of the cooperating witnesses. From the moment the company showed the government a draft of the amended civil complaint, the government vehemently insisted that there was no connection between its witnesses and Mr. Cheley’s hacking activity. Moreover, the government’s expressed view that Near North could face indictment or be named as a RICO enterprise if it pressed its rights in the civil suit further protected its witnesses. Near North’s counsel made it clear to the government that either the naming of Near North as a RICO enterprise in Mr. Segal’s case or the indictment of Near North itself would likely result in deleterious, even disastrous impacts to Near North’s business and to its approximately 850 employees. Near North filed an amended civil complaint adding Mr. Cheley and others to its case against the government witnesses. The government superseded with RICO charges against Mr. Segal only weeks later, naming Near North as a RICO enterprise and alleging that Mr. Segal furthered the alleged enterprise by purportedly engaging in “retaliatory litigation.” The witnesses have derived substantial benefit from this undermining of Near North’s civil hacking suit, especially after the government identified the hacking suit in the

bill of particulars as the sole instance of allegedly "retaliatory litigation," which the government somehow construes to be part of its charge in this case.<sup>19</sup>

In other instances, the cooperating witnesses have apparently leveraged their advance knowledge regarding the government's investigation of Mr. Segal to persuade Near North employees or personnel to leave Near North in favor of the witnesses' employer. Indeed, at least one Near North business partner has indicated that, in the course of Messrs. Berry and Walsh urging him to cut ties with Near North and to come work for their employer, the government's witnesses told him that the FBI would soon contact him, and then, sure enough, that business executive received a call from the FBI shortly thereafter.<sup>20</sup>

The attempts by government witnesses to exploit the government's actions against Mr. Segal began almost immediately. On the day of Mr. Segal's arrest, a Saturday, and before any known public disclosure of the arrest, employees of Mr. Ludwig's employer, including Mr. Ludwig's boss, called at least two employees of Near North to inform them that their "boss" had just been arrested.

---

<sup>19</sup> In addition to the government's negative characterization of the civil suit, the witnesses have also benefited from the government's failure to charge Mr. Cheley or others to whom he sent stolen information with any offense, well over a year after Cheley confessed in writing to hacking into Near North's network "at least twice a day" over an eight-month period. Near North has promptly and fully cooperated with law enforcement authorities in an effort to bring Mr. Cheley to justice. As soon as it received confirmation that Mr. Cheley was the perpetrator, Near North immediately reached out to state law enforcement agencies in both Lake and Cook counties. As discussions between Near North and the state's attorney offices continued, the federal government somehow became involved in the Cheley investigation and, in May 2002, all investigative efforts by state law enforcement agencies ceased. Having taken control of the hacking investigation to the exclusion of state authorities, the federal government's investigation of Mr. Cheley has been apparently proceeding at a glacier-like pace. For example, despite knowledge of Mr. Cheley's hacking no later than early May 2002, and the government's receipt on May 17, 2002, of the desktop hard drives that Mr. Cheley used while working at Company, it appears to the defense that the FBI waited several weeks before securing Mr. Cheley's laptop computer, the very device through which Mr. Cheley likely conducted 80% of his hacking activity. Not surprisingly, by this late date, Mr. Cheley's laptop had already been wiped clean, thereby eliminating an enormous potential amount of critical forensic evidence. Despite repeated requests to the prosecution team handling Mr. Segal's case and to the prosecutor handling the Cheley investigation, the defense has received no discovery from the government regarding the hacking investigation.

<sup>20</sup> Allen Kaercher owned an insurance agency in Nevada that merged with Near North in 1999. Mr. Kaercher met with Matt Walsh and Dana Berry in Las Vegas in November 14, 2002, and they advised Mr. Kaercher at that time that he would soon receive a call from the FBI. (Ex. 28.) On November 15, 2002, Mr. Kaercher received a call from the FBI. *Id.* The government has not produced to the defense any memorialization of the FBI's contacting Mr. Kaercher on November 15, 2002.

There is good reason to believe that the government was well aware that its witnesses stood to benefit commercially from the government's arrest, indictment, and re-indictment of Mr. Segal. The government appears to have facilitated their witnesses' receipt of certain court filings that the witnesses have in turn used to their competitive advantage. For example, recent discovery in the civil suit reveals that on November 1, 2002, the same day that the superseding indictment was entered on the Court's docket (the superseding indictment was returned on October 31, 2002), an unsigned copy of the superseding indictment was faxed from the United States Attorney's office to an unknown destination at 11:40 a.m. At 2:26 p.m., the same document, containing the fax line from the U.S. Attorney's office, was faxed again from a number belonging to Eric Brandfonbrener, the lawyer for government witnesses Berry, Walsh, and Gallagher. Then, at 3:23 p.m., the same document, bearing the fax numbers of Mr. Brandfonbrener and the U.S. Attorney's office, was faxed from Dana Berry's private fax line at AON. As noted earlier, the superseding indictment contained a racketeering charge, named Near North as a member of the RICO enterprise, and accused Mr. Segal of filing "retaliatory litigation." Although the superseding indictment is admittedly a public filing and would have been available to the witnesses had they sought a copy from the clerk's office, the fact that the government appears to have faxed an unsigned copy of it to counsel for its key witnesses, the same day the indictment was entered on the Court's docket, demonstrates the government's likely awareness that its witnesses expected to and did obtain a commercial advantage from supplying information to the government which the government in turn used in the indictment and prosecution of Mr. Segal.<sup>21</sup> Thus, the potential for personal benefit to the government's

---

<sup>21</sup> The government's witnesses also appear to have attempted to derive substantial commercial benefit in their competition with Near North and Mr. Segal by aggressively spreading word of Mr. Segal's arrest to the media. Mr. Walsh's cell phone records indicate that on Friday, January 25, 2002, Mr. Walsh called a cell phone number, believed to belong to the lead case agent on Mr. Segal's case, four times, the last call occurring at 7:39 p.m., and then called Dana Berry's cell phone number bright and early at 4:49 a.m. on January 26, 2002, the day of Mr.

witnesses from passing on to the government stolen confidential and privileged material of Mr. Segal should have been very clear to the government.

All of these benefits are, of course, in addition to the favorable treatment that the cooperating witnesses likely received from the government, including but not limited to freedom from prosecution.<sup>22</sup>

#### IV. CONCLUSION

Mr. Segal seeks an evidentiary hearing to get at the truth of exactly what hacked and otherwise stolen material was received by the government witnesses; what the government knew (or should have known) about the information and about its witnesses' involvement with the hacking activity; and when and how the government learned about it. Through Rule 17(c) subpoenas and various correspondence and conferences with the government, Mr. Segal has vigorously pursued discovery of evidence relevant to this motion. However, due to certain limitations, including the destruction of critical evidence on Mr. Cheley's laptop computer and an apparently incomplete government file, Mr. Segal has been able to gather only the "tip of the iceberg" of relevant evidence. Nevertheless, based on this "tip" alone, Mr. Segal can already demonstrate that:

- Between August 2001 and April 2002, a former Near North employee repeatedly hacked into Near North's network both from his home and "at least twice a day" from his place of employment.

---

(continued...)

Segal's arrest. On Sunday, January 27, 2002, the day after Mr. Segal's arrest, Mr. Walsh's cell phone records indicate that he placed a one-minute call to what appears to be an FBI cell phone number at 1:54 p.m., and then, two minutes later at 1:56 p.m., he received an incoming call from an unidentified number that lasted for eight minutes. Very early the following day, on Monday, January 28, 2002, Mr. Walsh placed three phone calls to various Chicago television and radio stations beginning at 6:30 a.m. The defense understands that the government did not issue a press release regarding Mr. Segal's arrest until the afternoon of January 28, 2002.

<sup>22</sup> The government recently advised in a discovery conference that it will produce to the defense (as it is required to do) any such materials given to its witnesses, including but not limited to letters of immunity and non-target letters. As of the filing of this motion, the defense had not been provided with any such materials.

- The hacker repeatedly accessed employees' e-mail, including Mr. Segal's, and often had unrestricted administrative access to Near North's entire network, giving him the ability to review, modify, and delete files, including e-mail, financial records, and accounting records.
- Shortly before Mr. Walsh and certain fellow employees began cooperating with and volunteering information to the government, Mr. Walsh and the hacker began to communicate via e-mail and the telephone.
- In these communications, Mr. Walsh provided the hacker with his telephone number, and telephone numbers for fellow government witnesses Dana Berry and Tim Gallagher. Walsh also provided the hacker the number of a fax machine that Mr. Walsh clearly identified as being located in Mr. Berry's private office.
- Over the next six months, the hacker forwarded copious amounts of confidential, proprietary, and privileged communications to Mr. Walsh and/or Mr. Berry. Whatever hacked information Mr. Walsh received from the hacker, he forwarded it to Mr. Berry. The hacker forwarded more than a hundred of these communications, including an extremely sensitive four-page single-spaced e-mail ultimately provided to counsel, and an e-mail from Mr. Segal to Harvey Silets, his criminal defense counsel.

Mr. Segal also has substantial evidence tending to show that the government knew or should have known about its witnesses' solicitation and receipt of the stolen information, and that the government may have acquiesced in its witnesses' procurement of the information. For instance:

- The government acknowledged being told by Mr. Walsh in the fall of 2001 that Mr. Walsh had received a small number of confidential e-mails involving Near North and Mr. Segal from a purportedly "unknown" source. The government has not produced any contemporaneous record of this conversation.
- Source, believed to be Matt Walsh, produced an e-mail to the government in October 2001 written "from the desk of Mike Segal" that had been forwarded to at least two e-mail addresses, both of which are redacted. The text in one of the forwarded e-mails indicates that the e-mail from Mr. Segal "fell off a truck into my e-mail."
- In February 2002, Mr. Walsh forwarded a hacked communication to the personal e-mail address of an FBI Special Agent investigating Mr. Segal, and indicated "as noted in the past, from time to time I receive these anonymously." The government has not produced any written record of this exchange between Mr. Walsh and the Special Agent.
- In September 2002, two days after Near North's counsel met with the government to discuss the company's filing of a civil suit based on the hacking activity. Two days after

the government stated that its investigation had yielded no connection between the hacker and its witnesses, the government suddenly memorialized how Berry had received via e-mail from a purportedly unknown source, *more than six months earlier*, a privileged communication between Mr. Segal and his criminal defense counsel, Harvey Silets. Berry's attorney recently stated in a court filing that Berry gave the government some version of the e-mail upon receipt, but the government has not produced to the defense any contemporaneous record of this event.

- In January 2003, the government memorialized that Source, again believed to be Mr. Walsh, "*had previously related* that he had received unsolicited e-mails that contained what appeared to be the e-mails of Michael Segal." The government has not produced any contemporaneous memorialization of these "previous" instances.

As to whether the witnesses procured the stolen information to assist the government, Mr.

Segal can establish that:

- The attorney representing government witnesses Walsh, Berry, and Gallagher in related civil litigation recently stated in open court that his clients did not use the hacked e-mails "except in connection with our cooperation with the government."
- The witnesses have benefited from the government staunchly disavowing any connection between its witnesses and the hacker, and publicly characterizing Near North's civil litigation against its former employees, now government witnesses, as "retaliatory."
- The government appears to have faxed an unsigned copy of the superseding indictment that eventually reached its witness's place of employment, a rival company to Near North, the same day the indictment was entered on the Court's docket.
- After assuming control of the hacking investigation to the exclusion of state law enforcement agencies that Near North had originally contacted, the federal government is believed to have waited several weeks before seizing the hacker's laptop, through which approximately 80% of the hacking activity occurred. The government still has not charged the hacker with a single crime, more than thirteen months after he confessed to hacking into Near North "at least twice a day" over an eight-month period.

All of this evidence, at a minimum, creates genuine issues of fact as to whether the government knew or should have known that its witnesses were procuring hacked information, whether the government acquiesced in their procurement of hacked information, and whether the witnesses procured this information to assist the government or to further their own interests.

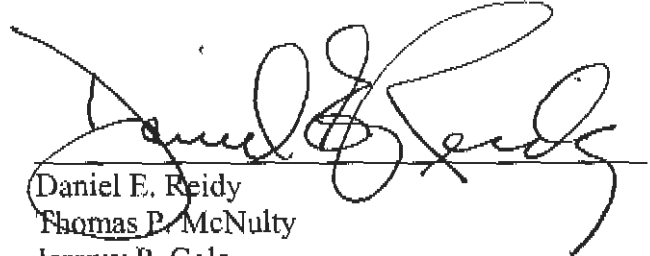
Therefore, Defendant Michael Segal respectfully requests that the Court hold an evidentiary



hearing that would allow him to prove by a preponderance of the evidence whether certain key witnesses were acting as agents of the government when they procured information that had been stolen from Mr. Segal and Near North, and, if so, to fashion an appropriate remedy for such a violation of Mr. Segal's constitutional rights.

Dated: June 10, 2003

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Daniel E. Reidy", is written over a horizontal line.

Daniel E. Reidy  
Thomas P. McNulty  
Jeremy P. Cole  
JONES DAY  
77 West Wacker Drive, Suite 3500  
Chicago, Illinois 60601-1692  
(312) 782-3939

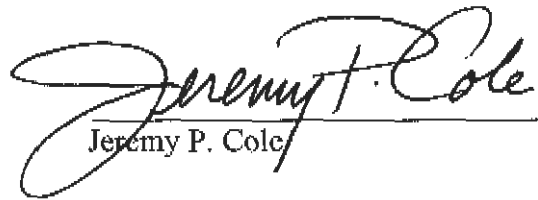
Attorneys for Defendant  
MICHAEL SEGAL

**CERTIFICATE OF SERVICE**

I hereby certify that we have caused a true and correct copy of Defendant's Motion for Evidentiary Hearing and Memorandum in Support and Defendant's Appendix of Exhibits in Support of Defendant's Motion for an Evidentiary Hearing to be served on:

Dean Polales, Esq.  
Virginia Kendall, Esq.  
William Hogan, Esq.  
Assistant U.S. Attorney  
219 South Dearborn Street, Suite 500  
Chicago, Illinois 60604

by messenger on June 10, 2003.

  
Jeremy P. Cole