

Case 5:08-cv-04052-JF Document 133 Filed 10/15/09 Page 63 of 70

Massachusetts	2	2	4	0	2	0	6
New York ED	2	2	4	0	2	0	6
New York SD	3	2	5	0	1	1	7
Texas ND	3	1	4	0	2	0	6
Virginia ED	4	2	6	1	2	1	10
Washington WD	3	2	5	0	2	1	8
Total	28	20	48	4	17	8	77

COMPONENTS

The program has 3 components: (1) **Prosecution**, (2) **Regional Prevention and Outreach** and (3) **Regional Training**.

1. Prosecution

- CHIP units will prosecute computer intrusions, copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components and other Internet crimes.

2. Regional Prevention and Outreach

- Prosecutors will work with CCIPS, the FBI and other agencies to establish good working relationships with the high tech community and to encourage victims of high tech crime to report such crimes to law enforcement.

3. Regional Training

- Cybercrime fighting requires special skills. CHIP units will receive the same high-level training provided by CCIPS, but will also be expected to develop and offer regional training programs to increase expertise among federal, state and local prosecutors.

- CHIP units will also be encouraged to send attorneys to work at CCIPS to train, and to call upon CCIPS for assistance in providing local training.

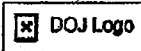
- More information on: CHIPs Program
- More information on: Attorney General Ashcroft's Remarks
- More information on: Law Enforcement Coordination for High-Tech Crimes
- More information on: Intellectual Property Policy
- More information on: Computer Crime Policy

Want to receive news of updates to the cybercrime.gov website?
Send a blank message to: cybercrime_subscribe@topica.com and we will add you to our email newsletter list.
(Mailing list privacy information)

Go to ... [CCIPS home page](#) || [Justice Department home page](#)

Updated page December 9, 2002
usdoj-orm/mis/krr

EXHIBIT “5”



Computer Crime and Intellectual Property Section (CCIPS)

Law Enforcement Coordination for High-Tech Crimes

- A. The Computer Hacking and Intellectual Property (CHIP) Program
 - B. High Technology Law Enforcement Training Opportunities
 - C. Coordination Between Law Enforcement and Industry
 - D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime
-

A. The Computer Hacking and Intellectual Property (CHIP) Program

In 1995, at the recommendation of the then-Computer Crime Unit (now the Computer Crime and Intellectual Property Section (CCIPS)), the Department of Justice created the Computer and Telecommunication Coordinator (CTC) Program to protect the nation's businesses and citizens from the rising tide of computer crime and intellectual property theft by designating one or more prosecutors in every U.S. Attorney's Office to be responsible for these issues. In 2001, following a successful model developed in the Northern District of California, the Department expanded the program in ten cities by designating Computer Hacking and Intellectual Property (CHIP) units. These units typically involved more prosecutors than under the CTC program and ~~were specifically charged with building relationships in-district with the FBI, other agencies, and the local high tech community.~~ New units were added frequently thereafter. In 2005, the CTC and CHIP programs were combined into a unified CHIP program. More information on the CHIP Program and historical information on the CTC program is available below.

- CHIPs Unit Established in the Eastern District of California United States Attorney Office (October 19, 2004)
- CHIPs Unit Established in the Eastern District of Virginia United States Attorney Office (January 14, 2002)
- CHIPs Unit Established in Central District of California United States Attorney Office (September 6, 2001)
- CHIPs Unit Established in Southern District of New York United States Attorney Office (September 5, 2001)
- CHIPs Unit Established in the Eastern District of New York (August 21, 2001)
- Fact sheet on Computer Hacking and Intellectual Property (CHIP) units (July 20, 2001)

- Attorney General Ashcroft's Speech Announcing Expansion of CHIP Program and Establishment of Nine New CHIP units (July 20, 2001)
- The Computer and Telecommunications Coordinator (CTC) Program, Stacey Levine, USA Bulletin (May 2001)
- CTC Responsibilities

B. High Technology Law Enforcement Training Opportunities

- Training Opportunities

C. Coordination Between Law Enforcement and Industry

Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue

On April 5, 2000, the Department of Justice hosted a Cybercrime Summit at Stanford Law School, titled "Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation," at which Attorney General Janet Reno and members of the Justice Department and other law enforcement agencies met with representatives of information technology and Internet companies. The main topic of the Summit was how to improve cooperation between law enforcement and industry in investigating computer network hacking. Linked below are the Attorney General's Opening Remarks from the Summit, as well as the Question & Answer session between industry representatives and the Attorney General.

- Opening Remarks of Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)
- Question and Answer Session with Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)

The Cybercitizen Partnership: Industry and Government Alliance

On March 15, 1999, Attorney General Janet Reno announced a new Cybercitizen Partnership, a new alliance between law enforcement and the technology community. The goal of the partnership is to coordinate the efforts of government, industry and the public to ensure public safety and responsible computer use. The partnership will also promote computer ethics and civic responsibility in the cyber age and aid law enforcement and industry in the battle against "on-line outlaws." The partnership will consist of three complementary segments. The first segment is a "good cybercitizenship" public awareness campaign. The second is a user-friendly computer and network security directory to help public and private sector organizations quickly find computer security resources. The third is an Information Security Professional fellowship program between industry and government that will raise the awareness levels of participants with respect to the views, perspectives and needs of their respective counterparts.

- Statement by Attorney General Janet Reno to Announce the Cybercitizen Partnership at the ITAA Policy Summit (March 15, 1999)
- ITAA and Attorney General Janet Reno Unveil New Tech Partnership (March 15, 1999)

D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime

Assistant Attorney General Michael Chertoff's Testimony Before the House Subcommittee on Crime

On June 12, 2001, Assistant Attorney General Michael Chertoff testified before the Members of the Subcommittee on Crime of the Committee on the Judiciary. In his statement he addressed the nature of cybercrime and the Department's current efforts to combat that problem.

- Text of Assistant Attorney General Michael Chertoff's testimony before the House Subcommittee on Crime of the Committee on the Judiciary (June 12, 2001)

Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute

On May 22, 2001, videotaped remarks by Attorney General John Ashcroft were presented before the first Annual Computer Privacy, Policy and Security Institute.

In his speech, the Attorney General addressed the Institute's concerns of computer security and threats to information assets and the means by which industry and law enforcement can work together in fighting cybercrime.

- Text of Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute (May 22, 2001)
- View Video Taped Remarks (21 Megabytes)
*Approximate download time: 56K Modem=55 minutes
- View Video Taped Remarks (13 Megabytes)
*Approximate download time: 56K Modem=35 minutes

**Note: the listed download times are estimated times under optimal conditions. Your actual download times may vary depending on your modem, internet traffic, and your internet connection type.*

Attorney General Reno's Address to the ITAA Cybercrime Summit

On June 9, 2000, Attorney General Janet Reno gave the keynote address at the ITAA Cybercrime Summit. In her speech, the Attorney General discussed the means by which industry and law enforcement can work together in fighting cybercrime. The text also includes the question and answer section.

- Text of Attorney General Reno's Keynote Address at the ITAA Cybercrime Summit (June 9, 2000)

Attorney General Janet Reno Testifies Before Senate Appropriations Committee

On Monday, February 16, 2000, Attorney General Janet Reno testified before the United States Senate Committee on Appropriations. Her testimony provided an overview of cybercrime and the challenges that it presents to law enforcement today.

- **Testimony by Attorney General Janet Reno before the United States Senate Committee on Appropriations (February 16, 2000)**

Attorney General Janet Reno Introduces Law Net Initiative

On January 10, 2000, Attorney General Janet Reno gave remarks before the National Association of Attorneys General in which she announced a new Law Net initiative. The Law Net will be a "strong, permanent network of federal, state and local computer crime experts to do the following: To share expertise and information technology, to assist each other 24 hours a day, seven days a week, around the clock, to prevent cybercrime wherever possible, and to bring those responsible for such crime, when it does occur, to justice; To work with industry, the academic world and privacy groups to build trust and to protect our privacy and the Constitutional rights of all Americans; And finally, to ensure that the Internet is a force that brings this world together and builds understanding across peoples and places and time.

- **Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of Attorneys General (January 10, 2000)**

Attorney General Janet Reno Addresses the High Technology Crime Investigation Association 1999 International Training Conference

On Monday, September 20, 1999, Attorney General Janet Reno addressed the High Technology Crime Investigation Association 1999 International Training Conference in San Diego, California. Her speech focused on the importance of interagency and state and federal law enforcement cooperation, as well as on the Department of Justice's policy position on encryption regulation.

- **Speech by Attorney General Janet Reno before the High Technology Crime Investigation Association 1999 International Training Conference (September 20, 1999)**

President Clinton Addresses National Academy of Sciences on Keeping America Secure for the 21st Century

On January 22, 1999, President William Jefferson Clinton addressed the National Academy of Science. His speech was titled "Keeping America Secure for the 21st Century." The speech he gave is available via the link below:

- **President Clinton's Speech to National Academy of Sciences (January 22, 1999)**

[Go to ... CCIPS home page](#) || [Justice Department home page](#)

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
26
27
28

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing:

**NOTICE OF MOTION AND MOTION TO STAY CIVIL ACTION PENDING
RESOLUTION OF CRIMINAL PROCEEDINGS; MEMORANDUM OF POINTS AND
AUTHORITIES; DECLARATION OF WILLIAM J. KOPENY AND BRIAN DUNNING
IN SUPPORT**

was filed with the Court's Electronic Filing System on October 15, 2009 and may be accessed electronically.

s/ Leo J. Presiado
Leo J. Presiado
Rus, Miliband & Smith, APC
2211 Michelson Drive, Seventh Floor
Irvine, California 92612
Tel: (949) 752-7100
Fax: (949) 252-1514
Email: lpresiado@rusmiliband.com
Attorneys for Defendants Thunderwood Holdings,
Inc., Brian Dunning and Briandunning.com

EXHIBIT “2”

1 DAVID R. EBERHART (S.B. #195474)
 2 deberhart@omm.com
 3 SHARON M. BUNZEL (S.B. #181609)
 4 sbunzel@omm.com
 5 COLLEEN M. KENNEDY (S.B. #227107)
 6 ckennedy@omm.com
 7 O'MELVENY & MYERS LLP
 Two Embarcadero Center, 28th Floor
 San Francisco, CA 94111
 Telephone: (415) 984-8700
 Facsimile: (415) 984-8701
 Attorneys for Plaintiff eBay Inc.

8
 9 **UNITED STATES DISTRICT COURT**
 10 **NORTHERN DISTRICT OF CALIFORNIA**
 11 **SAN JOSE DIVISION**

12 EBAY INC.,
 13 Plaintiff,

14 v.

15 DIGITAL POINT SOLUTIONS, INC.,
 16 SHAWN HOGAN, KESSLER'S
 17 FLYING CIRCUS, THUNDERWOOD
 18 HOLDINGS, INC., TODD DUNNING,
 19 DUNNING ENTERPRISE, INC., BRIAN
 20 DUNNING, BRIANDUNNING.COM,
 21 and DOES 1 - 10 and 12 - 20,

22 Defendants.

Case No. CV 08-4052 JF (PVT)

**SECOND AMENDED COMPLAINT
 FOR**

- (1) Violations of 18 U.S.C. § 1030
- (2) Violations of 18 U.S.C. § 1962(c)
- (3) Fraud
- (4) Violations of California Pen. Code § 502
- (5) Restitution and Unjust Enrichment
- (6) California B&P Code § 17200;

DEMAND FOR JURY TRIAL

22 For its Second Amended Complaint, Plaintiff eBay Inc. alleges as set forth below.
 23 The factual allegations set forth herein have evidentiary support or, to the extent they are
 24 contained in a paragraph made on information and belief, likely will have evidentiary
 25 support after a reasonable opportunity for further investigation or discovery.

PARTIES

- 27 1. At all times relevant herein, Plaintiff eBay Inc. ("eBay") was a corporation.
 28

SECOND AMENDED COMPLAINT
 CASE NO. CV 08-4052 JF (PVT)

1 organized and existing under the laws of the State of Delaware, with its principal place of
2 business in the State of California.

3 2. eBay is informed and believes and, on that basis, alleges that at all times
4 relevant herein Defendant Digital Point Solutions, Inc. ("Digital Point Solutions") was a
5 California corporation, sole proprietorship or other business entity, doing business in the
6 State of California. At various times relevant herein, Defendant Digital Point Solutions
7 may also have been known as and/or done business as "Data Point Solutions," "Digital
8 Point Solutions," and/or "Digital Point." Digital Point Solutions has succeeded to the
9 obligations and liabilities of any and all of such predecessor entities. At all times relevant
10 herein, Defendant Digital Point Solutions represented itself and held itself out to eBay as
11 an independent business entity with legal status separate from that of its individual
12 owner(s).

13 3. eBay is informed and believes and, on that basis, alleges that at all times
14 relevant herein Defendant Shawn Hogan was an individual residing and doing business in
15 the State of California and was the sole owner and/or sole proprietor of Defendant Digital
16 Point Solutions in any and all of its incarnations.

17 4. Defendants Digital Point Solutions and Shawn Hogan will be collectively
18 referred to herein as "DPS."

19 5. eBay is informed and believes and, on that basis, alleges that at all times
20 relevant herein Defendant Kessler's Flying Circus was a California general partnership
21 doing business in the State of California.

22 6. eBay is informed and believes and, on that basis, alleges that at all times
23 relevant herein Defendant Thunderwood Holdings, Inc. was a California corporation and
24 was a general partner of Defendant Kessler's Flying Circus.

25 7. eBay is informed and believes and, on that basis, alleges that at all times
26 relevant herein Defendant Brian Dunning was an individual residing and doing business in
27 the State of California and was the sole owner of Defendant Thunderwood Holdings, Inc.

28 8. eBay is informed and believes and, on that basis, alleges that at all times

1 relevant herein Dunning Enterprise, Inc., previously substituted for the fictitiously named
2 defendant Doe 11, was a California corporation doing business in the State of California
3 and was a general partner of Defendant Kessler's Flying Circus.

4 9. eBay is informed and believes and, on that basis, alleges that at all times
5 relevant herein Defendant Todd Dunning was an individual residing and doing business in
6 the State of California and was either a general partner of Defendant Kessler's Flying
7 Circus or held a controlling interest in Dunning Enterprise, Inc., which was a general
8 partner of Defendant Kessler's Flying Circus.

9 10. eBay is informed and believes and, on that basis, alleges that at all times
10 relevant herein Defendant BrianDunning.com was a website and/or business entity
11 through which Defendants Brian Dunning and/or Todd Dunning committed some or all of
12 the acts alleged herein.

13 11. Defendants Kessler's Flying Circus, Thunderwood Holdings, Inc., Dunning
14 Enterprise, Inc., BrianDunning.com, Brian Dunning, and Todd Dunning will be
15 collectively referred to herein as "KFC."

16 12. eBay is ignorant of the true names and capacities of defendants sued herein
17 as Does 1 through 10 and 12 through 20, inclusive, and therefore sues said defendants by
18 such fictitious names. eBay will amend this complaint to allege the true names and
19 capacities of said defendants when they are ascertained. eBay is informed and believes
20 and, on that basis, alleges that each of the fictitiously named defendants is responsible in
21 some manner to pay the obligations described herein, and that eBay's losses as alleged
22 herein were proximately caused by said defendants' conduct.

23 13. Unless otherwise specified, DPS, KFC and Does 1-10 and 12-20 will be
24 referred to collectively herein as "Defendants."

25 **JURISDICTION AND VENUE**

26 14. The Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331
27 and 1367.

28 15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b)(1),

1 1391(b)(2) and 1391(c), and 18 U.S.C. § 1965(a).

2 16. Pursuant to the User Agreements entered into by DPS and KFC, as
3 discussed in paragraph 26 *infra*, they have consented to the jurisdiction of and venue in
4 the Northern District of California. Specifically, under the User Agreements, the
5 Defendants have agreed that any claim or controversy at law or equity that arises out of
6 this Agreement or eBay's services must be resolved by a court located in Santa Clara
7 County, California.

8 **INTRADISTRICT ASSIGNMENT**

9 17. Assignment to the San Jose Division is proper pursuant to Local Rules 3-
10 2(c) and (e) because a substantial part of the events or omissions that give rise to eBay's
11 claim occurred in San Jose, Santa Clara County, California. eBay's corporate
12 headquarters are located in San Jose, Santa Clara County, California, and Defendants'
13 wrongful actions were specifically and purposefully directed at and intended to affect
14 eBay in San Jose, Santa Clara County, California as discussed in detail below.

15 **GENERAL ALLEGATIONS**

16 **eBay's Affiliate Marketing Program**

17 18. eBay offers to the public an online marketplace that enables trade on a local,
18 national and international basis. Through eBay's website, sellers may list items for sale
19 and buyers may bid on and purchase items of interest. eBay earns revenue when a seller
20 places an item for sale and when the item is sold. eBay may also earn revenue depending
21 on various features selected by the seller, *e.g.*, listing upgrades and photo displays.

22 19. eBay's Affiliate Marketing Program is designed to increase traffic to eBay's
23 website through the placement of advertisements for eBay on third-party websites. eBay
24 seeks to increase traffic to its site so that more people will be exposed to eBay's service
25 and begin using eBay to buy or sell goods, thereby generating revenue for eBay. The
26 persons and entities that advertise on behalf of eBay—whether on their own sites or on
27 sites of other third parties—are known as “affiliates.” eBay's Affiliate Marketing
28 Program is intended to compensate affiliates only when the advertisement in question

1 causes a user to take some action at eBay's site that directly provides revenue to eBay or
2 indicates that the new user is likely to take such an action in the future. Accordingly,
3 affiliates earn commissions payable by eBay under the Affiliate Marketing Program when
4 the following sequence of events occurs: (1) the affiliate publishes an eBay advertisement,
5 (2) a user clicks on the eBay advertisement and is directed to eBay's website (the
6 "Referred Visit"), and (3) that user subsequently engages in a commission-generating
7 event (a "Revenue Action"). Revenue Actions, include, by way of example: (1) becoming
8 a new, registered user of eBay within 30 days of the Referred Visit, or (2) purchasing an
9 item from a third-party seller on eBay within seven days of the Referred Visit. Because
10 compensation to the affiliate is tied to actions by the user, it is essential that eBay be able
11 to determine whether a Revenue Action occurred by virtue of the fact that the user was
12 referred to eBay by a particular affiliate's advertisement. eBay and/or Commission
13 Junction, Inc. ("CJ") tracks this information using information placed in the new user's
14 browser, as discussed below.

15 20. At all relevant times, eBay used the services of CJ, a subsidiary of
16 ValueClick, Inc., in administering the Affiliate Marketing Program. The relationship
17 between eBay and CJ was governed at all relevant times by various Advertiser Service
18 Agreements. Under those agreements, CJ was responsible for, among other things,
19 recruiting affiliates, tracking affiliate traffic, monitoring compliance by affiliates,
20 preventing and detecting fraudulent activity, and paying affiliates using funds remitted by
21 eBay.

22 21. eBay's obligation to pay commissions is tracked by matching a user's
23 Revenue Actions on eBay's site to the affiliate that directed the user to eBay. This
24 tracking is accomplished through the use of a digital tag called a "cookie" that is stored in
25 the user's web browser. Cookies are collections of data commonly used by websites to
26 store and associate useful information with a given user. Cookies typically store
27 information such as usernames, passwords, and user preferences for a particular user; that
28 information makes it more efficient for users to access web pages and provides a means

1 for websites to track and authenticate users. Cookies are placed or “dropped” in a user’s
2 browser by a website when that user visits the website.

3 22. In the case of eBay’s Affiliate Marketing Program, cookies are used to
4 confirm that a user was directed to eBay from a specific affiliate. When a user clicks on
5 an affiliate advertisement and is directed to eBay’s site, eBay’s site drops a cookie on the
6 user’s computer. That cookie identifies the site that referred the user to eBay and/or the
7 specific affiliate responsible for directing the traffic to eBay. If the user later engages in a
8 Revenue Action within the specified time period, eBay and/or CJ determines—based on
9 the data in the cookie—which affiliate, if any, should be credited with the referral and
10 receive the commission. If cookies from multiple affiliates are present on the user’s
11 computer, the affiliate identified in the most recent cookie dropped is credited with the
12 Revenue Action. If there is no qualifying cookie on the computer, then no affiliate is
13 credited. A substantial number of the Revenue Actions taken at eBay’s site are taken by
14 users who were not referred to eBay by any affiliate; consequently, no commission is
15 owed for those actions.

16 23. As part of the services it renders with respect to eBay’s Affiliate Marketing
17 Program, CJ pays affiliates on a periodic basis (usually monthly), with funds remitted by
18 eBay, based on the number of Revenue Actions taken by users referred by those affiliates.

19 The Fraudulent “Cookie Stuffing” Schemes.

20 24. “Cookie stuffing” is a term used to describe the forced placement of a
21 cookie on a computer, typically by causing a cookie from a particular website to be placed
22 on the user’s computer without the user knowing that he or she visited the website that
23 placed the cookie. DPS and KFC engaged in cookie stuffing intended to defraud eBay.
24 The allegations made on eBay’s information and belief set forth in paragraphs 25-34, 37-
25 41, and 47-60 below describing Defendants’ cookie stuffing schemes are based on eBay’s
26 analysis of the Defendants’ websites and/or technology and the way in which a user’s web
27 browser interacts with Defendants’ sites and/or technology, and on eBay’s analysis of
28 historical data relating to traffic purportedly driven to eBay by Defendants. Certain other

1 details regarding Defendants' cookie stuffing schemes are exclusively within Defendants'
2 control.

3 25. eBay is informed and believes and, on that basis, alleges that DPS and KFC
4 each accomplished their cookie stuffing through software programs and/or code that,
5 unbeknownst to the user, redirected the user's computer to the eBay website without the
6 user actually clicking on an eBay advertisement link, or even becoming aware that they
7 had left the page they were previously viewing. As a result, the eBay site would be
8 prompted to drop an eBay cookie on the user's computer even though the user never
9 clicked on an eBay advertisement or even realized that their computer had ever visited the
10 eBay site. DPS and KFC stuffed a large number of Internet users, with the expectation
11 and intention that some subset of those users would later come to eBay and take a
12 Revenue Action.

13 26. eBay is informed and believes and, on that basis, alleges that the software
14 programs utilized by each of DPS and KFC caused the user's computer to access eBay's
15 computers in an unauthorized way and/or to exceed the authorized access to eBay's
16 computers. Because DPS and KFC caused this access through and without the knowledge
17 or active participation of those users, the access of any such user's computer to eBay's site
18 is attributable to DPS and KFC. The only authorization given to the Defendants to access
19 eBay's site in any manner was by way of eBay's User Agreement. The User Agreement
20 was explicitly agreed to by the individual Defendants when they became registered eBay
21 users on the following dates: Shawn Hogan on May 17, 1999; Brian Dunning on
22 November 10, 2000; and Todd Dunning on May, 21, 2003. The remaining named
23 Defendants, Digital Point Solutions, Kessler's Flying Circus, Thunderwood Holdings,
24 Inc., Dunning Enterprise, Inc. and BrianDunning.com, were on constructive and/or actual
25 notice that the User Agreement governed their access to eBay's website, based on the
26 explicit agreement of their owners/principals to the terms of the User Agreement, as well
27 as eBay's display on its website at all relevant times of the statement that use of the
28 website constitutes acceptance of the User Agreement. Defendants' access to eBay was

1 unauthorized by, and violated, the terms of the User Agreement because it occurred solely
2 to force the dropping of the eBay cookie and thereby wrongfully access eBay's computer
3 servers. Each of the causes of action set forth herein arises out of those violations of the
4 User Agreement.

5 27. eBay is informed and believes and, on that basis, alleges that once the
6 cookie was stuffed on the user's computer by one or more of the Defendants, any future
7 Revenue Actions initiated by that user when the user later visited eBay intentionally, and
8 not as a result of any advertisement placed by Defendants, appeared to be eligible for
9 commissions payable to one of the Defendants (provided those actions took place within
10 the prescribed periods of time). Hence DPS or KFC would receive payment for actions by
11 users who had not been referred to eBay by Defendants' advertisements, thereby injuring
12 eBay.

13 28. eBay is informed and believes and, on that basis, alleges that after DPS
14 and KFC independently began their cookie stuffing schemes, they communicated with
15 each other regarding those cookie stuffing schemes. Those communications between
16 DPS and KFC included, but were not limited to attempts by KFC to improve its
17 software and/or otherwise improve the effectiveness of its cookie stuffing scheme in
18 order to increase the amount of commissions that KFC could fraudulently obtain from
19 eBay, as well as efforts by DPS to prevent detection of the DPS cookie stuffing
20 scheme by eBay.

21 29. eBay is informed and believes and, on that basis, alleges that DPS and KFC
22 used certain technological measures to prevent eBay from discovering their wrongdoing.
23 At certain relevant times DPS and KFC used technology or technologies that would stuff
24 cookies on only those computers that had not been previously stuffed by that Defendant.
25 The purpose of this action was to avoid discovery by eBay and/or CJ of evidence of
26 stuffing—e.g., by directly observing repeated stuffing to a test computer, by discovering
27 that a single user had multiple cookies pointing to the same affiliate or by discovering that
28 there was an abnormal ratio of cookies placed by DPS and KFC to the Revenue Actions

1 attributable to users referred by DPS and KFC—and thereby conceal the schemes from
2 eBay’s and/or CJ’s monitoring activities. In addition, at certain relevant times DPS and/or
3 KFC used technology that would avoid stuffing cookies on computers that appeared to be
4 geographically located in San Jose, California (the location of eBay’s headquarters) or
5 Santa Barbara, California (the location of CJ’s headquarters). The purpose of this action
6 was to evade efforts by eBay and/or CJ to detect the cookie stuffing mechanism if they
7 attempted to observe the wrongdoing from their normal places of business.

8 30. eBay is informed and believes and, on that basis, alleges that DPS also used
9 at least one additional technological measure to conceal its wrongdoing: DPS used
10 images placed on web pages to effectuate its cookie stuffing scheme, and caused those
11 images to be so small that they were effectively invisible to the user and, accordingly,
12 difficult to detect.

13 31. eBay is informed and believes and, on that basis, alleges that KFC also used
14 at least one additional technological measure to conceal its wrongdoing: KFC used
15 JavaScript code contained in web pages to effectuate its cookie stuffing scheme, and
16 purposefully obscured the purpose and effect of that code so that, even when that code
17 was discovered, it was difficult to determine its actual effect. This caused KFC’s cookie
18 stuffing to be difficult to detect, whether by human or machine efforts.

19 32. eBay is informed and believes and, on that basis, alleges that in addition to
20 these technological measures, DPS and KFC each actively sought to prevent detection by
21 eBay and CJ by explicitly denying to eBay and/or CJ that any wrongdoing had occurred.
22 For example, when Shawn Hogan was contacted by CJ in connection with suspicions of
23 cookie stuffing by DPS, he attributed the suspicious activity to “coding errors,” which he
24 later purported to have “corrected.” Brian Dunning also gave false information to eBay in
25 response to questions about unusual activity regarding his account. Additional false
26 statements intended to conceal the cookie stuffing activity are set forth below in paragraph
27 60 and are incorporated herein.

28 33. As a result of the cookie stuffing schemes employed by DPS and KFC, DPS

1 and KFC accessed eBay's servers millions of times in an unauthorized manner that
2 violated the User Agreement and interfered with the proper working of those computers.
3 The majority of those acts of unauthorized access did not cause the improper payment of a
4 commission and did not involve the performance by CJ of any obligations under any
5 contract it had with any of the parties to this action. A minority, but economically
6 significant, of those acts of unauthorized access caused eBay to pay commissions (via CJ)
7 to each of DPS and KFC for a substantial number of Revenue Actions that were in no way
8 related to the legitimate referral of any user by either DPS's or KFC's advertisements and
9 for which neither DPS nor KFC were due compensation.

10 34. On January 4, 2008, CJ filed an action against Defendants Kessler's Flying
11 Circus, Brian Dunning and Todd Dunning for breach of contract and other claims based
12 on KFC's cookie stuffing scheme perpetrated against eBay. CJ sought to recoup
13 commissions it had paid to those Defendants for the month of May 2007, after eBay
14 discovered KFC's cookie stuffing scheme and refused to reimburse CJ for the unearned
15 commissions it had paid to those Defendants for the previous month. CJ's action was
16 recently settled on undisclosed terms, and a request for dismissal has been filed. eBay
17 was not a party to CJ's action, and had no opportunity to litigate any issue in the CJ
18 action. eBay does not seek recovery through this litigation of any of the monies sought by
19 CJ through its now-settled litigation against Defendants Kessler's Flying Circus, Brian
20 Dunning and Todd Dunning.

21 **FIRST CAUSE OF ACTION**

22 **(Violations of 18 U.S.C. § 1030)**

23 35. eBay realleges each and every allegation set forth in Paragraphs 1 through
24 34, inclusive, and incorporates them by reference herein.

25 36. Through their cookie stuffing schemes as described above, DPS and KFC
26 each knowingly, intentionally and with intent to defraud accessed eBay's computers
27 without authorization and/or exceeded their authorized access to eBay's computers in
28 order to further their fraudulent schemes.

1 37. DPS's and KFC's access of eBay's computers was unauthorized because the
2 only purpose of that access was to defraud eBay. In addition, Defendants' access of
3 eBay's computers was unauthorized and/or exceeded their authorized access, because
4 each Defendant was a registered eBay user and/or was bound by the eBay User
5 Agreement in effect at the time, as set forth in paragraph 26 above. The User Agreements
6 that bound each of the Defendants were substantially similar. The User Agreements (a)
7 prohibited the use of any "device, software or routine" to interfere with or attempt to
8 interfere with the proper working of the eBay site or any activities conducted on the eBay
9 site, and (b) required compliance with all applicable laws regarding the use of eBay's
10 servers.

11 38. The User Agreements were the only basis on which any Defendant had
12 authorization to access eBay's site. No agreement entered into by any Defendant in
13 connection with eBay's Affiliate Marketing Program, including but not limited to any
14 Publisher Service Agreement that may have been entered into between CJ and one or
15 more of Defendants and/or any Terms and Conditions of the Affiliate Marketing Program
16 agreed to by one or more of Defendants, provides for or in any way contemplates such
17 access. The User Agreements therefore govern and control any access to eBay's site,
18 whether authorized or unauthorized, by Defendants. Defendants, through their cookie
19 stuffing schemes, violated those User Agreements by accessing eBay's computers without
20 authorization and/or exceeded the authorized access granted to them by the User
21 Agreements.

22 39. Upon information and belief, Defendants' access to eBay's computers that
23 was either unauthorized or exceeded the authorization granted by the User Agreements
24 did not always result in a commission being paid to any Defendant (for example, where a
25 user, after having a cookie stuffed on his or her computer by one of Defendants, did not
26 subsequently take any Revenue Action). In other cases, Defendants' access to eBay's
27 computers that was unauthorized or exceeded the authorization granted by the User
28 Agreements resulted in commissions being paid to Defendants for Revenue Actions

1 initiated by users that Defendants did not refer to eBay, which were in no way related to
2 Defendants' advertisements, and for which Defendants were due no compensation. In
3 both instances, Defendants' access caused harm to eBay's computers and caused damage
4 and loss to eBay within the meaning of 18 U.S.C. § 1030, regardless of whether any
5 commission was later paid to Defendants for any particular act of cookie stuffing.

6 40. Upon information and belief, through their unauthorized access, Defendants
7 DPS and DOES 1-10 caused harm and damage to eBay's computers including, but not
8 limited to, impairment of the integrity of eBay's data, and caused loss to eBay including,
9 but not limited to, costs incurred by eBay in responding to and conducting an assessment
10 of the damage caused by these Defendants' cookie stuffing scheme. Through their
11 unauthorized access, Defendants DPS and DOES 1-10 also caused damage and loss to
12 eBay as a result of commissions being wrongfully paid to those Defendants. The loss to
13 eBay that resulted from the unauthorized access by Defendants DPS and DOES 1-10 was
14 incurred in each year from at least December 2003 through June 2007, and totaled more
15 than \$5,000 in at least the one-month period ending June 30, 2007.

16 41. Upon information and belief, through their unauthorized access, Defendants
17 KFC and DOES 12-20 caused harm and damage to eBay's computers including, but not
18 limited to, impairment of the integrity of eBay's data, and caused loss to eBay including,
19 but not limited to, costs incurred by eBay in responding to and conducting an assessment
20 of the damage caused by these Defendants' cookie stuffing scheme. Through their
21 unauthorized access, Defendants KFC and DOES 12-20 also caused damage and loss to
22 eBay as a result of commissions being wrongfully paid to those Defendants. The loss to
23 eBay that resulted from the unauthorized access by Defendants KFC and DOES 12-20
24 was incurred in each year from at least December 2004 through June 2007, and totaled
25 more than \$5,000 in at least the one-year period ending in June 2007.

26 42. eBay's computers are used in interstate and foreign commerce.

27 43. DPS's and KFC's actions, whether or not they resulted in the payment of
28 any commissions to them, constitute violations of the Computer Fraud and Abuse Act, 18

1 U.S.C. § 1030, including but not limited to §§ 1030(a)(4), 1030(a)(5)(B) and
2 1030(a)(5)(C).

3 44. WHEREFORE, eBay prays for judgment against each of DPS and KFC, as
4 more fully set forth below.

5 **SECOND CAUSE OF ACTION**

6 **(Violations of 18 U.S.C. § 1962(c))**

7 45. eBay realleges each and every allegation set forth in Paragraphs 1 through
8 44, inclusive, and incorporates them by reference herein.

9 46. Defendants Shawn Hogan's, Brian Dunning's, and Todd Dunning's
10 unlawful, tortious and otherwise actionable conduct constitutes violations of 18 U.S.C. §
11 1962(c).

12 47. Defendant Shawn Hogan and DOES 1-10 (the "Hogan Group") engaged in
13 activities through the company Digital Point Solutions. Digital Point Solutions has been
14 in existence as a business entity since at least 1999. On information and belief, based on
15 information provided on the company's website, from 1999 to the present, Digital Point
16 Solutions has had at least four employees, including owner, President, CEO and Senior
17 Systems Analyst Shawn Hogan, Vice President and Staff Systems Analyst R. Robin
18 Quasebarth, Associate System Analyst Richard L. Crook, and Sales Representative D.
19 Shawn Callahan. On information and belief, based on information provided on the
20 company's website and information provided to an eBay employee by Defendant Shawn
21 Hogan, at various times Digital Point Solutions also had other employees as well as a
22 group of "volunteers" who provided services to Digital Point Solutions. Digital Point
23 Solutions was incorporated on and/or before May 14, 2007. At all times relevant herein,
24 Digital Point Solutions constituted an enterprise under RICO.

25 48. At all times relevant herein, through Digital Point Solutions, the Hogan
26 Group associated with each other and others for the common purpose of causing millions
27 of computers to access eBay's servers to defraud eBay of commission fees by designing
28 and implementing the cookie stuffing scheme described above. Upon information and

1 belief, the Hogan Group's activities were ongoing, and Digital Point Solutions functioned
2 as a continuing unit in operating the fraudulent cookie stuffing scheme from
3 approximately December 2003 through June 2007.

4 49. Defendants Brian Dunning, Todd Dunning and DOES 12-20 (the "Dunning
5 Group") engaged in activities through the companies Kessler's Flying Circus,
6 Thunderwood Holdings, Inc., Dunning Enterprise, Inc., and BrianDunning.com, and each
7 company constitutes a RICO enterprise. Through Kessler's Flying Circus, Thunderwood
8 Holdings, Inc., Dunning Enterprise, Inc., and BrianDunning.com, the Dunning Group
9 associated with each other and others for the common purpose of defrauding eBay of
10 commission fees by designing and implementing the cookie stuffing scheme described
11 above. Upon information and belief, the Dunning Group's activities were ongoing, and
12 Kessler's Flying Circus, Thunderwood Holdings, Inc., Dunning Enterprise, Inc. and
13 BrianDunning.com functioned individually, and with each other, as continuing units in
14 operating the fraudulent cookie stuffing scheme from approximately December 2004
15 through June 2007.

16 50. The members of the Hogan Group and Dunning Group each committed
17 multiple violations of the predicate act of mail and wire fraud, 18 U.S.C. § 1343, both
18 through their cookie stuffing schemes and through communications with eBay and
19 Commission Junction designed to fraudulently conceal those schemes.

20 51. As described in Paragraphs 25-33 above, schemes to defraud eBay existed
21 by which the members of the Hogan Group and Dunning Group each stuffed eBay
22 cookies onto computers for the purpose of defrauding eBay of commission fees due only
23 for legitimate Revenue Actions associated with a given affiliate. The members of the
24 Hogan Group and Dunning Group each participated in these schemes with the specific
25 intent to defraud eBay. Use of the Internet was essential to the schemes: the members of
26 the Hogan Group and Dunning Group stuffed a cookie onto a computer when a user was
27 browsing the Internet, and the stuffed cookie was later read and recognized when that
28 Internet user accessed eBay's website on the Internet and either registered with the site,

1 purchased an item or engaged in some other Revenue Action. The members of the Hogan
2 Group and Dunning Group each, by use of their technologies, caused users' web browsers
3 to convey a representation by the Hogan Group and/or the Dunning Group to eBay that
4 the user had accessed the eBay website via an advertisement placed by either DPS or
5 KFC, when in fact, a substantial portion of those users never knowingly or intentionally
6 visited the eBay website based on an advertisement placed by either DPS or KFC. These
7 fraudulent acts and representations were repeated multiple times, and each act constitutes
8 a violation of 18 U.S.C. § 1343 through the use of interstate wires. Moreover, because the
9 Hogan Group's and the Dunning Group's cookie stuffing activities were undertaken as
10 part of a scheme to defraud and for the purpose of executing that fraud by wire
11 transmissions, each instance of cookie stuffing constitutes a completed violation of 18
12 U.S.C. § 1343 regardless of whether any commission was credited or paid as a result.

13 52. On or about June 2007, eBay undertook an investigation into suspected
14 cookie stuffing by the Hogan Group and the Dunning Group. eBay was able to verify the
15 existence of the two schemes and to track specific instances of cookie stuffing through
16 several different methods.

17 53. eBay first ran its own tests and was able to observe and confirm fraudulent
18 cookie stuffing by both the Hogan Group and the Dunning Group.

19 a. For example, on or about June 5, 2007, an eBay employee visited the
20 website www.drago-sim.com using a secure computer that had its IP address masked (to
21 overcome countermeasures that prevented cookies from being stuffed onto computers
22 with San Jose IP addresses) and that was equipped to monitor and record Internet activity
23 occurring on the computer. The website www.drago-sim.com was a participant in DPS's
24 advertising network and contained a DPS-controlled banner ad. Although the eBay
25 employee never clicked on, or requested, any eBay ad or link to an eBay website, the
26 Hogan Group's code in the DPS-controlled banner ad secretly redirected the computer
27 being used by the eBay employee to an eBay website, and a DPS-associated cookie was
28 dropped. eBay observed an identical cookie stuff by the Hogan Group on the same date

1 by visiting the site www.songlyrics.com, which was also a participant in the DPS ad
2 network and which also contained a DPS-controlled banner ad.

3 b. Also on or about June 5, 2007, eBay was able to observe and record
4 fraudulent cookie stuffing activity caused by the Dunning Group's wholinked and
5 profilemaps applications. As with the investigation of the Hogan Group's cookie stuffing,
6 secure computers equipped with Internet monitoring and recording equipment were
7 directed to sites containing the Dunning Group's wholinked and profilemaps applications.
8 Without any further action being taken by the computers' users, the Dunning Group's
9 wholinked and profilemaps applications secretly redirected the computers to an eBay
10 website, and KFC-associated cookies were stuffed onto the computers.

11 54. In addition, on June 6, 2007, eBay asked Gallivan, Gallivan & O'Melia LLC
12 ("GGO") to undertake a cookie stuffing investigation. On that date, a GGO employee
13 visited the website www.jokes-time.com using a secure computer located in Mountain
14 View, California that had its IP address masked and had been equipped to monitor and
15 record Internet activity occurring on the computer. The jokes-time.com website was a
16 participant in DPS's advertising network and contained a DPS-controlled banner ad.
17 Without any action by the GGO employee other than visiting that website, the Hogan
18 Group's code in the DPS-controlled banner ad secretly redirected the GGO computer to
19 another DPS site and then to eBay's website, causing eBay's site to drop cookies that
20 were associated with DPS onto the GGO computer. On or about June 14, 2007, an
21 employee of GGO created a new eBay account using the computer that still contained the
22 cookies stuffed by the Hogan Group. The GGO employee then purchased an item from
23 eBay using the newly created account through the "buy it now" function. Using
24 information provided by GGO, eBay then tracked this new account and purchase, and
25 determined that DPS was credited both for the "new user" acquisition and for the sale.

26 55. On or about June 6, 2007, GGO also performed a second cookie stuffing
27 test from its offices located in the Seattle, Washington area, following the same steps
28 taken in Mountain View. As in the Mountain View test, the Hogan Group's code stuffed

1 DPS-associated cookies onto the GGO computer even though the computer user did not
2 navigate to eBay's website. An eBay "buy it now" purchase was made by a GGO
3 employee in the Seattle area the following day using the computer containing the stuffed
4 cookies. eBay was again able to track a commission from the sale that was credited to
5 DPS.

6 56. Having confirmed the ongoing cookie stuffing by both the Hogan Group
7 and the Dunning Group, eBay next set out to determine the extent of that unlawful
8 activity. On or about June 8-19, 2007, eBay made certain alterations to its website to both
9 detect further evidence of the cookie stuffing and, if found, to assess the volume of cookie
10 stuffing by the Hogan Group and the Dunning Group. eBay placed a special "gif" image
11 on the eBay.com home page. This special gif was served to any browser receiving an
12 eBay cookie. eBay had observed that Defendants' cookie stuffing schemes caused the
13 user's browser to be secretly redirected to eBay's home page for only a short period of
14 time—sufficient time for the cookie to be stuffed and little or no more. A browser that
15 had been redirected to eBay for purposes of cookie stuffing would not access eBay's site
16 long enough to be served the special gif, but a legitimate browser redirect to eBay (during
17 which a user clicks on an ad and comes to the eBay site) would be served that gif. eBay
18 then examined the data or traffic sent by all of its affiliates, including DPS and KFC.
19 eBay was able to review this data with a tremendous amount of granularity, capturing
20 individual cookie stuffs by the Hogan Group and the Dunning Group. The following are
21 examples of such individual cookie stuffs:

- 22 • On June 8, 2007, at approximately 12:32 p.m. PST, a cookie stuffed with
23 information for the affiliate using PID 2326993 was dropped from an eBay
24 California server to IP address 84.13.180.86. The user of this IP address was
25 located in Surrey, UK. PID 2326993 was an affiliate account number assigned to
26 KFC. The special gif was not served.
- 27 • On June 8, 2007, at approximately 12:37 p.m. PST, a cookie stuffed with
28 information for the affiliate using PID 2028993 was dropped from an eBay

1 California server to IP address 83.67.105.219. The user of this IP address was
2 located in South Yorkshire, UK. PID 2028993 was an affiliate account number
3 assigned to KFC. The special gif was not served.

4 • On June 8, 2007, at approximately 12:52 p.m. PST, a cookie stuffed with
5 information for the affiliate using PID 2028993 was dropped from an eBay
6 California server to IP address 172.174.248.28. The user of this IP address was a
7 customer utilizing the ISP America Online located in Virginia. PID 2028993 was
8 an affiliate account number assigned to KFC. The special gif was not served.

9 • On June 8, 2007, at approximately 12:58 p.m. PST, a cookie stuffed with
10 information for the affiliate using PID 2225634 was dropped from an eBay
11 California server to IP address 68.57.17.37. The user of this IP address was located
12 in Pennsylvania. PID 2225634 was an affiliate account number assigned to DPS.
13 The special gif was not served.

14 • On June 9, 2007, at approximately 12:43 p.m. PST, a cookie stuffed with
15 information for the affiliate using PID 2326993 was dropped from an eBay
16 California server to IP address 81.104.118.168. The user of this IP address was
17 located in Glasgow, Scotland. PID 2326993 was an affiliate account number
18 assigned to KFC. The special gif was not served.

19 • On June 9, 2007, at approximately 12:56 p.m. PST, a cookie stuffed with
20 information for the affiliate using PID 2225635 was dropped by an eBay California
21 server on IP address 71.210.107.53. The user of this IP address was located in
22 Arizona. PID 2225635 was an affiliate account number assigned to DPS. The
23 special gif was not served.

24 • On June 11, 2007, at approximately 12:18 p.m. PST, a cookie stuffed with
25 information for the affiliate using PID 2225634 was dropped by an eBay California
26 server on IP address 206.40.234.2 18. The user of this IP address is located in
27 Utah. PID 2225634 is an affiliate account number assigned to DPS. The special
28 gif was not served.

1 The cumulative results of the investigation demonstrated that over 99% of the traffic
2 directed by DPS and KFC during the time period of the investigation did not receive the
3 gif image, and was therefore fraudulent cookie stuffing traffic. During the short period of
4 this investigation, the data demonstrated that the Hogan Group had stuffed over 650,000
5 cookies and the Dunning Group had stuffed close to 20,000 cookies.

6 57. eBay also performed an additional analysis of historical data that uncovered
7 further evidence of cookie stuffing by the Hogan Group and the Dunning Group over the
8 period from April 1, 2004 through June 18, 2007. Cookie stuffing is premised on the
9 notion that if one stuffs a large number of Internet users, some subset of those users will
10 later come to eBay (by chance and through no action of the cookie stuffer) and take a
11 Revenue Action. eBay examined its historical data regarding the behavior of eBay users
12 in an effort to determine whether user behavior provided proof of cookie stuffing. eBay's
13 analysis showed that, in fact, there were substantial differences in the behavior of
14 legitimately-referred users and users referred by DPS and KFC, which supported the
15 conclusion that the Hogan Group and the Dunning Group engaged in cookie stuffing. For
16 legitimately-referred users, the historical data showed that a high percentage of Revenue
17 Actions (e.g., establishing a new eBay account or placing a winning bid on an item)
18 occurred within the first hour of a cookie drop. Such behavior was to be expected,
19 because the cookie was dropped at the same time that the user visited eBay's site and was
20 exposed to the content on the site that would drive a Revenue Action. The contrasting
21 historical data for DPS and KFC demonstrated that both the Hogan Group and the
22 Dunning Group had been engaged in cookie stuffing. Users allegedly referred by DPS
23 and/or KFC demonstrated behavior consistent with cookie stuffing and inconsistent with
24 legitimate referrals: those users did not take the high percentage of their Revenue Actions
25 during the first hour following the cookie drop and, instead, took Revenue Actions at a
26 nearly uniform rate over the life of the cookie. This behavior showed that those users had
27 not been exposed to the content of the eBay site at the same time that the cookie was
28 dropped; instead, the users had been stuffed and visited eBay at some random time after

1 the stuffing.

2 58. On information and belief, based on eBay's analysis and understanding of
3 how the Defendants' cookie stuffing schemes worked and on statements made by Todd
4 Dunning to one of eBay's employees, DPS and KFC retained electronic records of the IP
5 addresses of the individual computers they stuffed with cookies in order to prevent
6 stuffing multiple cookies on a single computer.

7 59. The Hogan Group and the Dunning Group fraudulently stuffed cookies onto
8 the computers of a large group of users without exposing them to the content on eBay's
9 site and a subset of those users later engaged in Revenue Actions that were unrelated to
10 any action by DPS or KFC but still produced enormous commissions for them. In other
11 words, DPS and KFC received commissions based on Revenue Actions by users for
12 which they were not responsible. But every act of cookie stuffing by the Hogan Group
13 and the Dunning Group, regardless of whether it resulted in the payment of a commission,
14 constituted a separate violation of 18 U.S.C. § 1343, because it constituted a use of
15 interstate wire communications in furtherance of the Defendants' schemes to defraud
16 eBay.

17 60. In addition to their cookie stuffing schemes, which occurred over several
18 years and involved hundreds of thousands or even millions of acts that each constituted a
19 separate violation of 18 U.S.C. § 1343, the Hogan Group and the Dunning Group also
20 engaged in efforts to conceal and avoid detection of their schemes through fraudulent
21 communications involving the interstate mails and wires. Examples of such
22 communications include the following:

- 23 • On or about September 5, 2005, after being contacted by (then) CJ employee
24 Christine Kim regarding suspicions of possible cookie stuffing by DPS,
25 Defendant Shawn Hogan falsely told Ms. Kim in a telephone conversation that the
26 apparent cooking stuffing arose from a "coding error" that had since been fixed.
- 27 • On or about February 15, 2006, Todd Dunning telephoned eBay employee Dan
28 Burkhart and reported that DPS and Hogan were cookie stuffing, which was true.

1 During the same telephone conversation, Mr. Dunning told Mr. Burkhart that his
2 brother Brian Dunning was an honest affiliate. That statement was false. Mr.
3 Dunning later told eBay employees that he had lied when he said that DPS and
4 Mr. Hogan were cookie stuffing. That statement was also false.

- 5 • On or about August 9, 2006, Brian Dunning falsely told eBay employee Christine
6 Kim in an email that he would explain KFC's "innovative" business model "in
7 detail." Mr. Dunning subsequently provided Ms. Kim with descriptions of KFC's
8 business model that failed to accurately describe KFC's methods, and created the
9 false impression that KFC was actually driving users to eBay's site, instead of
10 engaging in a fraudulent cookie stuffing scheme.
- 11 • On or about August 29, 2006, Brian Dunning falsely stated in an email to CJ
12 employee Andrea Bardakos and eBay employee Christine Kim that the success of
13 KFC's methods was based on "staggering amounts of up-front adoption."
- 14 • On or about August 31, 2006, Brian Dunning emailed CJ employees Andrea
15 Bardakos and Jeff Ransdell, and eBay employee Christine Kim, thanking them for
16 maintaining confidentiality regarding the "inner workings" of his business model
17 and stating that "a conversation was 'due' at some point, especially given the high
18 simplicity-to-effectiveness ratio of what we're doing." In fact, KFC's
19 "effectiveness" in receiving commissions was due to its fraudulent cookie stuffing
20 scheme.
- 21 • On or about September 1, 2006, eBay employee Christine Kim and Shawn Hogan
22 conducted an instant message exchange during which Ms. Kim asked Mr. Hogan
23 to provide specifics regarding the DPS ad network, and Mr. Hogan made various
24 statements to actively conceal the existence of his cookie stuffing, including
25 claims that his system "works like evolution in nature" and refusing to provide his
26 code or analytics because "while it's really (REALLY) neat and would like to
27 show everyone just to show off ... it's really not a good idea if I give it away."
- 28 • On or about September 7, 2006, Brian Dunning falsely stated in an email to eBay

1 employee Christine Kim that he was “absolutely confident” that KFC’s methods
2 were “in line with the intended spirit of the terms” of the AMP.

- 3 • In early November 2006, eBay employee Christine Kim questioned Shawn Hogan
4 after an eBay employee based in Amsterdam had written to her about DPS’s
5 results in the Netherlands, noting that “[n]ormally we only see these low
6 conversion rates when cookiedropping is involved.” On or about November 6,
7 2006, Mr. Hogan falsely told Ms. Kim in a conversation via telephone or instant
8 message that low conversion rates in the Netherlands were caused by Mr. Hogan’s
9 failure to “deep link” his ads there after a bug fix had been made.
- 10 • On or about January 22, 2007, Brian Dunning responded by email to eBay
11 employee Christine Kim’s query as to why KFC’s “winning bids and clicks” were
12 below the norm by falsely stating, “I wonder if the demographic of MySpace
13 users has much to do with it. They’re generally quite young, maybe they’re too
14 poor to win auctions.” This statement was false and was intended to conceal his
15 cookie stuffing because Mr. Dunning knew that the unusual statistics noted by
16 Ms. Kim were the result of his cookie stuffing.
- 17 • On or about February 7, 2007, Brian Dunning falsely stated in an email to eBay
18 employee Christine Kim that “in the past 3 days we’ve received click-throughs on
19 ads from 97,743 profiles. That only counts profiles where someone clicked the
20 ad, no telling how many other profiles people have added it to.” In fact, as Mr.
21 Dunning knew at the time, his click-throughs were the result of cookie stuffing
22 and not from users clicking on ads.

23 61. Each violation of 18 U.S.C. § 1343 constitutes a separate instance of
24 “racketeering activity” as defined in 18 U.S.C. § 1961(1) and was committed in
25 furtherance of the conspiracy to defraud eBay of commission fees not legitimately earned
26 by either DPS or KFC. Together, these violations constitute a pattern of racketeering
27 activity: the violations have the same or similar purposes, results, participants, victims
28 and/or methods of commission.

1 62. The racketeering activity committed by each of the members of the Hogan
2 Group and the Dunning Group affected the interstate activity of Internet web browsing.
3 In addition, Internet marketing, including the marketing at issue here that utilizes
4 advertisements seen by Internet users in all 50 states and provides commissions for
5 actions taken by eBay users across all 50 states, is also an interstate activity that was
6 affected by the racketeering activity committed by each of the members of the Hogan
7 Group and Dunning Group.

8 63. The actions of each of the members of the Hogan Group and the Dunning
9 Group were undertaken with fraud, malice or oppression, or with a conscious disregard of
10 the rights of eBay. Therefore, eBay is entitled to an award of exemplary and punitive
11 damages against each of the members of the Hogan Group and the Dunning Group, in an
12 amount according to proof at trial.

13 64. WHEREFORE, eBay prays for judgment against each of the members of the
14 Hogan Group and the Dunning Group, as more fully set forth below.

15 **THIRD CAUSE OF ACTION**

16 **(Fraud)**

17 65. eBay realleges each and every allegation set forth in Paragraphs 1 through
18 64, inclusive, and incorporates them by reference herein.

19 66. DPS and DOES 1-10, by use of their cookie stuffing computer programs
20 and/or code, caused users' web browsers to convey a representation by those Defendants
21 to eBay that the user had accessed the eBay website via an advertisement placed by DPS.
22 eBay is informed and believes and, on that basis, alleges that this conduct began in or
23 around December 2003 and continued through at least June 2007.

24 67. KFC and DOES 12-20, by use of their cookie stuffing computer programs
25 and/or code, caused users' web browsers to convey a representation by those Defendants
26 to eBay that the user had accessed the eBay website via an advertisement placed by KFC.
27 eBay is informed and believes and, on that basis, alleges that this conduct began in or
28 around December 2004 and continued through at least June 2007.

1 68. DPS and KFC also made a number of false statements regarding their
2 business methods, described above, in an effort to conceal their fraudulent cookie stuffing
3 schemes from detection by eBay or CJ.

4 69. The representations made and/or caused to be made by each of DPS, KFC
5 and DOES 1-10 and 12-20 were in fact false. The true facts were that a substantial
6 portion of the users ostensibly referred by each of DPS, KFC and DOES 1-10 and 12-20
7 to the eBay site had not been referred by those Defendants, that those users had never
8 knowingly or intentionally visited the eBay site based on any advertisement or referral
9 from any of those Defendants, and that the information contained in cookies in those
10 users' web browsers was actually the product of the false and misleading cookie stuffing
11 schemes employed by each of DPS, KFC and DOES 1-10 and 12-20.

12 70. When DPS, KFC and DOES 1-10 and 12-20 made these representations (or
13 caused them to be made), they knew them to be false and made these representations (or
14 caused them to be made) with the intention to deceive and defraud eBay and induce eBay
15 to act in reliance on these representations.

16 71. eBay, at the time these representations were made (or caused to be made) by
17 DPS, KFC and DOES 1-10 and 12-20, was ignorant of the falsity of the representations
18 and believed them to be true. In reliance on these representations, eBay was induced to,
19 and did, make commission payments to each of DPS and KFC (via CJ) in consideration
20 for referrals that eBay believed to be legitimate and bona fide. Had eBay known the true
21 facts, it would not have made such commission payments. eBay's reliance on the
22 representations of DPS, KFC and DOES 1-10 and 12-20 was justified.

23 72. As a proximate result of the fraudulent conduct of each of DPS, KFC and
24 DOES 1-10 and 12-20, eBay paid commissions and fees to DPS and KFC (via CJ) for
25 referrals that had never occurred, for which eBay received no value, and for which eBay
26 owed nothing to DPS or KFC.

27 73. As a proximate result thereof, eBay has been damaged in an amount to be
28 proven at trial.

1 74. Defendants' actions were undertaken with fraud, malice or oppression, or
2 with a conscious disregard of the rights of eBay and, therefore, eBay is entitled to an
3 award of exemplary and punitive damages against each of DPS, KFC and DOES 1-10 and
4 12-20, in an amount according to proof at trial.

5 75. WHEREFORE, eBay prays for judgment against each of DPS, KFC and
6 DOES 1-10 and 12-20, as more fully set forth below.

7 **FOURTH CAUSE OF ACTION**

8 **(Violations of California Penal Code § 502)**

9 76. eBay realleges each and every allegation set forth in Paragraphs 1 through
10 75, inclusive, and incorporates them by reference herein.

11 77. Each of DPS and KFC have knowingly and without permission: altered,
12 damaged, deleted, destroyed, or otherwise used eBay's computer, computer system, or
13 computer network in order to devise and execute a cookie stuffing scheme or artifice in
14 order to defraud and deceive; and/or altered, damaged, deleted, destroyed, or otherwise
15 used eBay's computer, computer system, or computer network in order to wrongfully
16 control or obtain money and property; and/or accessed or caused to be accessed eBay's
17 computer, computer system, or computer network.

18 78. DPS's and KFC's unauthorized access and use of eBay's computers has
19 damaged and caused loss to eBay.

20 79. DPS's and KFC's actions constitute violations of California Penal Code §
21 502(c), whether or not any commissions were credited or paid as a result of those actions.

22 80. DPS's and KFC's actions were undertaken with fraud, malice or oppression,
23 or with a conscious disregard of the rights of eBay and, therefore, eBay is entitled to an
24 award of exemplary and punitive damages against each of DPS and KFC, in an amount
25 according to proof at trial.

26 81. WHEREFORE, eBay prays for judgment against each of DPS and KFC, as
27 more fully set forth below.

28

FIFTH CAUSE OF ACTION

(Restitution and Unjust Enrichment)

1
2
3 82. eBay realleges each and every allegation set forth in Paragraphs 1 through
4 81, inclusive, and incorporates them by reference herein.

5 83. Through their cookie stuffing schemes, as described above, each of DPS and
6 KFC received a benefit from eBay, in the form of artificially and fraudulently inflated
7 commissions paid to DPS and KFC (via CJ) for Revenue Actions that were not associated
8 with any referral from those Defendants.

9 84. In light of DPS's and KFC's conduct, it would be unjust for DPS and KFC
10 to retain the benefits they obtained from eBay.

11 85. DPS and KFC have been unjustly enriched by eBay's payments and should
12 be required in equity to make restitution of these payments to eBay.

13 86. WHEREFORE, eBay prays for judgment against each of DPS and KFC, as
14 more fully set forth below.

SIXTH CAUSE OF ACTION

(California Business and Professions Code § 17200)

15
16
17 87. eBay realleges each and every allegation set forth in Paragraphs 1 through
18 86, inclusive, and incorporates them by reference herein.

19 88. Through their cookie stuffing schemes, as described above, each of DPS and
20 KFC engaged in unlawful, unfair and/or fraudulent business practices. Such conduct by
21 each of DPS and KFC violates California Business and Professions Code § 17200 et. seq.

22 89. As discussed herein, DPS's and KFC's business practices of engaging in
23 cookie stuffing were unlawful under state and federal laws, including but not limited to
24 the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, the civil RICO statute, 18 U.S.C. §
25 1962(c), California Penal Code § 502, and constituted common law fraud.

26 90. DPS's and KFC's conduct was also fraudulent and deceptive, and was
27 unfair to eBay, in that it offended established public policy, and/or was immoral,
28 unethical, oppressive, unscrupulous and substantially injurious to eBay.

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
26
27
28

91. As a direct result of DPS's and KFC's conduct, eBay has suffered an injury in fact and has lost money and/or property that has been wrongfully retained by each of DPS and KFC.

92. WHEREFORE, eBay prays for judgment against each of DPS and KFC, as more fully set forth below.

PRAYER FOR RELIEF

WHEREFORE, based upon the foregoing, eBay prays for judgment against Defendants, and each of them, for:

- i. Judgment in favor of eBay and against all Defendants on all causes of action;
- ii. An award of compensatory damages according to proof at trial;
- iii. An award of punitive damages according to proof at trial;
- iv. An award of treble damages against Defendants Shawn Hogan, Brian Dunning and Todd Dunning, pursuant to 18 U.S.C. § 1964 according to proof at trial;
- v. An award requiring Defendants to disgorge all ill-gotten gains and to return the eBay funds by which Defendants have been unjustly enriched;
- vi. An award of restitution, according to proof at trial;
- vii. An injunction prohibiting Defendants from (a) disseminating, sharing or otherwise making available any cookie stuffing technology to others; (b) possessing, disseminating, sharing, or otherwise making available any technology intended or capable of being used to defraud eBay; and (c) having any further involvement with any person or entity participating in the eBay Affiliate Marketing Program;
- viii. An award of pre-judgment and post-judgment interest;
- ix. An award of attorney's fees and costs of suit incurred herein; and
- x. Such other further relief as the Court may deem just and proper.

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
26
27
28

Dated: March 26, 2009

O'MELVENY & MYERS LLP

By: David R. Eberhart
David R. Eberhart
Sharon M. Bunzel
Colleen M. Kennedy
Attorneys for Plaintiff eBay INC.

DEMAND FOR JURY TRIAL

eBay hereby demands a trial by jury of all claims in this action.

Dated: March 26, 2009

O'MELVENY & MYERS LLP

By: David R. Eberhart
David R. Eberhart
Sharon M. Bunzel
Colleen M. Kennedy
Attorneys for Plaintiff eBay INC.

EXHIBIT “3”

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # 288A-SF-141681

On (date) 6/18/07

- item(s) listed below were:
- Received From
 - Returned To
 - Released To
 - Seized

(Name) Brian Andrew Dunning

(Street Address) 15 High Bluff

(City) Laguna Niguel, CA 92677

- Description of Item(s):
- 1) Check from "Progressive Solutions" for \$6000
 - 2) Yellow note pad with notes
 - 3) State of CA Certificate of Title (2007 Jeep 1J8GA69142K166078)
 - 4) Wells Fargo bank documents
 - 5) Washington Mutual bank documents
 - 6) White note pads w/ notes
 - 7) Thunderwood Holdings Docs
 - 8) Senex Docs
 - 9) Pacific Life docs
 - 10) IRS/ Orange Co. Clerks-Recorder Docs
 - 11) Fidelity Docs
 - 12) Merrill Lynch Docs
 - 13) Cingular Cell docs
 - 14) Misc. Docs
 - 15) Tax returns ^{all} 2003, 2004

Room A

Received By: [Signature]
(Signature)

Received From: [Signature]
(Signature)

FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

288A-SF-141681

On (date) 6/18/07

item(s) listed below were:

- Received From
- Returned To
- Released To
- Seized

(Name) Brian Andrew Dunning

(Street Address) 15 High Bluff

(City) Laguna Niguel, CA 92677

- Description of Item(s):
- 1) ⁵ Toshiba laptop S/N 62064761P
 - 16) Apple laptop (Macbook Pro) S/N M186073ZBJ3 w/keyboard
 - 17) (3) a.com data hard drives S/N 65182161, S/N 65204025, S/N (No serial #)
 - 18) Apple mini servers (4) S/N YM6332ZQWOB, S/N YM6370SKWKN, S/N YM64505DWKN, S/N YM6391LHWOB, S/N YM6251MJU36
 - 19) Toshiba Disk Drive S/N 16G001975
 - 20) Gateway Laptop S/N BC558470134
 - 21) Cingular Palm S/N PRCU01Q7H24F
 - 22) Garmin 59507833
 - 23) Sprint Treo S/N PTPC02V6HIK67
 - 24) Dynex USB 2.0
 - 25) Apple rechargeable battery S/N KF624096TY4B, misc. cables

Room A

Received By:

[Signature]
(Signature)

Received From:

[Signature]
(Signature)

UNITED STATES DEPARTMENT OF JUSTICE
FEDERAL BUREAU OF INVESTIGATION
Receipt for Property Received/Returned/Released/Seized

File # Z 88A-SF-141681

On (date) 6/12/07

- item(s) listed below were:
- Received From
 - Returned To
 - Released To
 - Seized

(Name) Brian Andrew Dunning
 (Street Address) 15 High Bluff
 (City) Laguna Niguel, CA 92657

- Description of Item(s):
- 26) Apple Laptop S/N W840805ANRX, cable (Room C)
 - 27) Apple desk top S/N W83201VMNHX (Room F), keyboard
 - 28) Apple laptop S/N Q704609WJ74 (Room D)
 - 29) Samsung cell phone S/N RVEAC63868X, charger (Room D)
 - 30) Samsung cell phone 24114248537, charger (Room D)
 - 31) Misc docs, 4 CDs (outside trash can)
 - 32) IPOD 30GB S/N 8K6404BRV9R (Room M)
 - 33) Apple IMAC S/N W86494QVVUV (Room I)
 - 34) Ipad 4GB YM6201NC52C (Room I)
 - 35) Ipad 16GB S/N U23170C2NRH (Room I)

Received By: [Signature]
(Signature)

Received From: [Signature]
(Signature)

EXHIBIT “4”



CHIP (COMPUTER HACKING AND INTELLECTUAL PROPERTY) FACT SHEET

HISTORY

Nine additional units will be added to a program called CHIP (Computer Hacking and Intellectual Property) that has proven successful in Northern California. That project demonstrated the benefits of a unit of prosecutors working closely with the FBI and other agencies to establish a relationship with the local high tech community and encourage them to refer cases to law enforcement. In addition, the project provides the skills and training not yet available to law enforcement on a widespread basis.

The new CHIP units are the next phase in the Department's ongoing efforts to combat cybercrime and Intellectual Property theft. In 1991, the Department created what is now the Computer Crime and Intellectual Property Section (CCIPS) in the Criminal Division. This Section is comprised of 22 attorneys who specialize in these crimes and provide national training, advice and coordinate prosecution of computer intrusion and intellectual property cases. The CHIP team members will complement the highly trained network of prosecutors at CCIPS and the US Attorneys' Offices.

PROGRAM DETAILS

CHIP units will be established in eight cities in addition to San Francisco, where the concept was pioneered. The cities have been chosen based on a number of factors, including their proximity to high-tech industry areas, their potential for growth in that area and the presence of adequate FBI resources to investigate these crimes.

- Los Angeles
- San Diego
- Atlanta
- Boston
- New York (Brooklyn and Manhattan)
- Dallas
- Seattle
- Alexandria, Virginia

- Together, the 10 units will have a total of 77 positions, including 48 prosecutors.
- This will provide 4 to 6 prosecutors in each participating district, through combining new and existing resources in the selected districts.

RESOURCES

The FY 2001 Appropriation provided \$3,074,000 to fund 50 positions and 25 FTE, including 28 attorneys.

The following chart shows the proposed unit composition:

Districts	New AUSA Allocation	"AUSA" District Match	Total CHIP AUSAs	New Paralegal Allocation	New Support Allocation	"Support" District Match	Unit Position Total
California CD	2	4	6	1	1	2	10
California ND	4	2	6	1	2	1	10
California SD	2	2	4	1	1	2	8
Georgia ND	3	1	4	0	2	0	6

Massachusetts	2	2	4	0	2	0	6
New York ED	2	2	4	0	2	0	6
New York SD	3	2	5	0	1	1	7
Texas ND	3	1	4	0	2	0	6
Virginia ED	4	2	6	1	2	1	10
Washington WD	3	2	5	0	2	1	8
Total	28	20	48	4	17	8	77

COMPONENTS

The program has 3 components: (1) **Prosecution**, (2) **Regional Prevention and Outreach** and (3) **Regional Training**.

1. Prosecution

- CHIP units will prosecute computer intrusions, copyright and trademark violations, theft of trade secrets and economic espionage, theft of computer and high tech components and other Internet crimes.

2. Regional Prevention and Outreach

- Prosecutors will work with CCIPS, the FBI and other agencies to establish good working relationships with the high tech community and to encourage victims of high tech crime to report such crimes to law enforcement.

3. Regional Training

- Cybercrime fighting requires special skills. CHIP units will receive the same high-level training provided by CCIPS, but will also be expected to develop and offer regional training programs to increase expertise among federal, state and local prosecutors.

- CHIP units will also be encouraged to send attorneys to work at CCIPS to train, and to call upon CCIPS for assistance in providing local training.

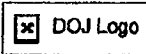
- **More information on: CHIPS Program**
- **More information on: Attorney General Ashcroft's Remarks**
- **More information on: Law Enforcement Coordination for High-Tech Crimes**
- **More information on: Intellectual Property Policy**
- **More information on: Computer Crime Policy**

Want to receive news of updates to the cybercrime.gov website?
Send a blank message to: cybercrime-subscribe@topica.com and we will add you to our email newsletter list.
(Mailing list privacy information)

Go to . . . [CCIPS home page](#) || [Justice Department home page](#)

Updated page December 9, 2002
usdoj-orm/mis/krr

EXHIBIT “5”



Computer Crime and Intellectual Property Section (CCIPS)

Law Enforcement Coordination for High-Tech Crimes

- A. The Computer Hacking and Intellectual Property (CHIP) Program
 - B. High Technology Law Enforcement Training Opportunities
 - C. Coordination Between Law Enforcement and Industry
 - D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime
-

A. The Computer Hacking and Intellectual Property (CHIP) Program

In 1995, at the recommendation of the then-Computer Crime Unit (now the Computer Crime and Intellectual Property Section (CCIPS)), the Department of Justice created the Computer and Telecommunication Coordinator (CTC) Program to protect the nation's businesses and citizens from the rising tide of computer crime and intellectual property theft by designating one or more prosecutors in every U.S. Attorney's Office to be responsible for these issues. In 2001, following a successful model developed in the Northern District of California, the Department expanded the program in ten cities by designating Computer Hacking and Intellectual Property (CHIP) units. These units typically involved more prosecutors than under the CTC program and ~~were specifically charged with building relationships in-district with the~~ FBI, other agencies, and the local high tech community. New units were added frequently thereafter. In 2005, the CTC and CHIP programs were combined into a unified CHIP program. More information on the CHIP Program and historical information on the CTC program is available below.

- CHIPs Unit Established in the Eastern District of California United States Attorney Office (October 19, 2004)
- CHIPs Unit Established in the Eastern District of Virginia United States Attorney Office (January 14, 2002)
- CHIPs Unit Established in Central District of California United States Attorney Office (September 6, 2001)
- CHIPs Unit Established in Southern District of New York United States Attorney Office (September 5, 2001)
- CHIPs Unit Established in the Eastern District of New York (August 21, 2001)
- Fact sheet on Computer Hacking and Intellectual Property (CHIP) units (July 20, 2001)

- Attorney General Ashcroft's Speech Announcing Expansion of CHIP Program and Establishment of Nine New CHIP units (July 20, 2001)
- The Computer and Telecommunications Coordinator (CTC) Program, Stacey Levine, USA Bulletin (May 2001)
- CTC Responsibilities

B. High Technology Law Enforcement Training Opportunities

- Training Opportunities

C. Coordination Between Law Enforcement and Industry

Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue

On April 5, 2000, the Department of Justice hosted a Cybercrime Summit at Stanford Law School, titled "Cybercrime Summit: A Law Enforcement/Information Technology Industry Dialogue on Prevention, Detection, Investigation and Cooperation," at which Attorney General Janet Reno and members of the Justice Department and other law enforcement agencies met with representatives of information technology and Internet companies. The main topic of the Summit was how to improve cooperation between law enforcement and industry in investigating computer network hacking. Linked below are the Attorney General's Opening Remarks from the Summit, as well as the Question & Answer session between industry representatives and the Attorney General.

- Opening Remarks of Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)
- Question and Answer Session with Attorney General Janet Reno at the Cybercrime Summit (April 5, 2000)

The Cybercitizen Partnership: Industry and Government Alliance

On March 15, 1999, Attorney General Janet Reno announced a new Cybercitizen Partnership, a new alliance between law enforcement and the technology community. The goal of the partnership is to coordinate the efforts of government, industry and the public to ensure public safety and responsible computer use. The partnership will also promote computer ethics and civic responsibility in the cyber age and aid law enforcement and industry in the battle against "on-line outlaws." The partnership will consist of three complementary segments. The first segment is a "good cybercitizenship" public awareness campaign. The second is a user-friendly computer and network security directory to help public and private sector organizations quickly find computer security resources. The third is an Information Security Professional fellowship program between industry and government that will raise the awareness levels of participants with respect to the views, perspectives and needs of their respective counterparts.

- Statement by Attorney General Janet Reno to Announce the Cybercitizen Partnership at the ITAA Policy Summit (March 15, 1999)
- ITAA and Attorney General Janet Reno Unveil New Tech Partnership (March 15, 1999)

D. DOJ Speaks Out on Law Enforcement Coordination to Address Cybercrime

Assistant Attorney General Michael Chertoff's Testimony Before the House Subcommittee on Crime

On June 12, 2001, Assistant Attorney General Michael Chertoff testified before the Members of the Subcommittee on Crime of the Committee on the Judiciary. In his statement he addressed the nature of cybercrime and the Department's current efforts to combat that problem.

- Text of Assistant Attorney General Michael Chertoff's testimony before the House Subcommittee on Crime of the Committee on the Judiciary (June 12, 2001)

Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute

On May 22, 2001, videotaped remarks by Attorney General John Ashcroft were presented before the first Annual Computer Privacy, Policy and Security Institute.

In his speech, the Attorney General addressed the Institute's concerns of computer security and threats to information assets and the means by which industry and law enforcement can work together in fighting cybercrime.

- Text of Attorney General Ashcroft's Remarks Before the First Annual Computer Privacy, Policy & Security Institute (May 22, 2001)
- View Video Taped Remarks (21 Megabytes)
*Approximate download time: 56K Modem=55 minutes
- View Video Taped Remarks (13 Megabytes)
*Approximate download time: 56K Modem=35 minutes

**Note: the listed download times are estimated times under optimal conditions. Your actual download times may vary depending on your modem, internet traffic, and your internet connection type.*

Attorney General Reno's Address to the ITAA Cybercrime Summit

On June 9, 2000, Attorney General Janet Reno gave the keynote address at the ITAA Cybercrime Summit. In her speech, the Attorney General discussed the means by which industry and law enforcement can work together in fighting cybercrime. The text also includes the question and answer section.

- Text of Attorney General Reno's Keynote Address at the ITAA Cybercrime Summit (June 9, 2000)

Attorney General Janet Reno Testifies Before Senate Appropriations Committee

On Monday, February 16, 2000, Attorney General Janet Reno testified before the United States Senate Committee on Appropriations. Her testimony provided an overview of cybercrime and the challenges that it presents to law enforcement today.

- **Testimony by Attorney General Janet Reno before the United States Senate Committee on Appropriations (February 16, 2000)**

Attorney General Janet Reno Introduces Law Net Initiative

On January 10, 2000, Attorney General Janet Reno gave remarks before the National Association of Attorneys General in which she announced a new Law Net initiative. The Law Net will be a "strong, permanent network of federal, state and local computer crime experts to do the following: To share expertise and information technology, to assist each other 24 hours a day, seven days a week, around the clock, to prevent cybercrime wherever possible, and to bring those responsible for such crime, when it does occur, to justice; To work with industry, the academic world and privacy groups to build trust and to protect our privacy and the Constitutional rights of all Americans; And finally, to ensure that the Internet is a force that brings this world together and builds understanding across peoples and places and time.

- **Remarks of the Honorable Janet Reno, Attorney General of the United States, to the National Association of Attorneys General (January 10, 2000)**

Attorney General Janet Reno Addresses the High Technology Crime Investigation Association 1999 International Training Conference

On Monday, September 20, 1999, Attorney General Janet Reno addressed the High Technology Crime Investigation Association 1999 International Training Conference in San Diego, California. Her speech focused on the importance of interagency and state and federal law enforcement cooperation, as well as on the Department of Justice's policy position on encryption regulation.

- **Speech by Attorney General Janet Reno before the High Technology Crime Investigation Association 1999 International Training Conference (September 20, 1999)**

President Clinton Addresses National Academy of Sciences on Keeping America Secure for the 21st Century

On January 22, 1999, President William Jefferson Clinton addressed the National Academy of Science. His speech was titled "Keeping America Secure for the 21st Century." The speech he gave is available via the link below:

- **President Clinton's Speech to National Academy of Sciences (January 22, 1999)**

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
26
27
28

CERTIFICATE OF SERVICE

The undersigned hereby certifies that the foregoing:

OPPOSITION TO MOTION TO COMPEL RESPONSES TO REQUESTS FOR PRODUCTION, INTERROGATORIES AND REQUESTS FOR ADMISSION; DECLARATIONS OF WILLIAM J. KOPENY, LEO J. PRESIADO AND BRIAN DUNNING IN SUPPORT

was filed with the Court's Electronic Filing System on October 23, 2009 and may be accessed electronically.

s/ Leo J. Presiado
Leo J. Presiado
Rus, Miliband & Smith, APC
2211 Michelson Drive, Seventh Floor
Irvine, California 92612
Tel: (949) 752-7100
Fax: (949) 252-1514
Email: lpresiado@rusmiliband.com
Attorneys for Defendants Thunderwood Holdings, Inc., Brian Dunning and Briandunning.com