

Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

September 15 20 11
WILLIAM M. McCOOL, Clerk
By [Signature] Deputy

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

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA,
Plaintiff,

NO. CR 11-301 RAJ

v.
JOSHUAH ALLEN WITT,
BRAD EUGENE LOWE, and
JOHN EARL GRIFFIN,
Defendants.

INDICTMENT

The Grand Jury charges that:

COUNT 1

**(Conspiracy to Intentionally Access a Protected Computer
Without Authorization With Intent to Defraud)**

A. The Offense

1. Beginning at a time uncertain, but not later than April 27, 2008, and continuing until at least December 13, 2010, within the Western District of Washington and elsewhere, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN did knowingly and willfully conspire, combine, confederate, and agree together with others, known and unknown to the Grand Jury, to commit offenses against the United States, to wit: intentionally accessing a protected computer without authorization, knowingly and with intent to defraud, and by means of such conduct furthering the intended fraud, in violation of Title 18, United States Code, Sections 1030(a)(4), 1030(b), and 1030(c)(3)(A), and committed acts in furtherance of that conspiracy.

1 **B. Object and Purpose of the Conspiracy**

2 2. The object of the conspiracy was to gain unauthorized access to the computer
3 networks of local businesses¹ in order to steal or manipulate a wide variety of data; to then use
4 that data to commit an array of frauds to generate proceeds consisting of consumer goods and/or
5 cash; and then to convert those proceeds of fraud to the personal use and benefit of JOSHUAH
6 ALLEN WITT, BRAD EUGENE LOWE, JOHN EARL GRIFFIN, and others known and
7 unknown to the Grand Jury.

8 **C. Manner and Means of the Conspiracy**

9 3. It was part of the conspiracy that JOSHUAH ALLEN WITT, BRAD EUGENE
10 LOWE, and JOHN EARL GRIFFIN would use a variety of methods to gain unauthorized access
11 to (“hack”) the computer networks of small and medium-sized businesses located in the Puget
12 Sound region.

13 4. It was further part of the conspiracy that one of the techniques used by JOSHUAH
14 ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN to facilitate hacks of local
15 businesses is a technique known as “war-driving.”

16 War-driving refers to the act of searching for accessible wireless (“WiFi”) networks by a
17 person in a moving vehicle, using a portable (laptop or notebook) computer, coupled with a long
18 range antennae. Once a WiFi network is located through war-driving, it can then also be
19 remotely reconnoitered for information that may reveal the relative security, and possible
20 vulnerabilities of the network. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN
21 EARL GRIFFIN used the war-driving technique, and information they obtained as a result, in
22 order to identify and reconnoiter wireless networks for attack.

23 5. It was further part of the conspiracy that another means used by JOSHUAH
24 ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN to facilitate network
25 hacks of local businesses was to take possession of lost or stolen laptop computers that belonged
26 to local businesses, or employees of local businesses, and then to hack a business’s network
27

28 ¹Individual local businesses victimized in this scheme will be identified for purposes of the
Indictment as “B-[1,2,3, et cet.]” to protect their identities.

1 remotely with the use of that laptop computer. JOSHUAH ALLEN WITT, BRAD EUGENE
2 LOWE, and JOHN EARL GRIFFIN thereby obtained saved access credentials on the laptop
3 computers, such as WiFi access keys, virtual private network (“VPN”) credentials, remote
4 desktop credentials or other such access credentials to hack the business’s network. JOSHUAH
5 ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN obtained possession and
6 control over the laptop computers they used for hacking either by stealing them in burglaries that
7 they themselves committed, or through other illegitimate sources.

8 6. It was further part of the conspiracy that another means JOSHUAH ALLEN
9 WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN used to facilitate network
10 hacks of local businesses was to first burglarize a business, and then to gain unauthorized
11 physical access to the business’s network by attaching storage media containing password
12 cracking or password bypass programs to computer servers or other network hardware present on
13 the scene. After obtaining such access, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE,
14 and JOHN EARL GRIFFIN would download data (such as usernames and passwords) and/or
15 upload malicious software (“malware”) that would allow them subsequently to remotely gain
16 further unauthorized access to the business’s network.

17 7. It was further part of the conspiracy that once JOSHUAH ALLEN WITT, BRAD
18 EUGENE LOWE, and JOHN EARL GRIFFIN had successfully hacked a business’s network,
19 they would then knowingly and purposefully transmit software programs, code, and commands
20 that they intended to use maliciously to alter or destroy or otherwise do damage to the business’s
21 network or data contained on and in it; to steal large volumes and a wide array of data; and to
22 alter data regarding their own activities on the network in an effort to conceal their hacking
23 activities and evade detection.

24 8. It was further part of the conspiracy that JOSHUAH ALLEN WITT, BRAD
25 EUGENE LOWE, and JOHN EARL GRIFFIN used their unauthorized access to victim business
26 networks to commit fraud in a variety of ways, including but not limited to the following:

27 a. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
28

1 GRIFFIN would steal online banking credentials of victim businesses in order to gather and use
2 information about the bank accounts held by the victim business.

3 b. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL

4 GRIFFIN would commit fraud by stealing credentials (including usernames and passwords) that
5 would enable them to obtain unauthorized access to a business's existing electronic payroll
6 disbursement software/accounts. Alternatively, they would use the stolen credentials to establish
7 new fraudulent electronic payroll disbursement accounts, to which they would link the business
8 bank account as a funding source. When compromising an existing electronic payroll
9 disbursement account, they would alter data in that account, with the goal of rerouting funds that
10 were intended for employee payroll direct deposits instead to bank accounts that the co-
11 conspirators had fraudulently opened, using stolen identity information. The stolen identity
12 information used for establishing these fraudulent bank accounts often belonged to the employees
13 of the victim business. The co-conspirators also would change (raise) employees' pay rates in
14 order to increase fraudulent disbursements from payroll accounts. They would purchase loadable
15 debit cards, establish online accounts for the loadable debit cards, and route funds from the
16 victim business's own accounts via fraudulent electronic payroll disbursement accounts that the
17 co-conspirators had established or seized, to the loadable debit cards. They would then take the
18 debit cards they had loaded fraudulently with the victim business's funds to local ATM
19 machines, where they would cash out multiple debit cards, in quick succession, in order to drain
20 the victim business's compromised accounts of the maximum amount of funds, as quickly as
21 possible. They would also use the loadable debit cards for Point-of-Sale (POS) purchases.

22 c. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL

23 GRIFFIN also would commit fraud by stealing credentials (including usernames and passwords)
24 for a victim business's online accounts with office supply, computer, and electronics companies,
25 and use them to place multiple orders fraudulently for the purchase of high-end computers,
26 computer-related supplies and other electronic equipment and devices. When they received those
27 shipments of fraudulently procured goods, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE,
28 and JOHN EARL GRIFFIN would convert them to their own personal use (sometimes for use to

1 | commit other online crimes), or fence or barter them for illegal drugs or other illicit items or
2 | proceeds.

3 | d. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
4 | GRIFFIN also would commit fraud both by fraudulently accessing other existing online accounts
5 | - such as eBay and PayPal accounts that belonged to the victim businesses, or their owners or
6 | employees - and by fraudulently establishing new accounts with online companies such as eBay
7 | and PayPal under the stolen identities of others. JOSHUAH ALLEN WITT, BRAD EUGENE
8 | LOWE, and JOHN EARL GRIFFIN would then use these accounts to fraudulently purchase
9 | goods that they would subsequently convert to their own use or benefit.

10 | e. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
11 | GRIFFIN also would fraudulently use individually identifiable credit card account numbers
12 | belonging to the owners, employees, and customers of businesses they hacked to fraudulently
13 | purchase goods that they would subsequently convert to their own use or benefit. The items that
14 | they purchased fraudulently in these ways included laptop computers, long range computer
15 | antennas, other electronic devices, tools that would be useful to effect physical burglaries, and
16 | many parts for a variety of specific makes and models of automobiles owned by them or their
17 | associates. When JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
18 | GRIFFIN received those fraudulently procured goods, they would convert them to their own
19 | personal use (sometimes for use to commit other online crimes), or fence or barter them for
20 | illegal drugs or other criminal proceeds.

21 | f. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
22 | GRIFFIN also would aid and abet additional fraudulent activities of others, known and unknown
23 | to the Grand Jury, by providing personally identifiable information, such as names, dates of birth
24 | and social security numbers, and also banking and financial information of the owners,
25 | employees, and customers of the businesses they hacked, to other coconspirators or other known
26 | criminal associates, who would in turn use that information fraudulently to open credit card or
27 | other accounts.

1 9. It was further part of the conspiracy that JOSHUAH ALLEN WITT, BRAD
2 EUGENE LOWE, and JOHN EARL GRIFFIN intended to, and did successfully take control of,
3 or “own” the electronic/virtual fax transmission systems of victim businesses, which they would
4 use for harvesting additional financial and personal identifying information.

5 10. It was further part of the conspiracy that JOSHUAH ALLEN WITT, BRAD
6 EUGENE LOWE, and JOHN EARL GRIFFIN intended to, and did successfully take control of,
7 or “own” the e-mail servers of some of the victim businesses they hacked, enabling them to
8 monitor the victim business’s discovery and response to the network intrusion incident, to
9 include eavesdropping on communications with law enforcement agents.

10 11. It was further part of the conspiracy that JOSHUAH ALLEN WITT, BRAD
11 EUGENE LOWE, and JOHN EARL GRIFFIN amassed multiple computer servers, and used the
12 combined computing power of those servers to crack passwords they then used to further their
13 illicit and criminal online activities.

14 12. It was further part of the conspiracy that JOSHUAH ALLEN WITT, BRAD
15 EUGENE LOWE, and JOHN EARL GRIFFIN took a number of steps to conceal their criminal
16 actions, mask their own identities in relation to them, and evade detection for them. Those
17 efforts and actions included the following:

18 a. When they placed fraudulent orders online for merchandise, JOSHUAH ALLEN
19 WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN would use a variety of identities
20 and also a variety of “drop addresses” for merchandise shipment. The addresses used typically
21 were not those of JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
22 GRIFFIN, but were instead addresses that were in the vicinity of residences of a variety of
23 associates, or fabricated addresses in the vicinity of associates, or addresses or fabricated
24 addresses for locations which they could themselves monitor, for deliveries.

25 b. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL
26 GRIFFIN routinely and consistently used the wireless Internet access accounts of others (also
27 known as “piggybacking”) when they were conducting intrusions into victim business networks,
28 or engaging in any of their online fraudulent activities. Because they methodically used the

1 Internet access accounts of others in this way, (including those of the victim businesses, but also
2 those of other innocent third parties), their online criminal activities would “trace back” to the
3 accounts of the victim businesses or the other innocent third parties, making it appear as though
4 someone at the victim business, or some other innocent third party, was responsible for the
5 criminal conduct.

6 c. As part of and in conjunction with their hacking activities, JOSHUAH ALLEN
7 WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN would manipulate or destroy data
8 on a victim business’s network that would evidence the hack or potentially connect them to it.
9 This included, for example, the destruction of firewall logs that would have evidenced an
10 intrusion and alerted the victim business to it. By destroying evidence of their intrusion and their
11 presence on the victim business’s network, JOSHUAH ALLEN WITT, BRAD EUGENE
12 LOWE, and JOHN EARL GRIFFIN could undermine a victim business’s network defenses,
13 extend the duration of their intrusion, and thereby maximize their opportunities to steal valuable
14 data from which they could profit fraudulently. By destroying evidence of their intrusion and
15 their presence on the victim business’s network, JOSHUAH ALLEN WITT, BRAD EUGENE
16 LOWE, and JOHN EARL GRIFFIN could also reduce the risk that law enforcement agents
17 would be able to identify them as the perpetrators of the network intrusion activity.

18 13. It was further part of the conspiracy that during the period from April 27, 2008,
19 through at least December 13, 2010, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and
20 JOHN EARL GRIFFIN hacked the computer networks of at least 13 businesses located in the
21 Puget Sound region, and after they had successfully hacked those businesses, stole a variety of
22 data from those systems that they used to commit a wide array of fraudulent transactions in order
23 to generate proceeds or goods that they would subsequently convert to their own use or benefit,
24 or to that of other coconspirators known and unknown to the Grand Jury, or to other criminal
25 associates.

26 14. It was further part of the conspiracy that during the period from April 27, 2008,
27 through at least December 13, 2010, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and
28 JOHN EARL GRIFFIN burgled or caused to be burgled at least 41 businesses in the Puget Sound

1 region. JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN
2 targeted businesses for burglary that likely would have high end computers and computer servers
3 on their premises. The coconspirators targeted these businesses because they likely would have
4 computer networks that, if successfully hacked, would yield data that could be used fraudulently
5 for profit; and because the high end computers and servers stolen from these businesses could
6 readily be sold to others.

7 **D. Overt Acts**

8 In furtherance of the conspiracy and to achieve the objects thereof, at least one of the
9 coconspirators committed or caused to be committed, in the Western District of Washington, and
10 elsewhere, at least one of the following overt acts, among others:

11 15. On or about April 27, 2008, JOSHUAH ALLEN WITT and JOHN EARL
12 GRIFFIN hacked the computer network of B-1, a business located in Seattle, WA, and installed
13 malicious software used to harvest and steal data, including usernames and passwords.

14 16. The data that JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN stole from
15 the computer network of B-1 included the username and password for B-1's Officedepot.com
16 account. With those credentials, JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN
17 connected over the Internet to B-1's Officedepot.com account, and placed orders for computers
18 and computer equipment that totaled approximately \$15,500.00

19 17. On or about May 27, 2008, JOSHUAH ALLEN WITT and JOHN EARL
20 GRIFFIN hacked the computer network of B-2, a business located in Seattle, WA, and installed
21 malicious software used to harvest and steal data, including credit card account numbers that
22 belonged to J.L., an owner of B-2, and also B.N., P.T., K.B., T.S., E.S., J.M., who were
23 customers of B-2. JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN then used those credit
24 card account numbers (access devices) fraudulently, over the Internet, in the following ways,
25 among others:

26 a. They used the stolen credit card account number of B.N. to make \$8,144.98 in
27 fraudulent online purchases for items that included car parts and technology-related equipment;
28

1 b. They used the stolen PayPal account of P.T. to remove \$6,890.34 from associated
2 credit card accounts and use it for fraudulent funds transfers and purchases of merchandise,
3 including a wireless booster antenna, extended life laptop computer batteries, and multiple
4 purchases of car audio equipment and car parts;

5 c. They used stolen credit card accounts of T.S. to fraudulently purchase
6 approximately \$6,000.00 in merchandise;

7 d. They used the stolen credit card account of E.S. to fraudulently purchase
8 merchandise that included tool kits designed for use by firefighters for gaining entry to locked
9 buildings;

10 e. They used the stolen credit card account of J.M. to fraudulently purchase
11 approximately \$5,500.00 in merchandise.

12 18. On or before November 1, 2008, JOSHUAH ALLEN WITT and JOHN EARL
13 GRIFFIN hacked the computer network of B-5, a commercial business located in downtown
14 Seattle, WA. Once they had done so, they installed various malware programs that they intended
15 to, and did use maliciously to capture and steal data, and also altered and destroyed or otherwise
16 damaged the business's network or data contained on and in it.

17 19. On or about November 1, 2008, JOSHUAH ALLEN WITT and JOHN EARL
18 GRIFFIN stole the access credentials for B-5's online ADP payroll account, and then used the
19 access credentials they had stolen from B-5 to get unauthorized access, over the Internet, to B-5's
20 ADP payroll account.

21 20. On or about November 7, 2008, JOSHUAH ALLEN WITT and JOHN EARL
22 GRIFFIN stole personally identifiable and bank account information belonging to B.S., the
23 owner of B-5.

24 21. On or about November 7, 2008, JOSHUAH ALLEN WITT and JOHN EARL
25 GRIFFIN connected over the Internet to the online payment service, "Paypal," fraudulently
26 opened a Paypal account under the name of B.S., and connected the Paypal account with B.S.'s
27 Bank of America personal checking account.

1 22. On or about November 9, 2008, JOSHUAH ALLEN WITT and JOHN EARL
2 GRIFFIN connected over the Internet to the online auction service, "eBay," where they
3 fraudulently opened an account that they associated with the Paypal account they had previously
4 fraudulently opened under the name of B.S.

5 23. During the period from November 9, 2008, through November 30, 2008,
6 JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN placed bids and purchased or attempted
7 to purchase approximately 16 different items from the account they had fraudulently opened on
8 eBay under the name of B.S., which items included a 2006 Dodge Charger 5.7 L Hemi Engine
9 for a price of \$3,949.99, a 2006 Charger 300 C Hemi 5.7L Engine Transmission for a price of
10 \$4,249.00, several laptop computers at a cost of several thousand dollars, a new Rolex watch at a
11 cost of \$5,490.90, and multiple long range booster antennas at a cost of \$89.00 each.

12 24. On or about November 12, 2008, JOSHUAH ALLEN WITT and JOHN EARL
13 GRIFFIN connected over the Internet to the online bank, "Metabank," where they opened
14 multiple Metabank accounts under the name of B.S., and also under the names of R.D., and T.B.,
15 who were employees of B-5.

16 25. On or about November 19, 2008, JOSHUAH ALLEN WITT and JOHN EARL
17 GRIFFIN fraudulently established a Quickbooks payroll account with Intuit, using company
18 information belonging to B-5, and linked B-5's Bank of America business checking account to
19 the Quickbooks payroll account. JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN then
20 added the owner of B-5 and four other employees as payroll recipients to the Quickbooks payroll
21 account, and scheduled disbursements to these accounts totaling \$36,158.49.

22 26. On or about November 15, 2008, through November 23, 2008, JOSHUAH
23 ALLEN WITT and JOHN EARL GRIFFIN made a series of fraudulent purchases, and also
24 account transfers on and from a Visa credit account issued by the Bank of America to B-5, which
25 included a series of transfers to the Intuit payroll account that had previously been fraudulently
26 established by JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN.

27 27. On or about November 17, 2008, JOSHUAH ALLEN WITT and JOHN EARL
28 GRIFFIN stole the access credentials for B-5's online account with Geeks.com, which account

1 was commonly used by the business for procurement of electronic equipment and supplies.
2 JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN then connected over the Internet to
3 Geeks.com, and used the stolen access credentials of B-5 to place an order for the purchase of a
4 Toshiba Protege computer, at a cost of \$1521.24.

5 28. On or about November 19, 2008, JOSHUAH ALLEN WITT and JOHN EARL
6 GRIFFIN stole the logon credentials for the Amazon.com account used by B-5. JOSHUAH
7 ALLEN WITT and JOHN EARL GRIFFIN then connected over the Internet to Amazon.com and
8 used the stolen logon credentials of B-5 to place an order for a Lenovo Laptop computer at a cost
9 of \$3091.96.

10 29. On or about November 24, 2008, JOSHUAH ALLEN WITT and JOHN EARL
11 GRIFFIN gained unauthorized access to B-5's computer network, and from that network, gained
12 unauthorized access to B-5's ADP payroll account. While logged into B-5's ADP payroll
13 account, JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN replaced existing payroll
14 destination deposit account numbers with the account numbers for the Metabank accounts they
15 had fraudulently opened under the names of B.S., R.D., and T.B. They also changed the rate of
16 pay for the owner and these two employees. The total attempted theft of payroll funds that
17 resulted was \$11,499.07.

18 30. Beginning on or about November 25, 2008, JOSHUAH ALLEN WITT and JOHN
19 EARL GRIFFIN used stolen personal identifying information to open loadable debit card
20 accounts at Metabank under the names of C.S., W.F., A.F., A.B., J.W., D.S., and B.S., who were
21 employees of B-5.

22 31. On or about December 10, 2008, JOSHUAH ALLEN WITT and JOHN EARL
23 GRIFFIN again gained unauthorized access to B-5's ADP payroll account. While logged into B-
24 5's ADP payroll account on this occasion, JOSHUAH ALLEN WITT and JOHN EARL
25 GRIFFIN replaced existing payroll destination deposit account numbers for additional
26 employees, with the account numbers for the Metabank accounts they had fraudulently opened
27 under the names of those six individuals. They also changed the rate of pay for these individuals.
28 The combined attempted theft of payroll funds totaled approximately \$15,141.26.

1 32. On or about February 9, 2009, JOSHUAH ALLEN WITT and JOHN EARL
2 GRIFFIN used the "war-driving" technique to locate the WiFi network of B-7, and once they had
3 located the network, used software programs to reconnoiter the network to assess its relative
4 security and possible vulnerabilities. JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN
5 then successfully hacked the computer network of B-7, and configured the network to give
6 themselves remote access.

7 33. Once JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN had successfully
8 hacked the computer network of B-7, they connected over the Internet to the online bank,
9 Metabank, where they opened multiple Metabank accounts under the names of employees of B-7,
10 including N.A., A.D., A.L., P.F., T.V., N.W., D.H., M.H., T.S., and D.B.

11 34. After they had established those multiple Metabank accounts, JOSHUAH ALLEN
12 WITT and JOHN EARL GRIFFIN opened a Quickbooks payroll account for B-2, which they
13 then linked to B-7's business banking account.

14 35. During the period from February 12, 2009, through March 2, 2009, JOSHUAH
15 ALLEN WITT and JOHN EARL GRIFFIN initiated "payroll" transfers of funds from the
16 business banking account of B-7, and routed them through the Quickbooks payroll account they
17 had opened under the name of B-2, to the Metabank accounts they had opened under the names
18 of B-7 employees. The transfers initiated and made or that were attempted to be made in this
19 way totaled approximately \$75,305.59.

20 36. On or about August 21, 2009, JOHN EARL GRIFFIN illicitly obtained a laptop
21 computer that belonged to, or had been issued to an employee of B-10, a nonprofit organization
22 located in Seattle, WA. JOHN EARL GRIFFIN found and used remote desktop credentials
23 saved to the laptop computer to gain unauthorized access to the computer network of B-10.

24 37. After accessing the computer network of B-10, JOHN EARL GRIFFIN and
25 JOSHUAH ALLEN WITT opened accounts with loadable debit cards through Metabank, under
26 the identities of R.H., the president and CEO of B-10, and also under the identity of J.P., who
27 was an employee of B-2.

1 38. JOHN EARL GRIFFIN and JOSHUAH ALLEN WITT thereafter opened
2 Quickbooks accounts, and attempted to transfer money from the company accounts of B-10,
3 through the Quickbooks accounts, to the loadable debit cards issued through Metabank for R.H.
4 and J.P.

5 39. JOHN EARL GRIFFIN and JOSHUAH ALLEN WITT also used the credit card
6 accounts of B-10 employees for purchases and for PayPal fund transfers.

7 40. On or about November 22, 2009, BRAD EUGENE LOWE burglarized B-11, and
8 stole computer equipment.

9 41. On or about May 16, 2010, JOHN EARL GRIFFIN, JOSHUA ALLEN WITT and
10 BRAD EUGENE LOWE burglarized B-15, and stole computers and servers, among other things.

11 42. On or about May 20, 2010, JOHN EARL GRIFFIN, JOSHUA ALLEN WITT,
12 and BRAD EUGENE LOWE hacked the computer network of B-16, a business located in
13 Seattle, WA, and stole personally identifiable information and user credentials for the business
14 and its employees, including VPN credentials for remote user access to the company's computer
15 network. In the weeks that followed, JOHN EARL GRIFFIN, JOSHUA ALLEN WITT and
16 BRAD EUGENE LOWE made multiple attempts to access B-16's computer network, some of
17 which were made by piggy-backing onto wireless Internet access accounts of third parties who
18 resided in close proximity to JOHN EARL GRIFFIN's father, to JOHN EARL GRIFFIN's
19 girlfriend, or in close proximity to the residence of BRAD EUGENE LOWE.

20 43. On or about July 31, 2010, JOSHUAH ALLEN WITT and BRAD EUGENE
21 LOWE burglarized B-30, a company in Renton, WA. During the burglary, JOSHUAH ALLEN
22 WITT and BRAD EUGENE LOWE stole laptop computers, desktop computers, computer
23 peripherals, servers, and other property from B-30, with a total value of approximately
24 \$170,600.00. JOSHUAH ALLEN WITT and BRAD EUGENE LOWE fenced much of this
25 stolen equipment.

26 44. After they had burglarized B-30, JOSHUAH ALLEN WITT and BRAD EUGENE
27 LOWE provided JOHN EARL GRIFFIN with access to laptop computers they had stolen from
28

1 B-30, so that he could he search those laptop computers for saved access credentials that would
2 facilitate hacking the computer network of B-30.

3 45. JOHN EARL GRIFFIN found, and then exploited VPN credentials on laptop
4 computers stolen from B-30 to hack the computer network of B-30.

5 46. On or about August 15, 2010, JOHN EARL GRIFFIN installed malware on the
6 computer network of B-30 in order to capture and steal data that included usernames and
7 passwords to online accounts that belonged to B-30.

8 47. Using data that JOHN EARL GRIFFIN stole from the computer network of B-30,
9 JOHN EARL GRIFFIN, JOSHUA ALLEN WITT and BRAD EUGENE LOWE placed orders on
10 B-30's account with Zones.com for merchandise that included laptop computers and WiFi
11 booster antennas, for a total cost of \$15,478.72.

12 48. On or about August 22, 2010, JOHN EARL GRIFFIN, JOSHUA ALLEN WITT,
13 and BRAD EUGENE LOWE attempted to effect an online transfer of \$9,200.00 from the Paypal
14 account of B-30 to an account that had been fraudulently established by JOHN EARL GRIFFIN,
15 JOSHUA ALLEN WITT and BRAD EUGENE LOWE at Zion Bank.

16 49. On or about August 24, 2010, JOHN EARL GRIFFIN, JOSHUA ALLEN WITT,
17 and BRAD EUGENE LOWE attempted to effect an online transfer of \$6,850.00 from the Paypal
18 account of B-30 to an account that had been fraudulently established by JOHN EARL GRIFFIN,
19 JOSHUA ALLEN WITT and BRAD EUGENE LOWE at Metabank.

20 50. As part of their hack of the computer network of B-30, JOHN EARL GRIFFIN,
21 JOSHUA ALLEN WITT, and BRAD EUGENE LOWE took control of B-30's e-mail server,
22 which gave them the ability to read, redirect, and destroy e-mail messages to and from B-30
23 employees.

24 51. As part of their hack of the computer network of B-30, JOHN EARL GRIFFIN,
25 JOSHUA ALLEN WITT, and BRAD EUGENE LOWE stole hundreds of internal company
26 documents, e-mail messages, and spreadsheets, including a spreadsheet that contained the names,
27 dates of birth, social security numbers, and salaries of over 50 company employees.
28

1 52. As part of their hack of the computer network of B-30, JOHN EARL GRIFFIN,
2 JOSHUA ALLEN WITT, and BRAD EUGENE LOWE deleted data, including logging records,
3 that would have evidenced their hacking activities on that computer network.

4 53. On or about August 19, 2010, JOHN EARL GRIFFIN hacked the computer
5 network of B-31, and installed malware that included a key-logging program that he used to
6 capture data that included customer credit card, and also personally identifiable information for
7 those same customers.

8 All in violation of Title 18, United States Code, Section 371.

9
10 **COUNT 2**

11 **(Intentionally Causing and Attempting to Cause Damage to a Protected Computer**
12 **and Thereby Causing Loss in Excess of \$5,000)**

13 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
14 through 14 of Count 1 of this Indictment.

15 2. Beginning at a time uncertain, but no later than August 15, 2010, and continuing
16 until at least August 31, 2010, within the Western District of Washington and elsewhere,
17 JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN knowingly
18 caused and attempted to cause the transmission of a program, information, code, and command,
19 including, in particular, the transmission and installation of the "CAIN" software program, and
20 also commands causing the alteration of VPN and Exchange logs, and as a result of that conduct,
21 intentionally caused and attempted to cause damage, without authorization, to a computer
22 belonging to, and used in interstate commerce and communications by B-30, a business located
23 in Renton, WA, and by such conduct caused a loss from a related course of conduct affecting one
24 or more other protected computers aggregating at least \$5,000 in value during a one-year period.

25 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b),
26 1030(c)(4)(B), and 2.

1
2
3 **COUNT 3**

4 **(Intentionally Causing and Attempting to Cause Damage to a Protected Computer**
5 **and Thereby Causing Loss in Excess of \$5,000)**

6 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
7 through 14 of Count 1 of this Indictment.

8 2. Beginning at a time uncertain, but no later than August 19, 2010, and continuing
9 until at least December 15, 2010, within the Western District of Washington and elsewhere,
10 JOHN EARL GRIFFIN knowingly caused and attempted to cause the transmission of a program,
11 information, code, and command, including, in particular, the transmission and installation of the
12 "eBlaster" and the "Abel" software programs, and as a result of that conduct, intentionally caused
13 and attempted to cause damage, without authorization, to a computer belonging to, and used in
14 interstate commerce and communications by B-31, a business located in Seattle, WA, and by
15 such conduct caused a loss from a related course of conduct affecting one or more other protected
16 computers aggregating at least \$5,000 in value during a one-year period.

17 All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), 1030(b),
18 1030(c)(4)(B).

19
20 **COUNT 4**

21 **(Accessing a Protected Computer without Authorization to Further Fraud)**

22 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
23 through 14 of Count 1 of this Indictment.

24 2. On or about April 27, 2008, within the Western District of Washington and
25 elsewhere, JOSHUAH ALLEN WITT and JOHN EARL GRIFFIN knowingly and with intent to
26 defraud, accessed and attempted to access a protected computer that belonged to B-1, a business
27 located in Seattle, WA, without authorization and in excess of authorization, and by means of
28 such conduct furthered an intended fraud by stealing the username and password for B-1's

1 Officedepot.com account, which information JOSHUAH ALLEN WITT and JOHN EARL
2 GRIFFIN then used fraudulently to place orders online through Officedepot.com for computers
3 and computer equipment exceeding \$5,000 in value within a period of one year.

4 All in violation of Title 18, United States Code, Section 1030(a)(4), 1030(b),
5 1030(c)(3)(A), and 2.

6
7 **COUNT 5**

8 **(Accessing a Protected Computer without Authorization to Further Fraud)**

9 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
10 through 14 of Count 1 of this Indictment.

11 2. On or about August 14, 2010, within the Western District of Washington and
12 elsewhere, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN
13 knowingly and with intent to defraud, accessed and attempted to access a protected computer that
14 belonged to B-30, a business located in Redmond, WA, without authorization and in excess of
15 authorization, and by means of such conduct furthered an intended fraud by stealing the
16 username and password for B-30's account with Zones.com, which information JOSHUAH
17 ALLEN WITT, BRAD EUGENE LOWE, and JOHN EARL GRIFFIN then used fraudulently to
18 place orders online through Zones.com for merchandise that included laptop computers and WiFi
19 booster antennas exceeding \$5,000 in value within a period of one year.

20 All in violation of Title 18, United States Code, Section 1030(a)(4), 1030(b),
21 1030(c)(3)(A), and 2.

22
23 **COUNT 6**

24 **(Access Device Fraud)**

25 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
26 through 14 of Count 1 of this Indictment.

27 2. Beginning on or about November 24, 2008, and continuing until on or about
28 December 2, 2008, in the Western District of Washington and elsewhere, JOSHUAH ALLEN

1 WITT and JOHN EARL GRIFFIN, knowingly and with intent to defraud, effected transactions
2 with the American Express credit card account number (#*****7008) issued to J.M., of
3 Moultonborough, N.H., to receive services and merchandise that included "hide-my-ip" services
4 from a company located in California, and auto parts from vendors located in Ohio and
5 Tennessee, the combined retail value of which services and merchandise totaled \$5,500.48, said
6 conduct affecting interstate and foreign commerce.

7 All in violation of Title 18, United States Code, Section 1029(a)(5), 1029(b), and 2.

8
9 **COUNT 7**

10 **(Aggravated Identity Theft)**

11 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
12 through 14 of Count 1 of this Indictment.

13 2. Beginning on or about November 24, 2008, and continuing until on or about
14 December 2, 2008, in the Western District of Washington and elsewhere, JOSHUAH ALLEN
15 WITT and JOHN EARL GRIFFIN knowingly transferred, possessed and used, without lawful
16 authority, a means of identification of another person, to wit, the name and personally
17 identifiable American Express credit card number of *****7008 belonging to J.M., of
18 Moultonborough, N.H. during and in relation to a felony listed in Title 18, United States Code,
19 Section 1028A(c), to wit, Access Device Fraud, in violation of Title 18, United States Code,
20 Section 1029.

21 All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

22
23 **COUNT 8**

24 **(Access Device Fraud)**

25 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
26 through 14 of Count 1 of this Indictment.

27 2. Beginning on or about December 6, 2008, and continuing until on or about
28 December 20, 2008, in the Western District of Washington and elsewhere, JOSHUAH ALLEN

1 WITT and JOHN EARL GRIFFIN, knowingly and with intent to defraud, effected transactions
2 with the Capital One credit card account number (#*****4600) issued to S.G., of Eagle
3 County, CO, to receive merchandise that included auto parts from a vendor located in Nebraska, ,
4 the combined retail value of which merchandise totaled approximately \$9,100.00, said conduct
5 affecting interstate and foreign commerce.

6 All in violation of Title 18, United States Code, Section 1029(a)(5), 1029(b), and 2.

7
8 **COUNT 9**

9 **(Aggravated Identity Theft)**

10 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
11 through 14 of Count 1 of this Indictment.

12 2. Beginning on or about December 6, 2008, and continuing until on or about
13 December 20, 2008, in the Western District of Washington and elsewhere, JOSHUAH ALLEN
14 WITT and JOHN EARL GRIFFIN knowingly transferred, possessed and used, without lawful
15 authority, a means of identification of another person, to wit, the name and personally
16 identifiable Capital One credit card number of #*****4600 belonging to S.G., of Eagle
17 County, CO, during and in relation to a felony listed in Title 18, United States Code, Section
18 1028A(c), to wit, Access Device Fraud, in violation of Title 18, United States Code, Section
19 1029.

20 All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

21
22 **COUNT 10**

23 **(Aggravated Identity Theft)**

24 1. The Grand Jury re-alleges and incorporates as if fully set forth herein Paragraphs 1
25 through 14 of Count 1 of this Indictment.

26 2. On or about August 14, 2010, in the Western District of Washington and
27 elsewhere, JOSHUAH ALLEN WITT, BRAD EUGENE LOWE and JOHN EARL
28 GRIFFIN knowingly transferred, possessed and used, without lawful authority, a means

1 numbers of over 50 employees of B-30, a business in Renton, WA, during and in relation to
2 a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Accessing a Protected
3 Computer without Authorization to Further Fraud in violation of Title 18, United States Code,
4 Section 1030.

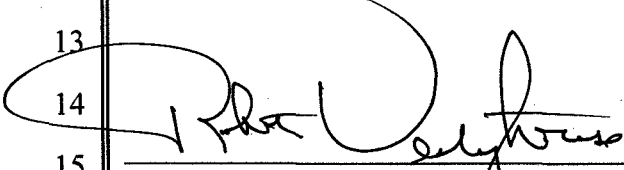
5 All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

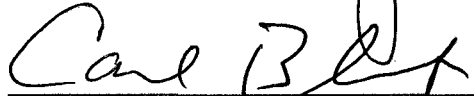
7 A TRUE BILL:


9 DATED:

10 Signature of the Foreperson redacted pursuant
11 to the policy of the Judicial Conference

12 _____
13 FOREPERSON

14 
15 _____
16 JENNY A. DURKAN
United States Attorney

17 
18 _____
19 CARL BLACKSTONE
Assistant United States Attorney

20 
21 _____
22 KATHRYN A. WARMA
Assistant United States Attorney