

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW MEXICO

IN THE MATTER OF THE SEARCH OF:
7100 GLADDEN AVENUE, NE,
ALBUQUERQUE, NM 87110

Case No. _____

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Michael Boady, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as 7100 GLADDEN AVENUE, NE, ALBUQUERQUE, NM 87110, hereinafter "PREMISES," further described in Attachment A, for the things described in Attachment B.

2. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws. I have been a Special Agent (SA) with the Federal Bureau of Investigation ("FBI") for almost seven years. I have participated in investigations of computer crimes, crimes against children on the Internet and, among other things, have conducted or participated in surveillance, the execution of search warrants, and debriefings of informants. Through my training, education and experience, I have become familiar with the manner in which computers, computer equipment, software, and electronically stored information are used in furtherance of criminal activity.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

PROBABLE CAUSE

4. Since October 2010, the Albuquerque Division of the FBI has been investigating a pattern of criminal activity causing a significant loss of money for several New Mexico retail stores including OfficeMax, Office Depot, and Staples.

5. The OfficeMax MaxPerks Loyalty program issues a reward card number that allows each of their customers to earn gift card rewards toward future OfficeMax purchases. There are two types of MaxPerks accounts, "MaxPerks for Teachers" and "MaxPerks for Business" accounts. The Business account is available for any customer. For every \$500 spent at OfficeMax using the Business reward card, OfficeMax rewards that customer with \$25 in MaxPerks reward certificates, which are issued monthly. The Teacher accounts are more lucrative and only available to teachers. Every \$75 spent at OfficeMax using the Teacher reward card results in a \$10 MaxPerks reward certificate, which is issued quarterly and has an annual maximum of \$100.

6. If a customer signs up in person, he/she fills out the registration card and immediately receives a MaxPerks card with a MaxPerks account number. If the customer registered online, the MaxPerks card is provided electronically to be printed out. When signing up for an account, customers are asked to provide their name, address, phone, type of account (business or teacher), and email. Each MaxPerk account can be accessed online by providing the customer's email or account number and a password. To get credit for a purchase made at an OfficeMax, the customer can provide the cashier with either his/her MaxPerks card number, telephone number, or mailing address associated with the account. The purchase is then associated with that MaxPerks account.

7. If the customer forgets to utilize his/her card during the purchase, the customer can log-in to his/her account via the internet and add the purchase to it. An online adjustment requires four pieces of information: the store number, date, register number, and transaction number. This information is located on the store receipt. At the end of the month or quarter, depending on the type of account, the customer can log-in to his/her account and print out the rewards. These rewards are credits towards future OfficeMax purchases and cannot be redeemed for cash.

8. All MaxPerks customers are allowed to participate in the ink and toner cartridge recycling program. The ink and toner recycling program is intended to protect the environment by recycling cartridges that would otherwise be discarded. Customers can return their cartridges to OfficeMax and receive \$3 per cartridge, with a maximum of \$60 per month.

9. To receive rewards for recycling ink or toner cartridges, a customer is required to spend an equal amount at OfficeMax prior to issuance. For example, if a customer brings five ink cartridges to OfficeMax for recycling, his or her MaxPerks account must reflect a "qualified purchase balance" of \$15 before the customer will be issued the \$15 MaxPerks award.

10. The terms and conditions for the MaxPerks program, which must be agreed before setting up an account, limit one MaxPerks account per person. MaxPerks rewards are not transferrable.

Discovery of the Fraud

11. Around August 2010, OfficeMax discovered that the MaxPerks loyalty program began to show a significant increase in MaxPerks rewards claimed from customer purchases.

12. OfficeMax suspected fraud and began to investigate the accounts used to claim the rewards. The OfficeMax investigation identified over 5,400 MaxPerks accounts that were set

up between March 3, 2010 and January 24, 2011, with similarities in the subscriber information and/or method of payment(s) that led OfficeMax to believe it was the same individual(s) who set up all of the accounts.

13. To date, the created accounts have generated approximately \$179,373 in rewards, which were issued to Matthew Channon ("CHANNON"), the suspected perpetrator of the schemes. Of the approximately \$179,373 in rewards, OfficeMax was successful in voiding approximately \$133,000 of the pending rewards before they were received by CHANNON. Additionally, OfficeMax was able to void approximately \$11,888 in rewards which had previously been issued to CHANNON, prior to him using them. OfficeMax believes that if the fraud had not been discovered, the company could have paid out approximately \$540,000 dollars for the over 5,400 accounts that were created.

14. To execute the MaxPerks scheme, the fraudster had to perform several tasks. First, since each Teacher account only allows a \$100 payout annually, the fraudster had to set up numerous "MaxPerks for Teachers" accounts and associate each one with a different name, email address, and mailing address. The MaxPerks program requires a unique email address and mailing address for each reward account, to prevent a person from having more than one account.

15. Next, the fraudster had to be able to claim in-store purchases previously made by other customers that were not already associated with a MaxPerk reward account. In order to claim a purchase online, the fraudster had to obtain certain pieces of information about the in-store purchases.

16. To execute the portion of the scheme involving the cartridge recycling, the fraudster needed have access to large quantities of spent ink or toner cartridges and also needed a

large number of MaxPerks accounts. As mentioned previously, each account is allowed to recycle only 20 cartridges per month for \$3 each (for a total of \$60), and for every dollar in ink rewards, an equal amount of money had to be spent at OfficeMax.

MaxPerks Accounts

17. Of the over 5,400 MaxPerks accounts identified by OfficeMax, approximately 5,287 were created with one of four email sequences: Bargle12345678, Garble12345678, Coach12345678, and Teechur12345678, (herein referred to as "BARGLE", "GARBLE", "COACH", and "TEECHUR"). Additionally, OfficeMax identified approximately 96 accounts, which are referred to as "Elementary Accounts," which are discussed further in paragraphs 28 and 29 below.

18. Before a MaxPerk account can be set up online, the email address associated with the account must be validated - that is, the customer will receive an email at the email account provided and will have to click on a link to confirm that they are the email account holder. All of the accounts were associated with Google Mail ("Gmail") accounts. The sequencing of the email addresses appears to be computer generated. The periods inserted within the sequences make them appear unique to OfficeMax. For example, the MaxPerks system recognizes B.argle12345678@gmail.com to be a distinct email address from Ba.rgle12345678@gmail.com.

19. The business names of the BARGLE, GARBLE, COACH, and TEECHUR accounts also appear to be computer generated. For many of these accounts, the member's address or city was part of the member's listed business name. The name was the city or address plus "Elementary School," "Academy," or similar. An example of this would be that an account registered to Denver, CO would have the business name of "Denver Elementary School."

20. Apart from the BARGLE, GARBLE, COACH, and TEECHUR accounts, OfficeMax identified approximately 120 accounts that appear to have been part of the same scheme. As with many of the accounts associated with those four sequences, these 120 other accounts all have a business name using the city or address plus "Elementary School." These accounts did not have email addresses associated with them. This could be because the account was set up in the store and the registrant did not provide one, or it could be that the registrant logged into the account and deleted the email associated with it.

21. According to Google, Gmail accounts do not recognize special characters such as a period ("."). An email sent to C.OA.CH.1.23.4.5.6.7.8@gmail.com, where there are periods placed between the alpha-numerical characters, is recognized by Gmail as being sent to COACH12345678@gmail.com. Therefore, only one Gmail address is associated with all of the different COACH email sequences; the same is true for the BARGLE, GARBLE, and TEECHUR sequences.

22. There were approximately 2,358 "BARGLE" accounts created between June 4, 2010 and August 5, 2010. The subscriber information for this account, provided by Google, includes the following:

Name: Bargle Bargleton

Email: bargle12345678@gmail.com

Secondary Email: Teechur12345678@gmail.com

Created on: 2010/06/04-18:36:41-UTC

IP: 166.205.9.207, on 2010/06/04-18:36:41-UTC

23. There were approximately 1092 "GARBLE" accounts created between August 17, 2010 and September 17, 2010. The subscriber information for this account, provided by Google, includes the following:

Name: Garble Garbleton

Email: garble12345678@gmail.com

Secondary Email: bargle12345678@gmail.com

Created on: 2010/08/17-16:28:35-UTC

Registration IP: 204.8.156.142 on 2010/08/17-16:28:35-UTC

24. There were approximately 908 "COACH" accounts created between May 4, 2010 and June 4, 2010. The subscriber information for this account, provided by Google, includes the following:

Name: Coach Alphabet

Email: coach12345678@gmail.com

Secondary Email: sws11@live.com

Created on: 2010/05/05-02:00:49-UTC

Registration IP: 98.230.199.128 on 2010/05/05-02:00:49-UTC

25. There were approximately 920 "TEECHUR" accounts created between March 3, 2010 and April 22, 2010. The subscriber information for this account, which was provided by Google includes the following:

Name: Tee Chur

Email: teechur12345678@gmail.com

Created on: 2010/03/09-01:32:00-UTC

Registration IP: 166.205.9.73, on 2010/03/09-01:32:00-UTC

26. It should be noted that the BARGLE, COACH, and TEECHUR accounts have all been accessed from IP address 192.251.226.206. This confirms that all of the accounts have likely been accessed from the same computer network and is likely the same person. Additionally, as mentioned above, the GARBLE account provided the BARGLE account as a secondary email address.

27. This chart provides a sampling of the typical subscriber information that was provided for the suspicious MaxPerks accounts.

Business Name	Contact Name	Address	City	State	Phone	Email Address
HOUSTON ACADEMY	MARIA R CROSS	3044 GAMBLER LANE	HOUSTON	TX	281-966- 8904	T.EECH.UR12345678@GMAIL.COM
MOUNTAIN VIEW ELEMENTARY SCHOOL	DAMIAN E VICKERY	3089 GROVE AVENUE	MOUNTAIN VIEW	OK	580-347- 3093	TEECH.U.R.12345678@GMAIL.COM
WASHINGTON ELEMENTARY SCHOOL	RUTH R ROYER	905 LAKE FLOYD CIRCLE	WASHINGTON	DC	301-944- 5281	TEECH.U.R.12345678@GMAIL.COM
TIFTON ELEMENTARY SCHOOL	ANTHONY R LOTT	1557 JUNKINS AVENUE	TIFTON	GA	229-556- 2971	TEECH.UR.12345678@GMAIL.COM
EAGLEVILLE ELEMENTARY SCHOOL	SONIA S BASH	1787 FRANKLEE LANE	EAGLEVILLE	PA	484-597- 7646	TEECHU.R.12345678@GMAIL.COM
THOUSAND OAKS ELEMENTARY SCHOOL	HOLLY D BAKER	1292 LEISURE LANE	THOUSAND OAKS	CA	805-491- 2314	TEECHUR.12345678@GMAIL.COM

As is demonstrated by the bolded selections, the business name and the city usually have commonalities. A review of the account subscriber information provided by the fraudster showed that the physical addresses provided were invalid.

28. The chart below is a sampling of the "Elementary Accounts" of which there were approximately 96:

Business Name	Contact Name	Address	City	ST	Zip	Phone
CUYAHOGA FALLS ELEMENTARY SCHOOL	BARGLE12345678@GMA J WARD	1482 BRIARHILL LANE	CUYAHOGA FALLS	OH	44221	3302509319
MAPLEWOOD ELEMENTARY SCHOOL	BARGLE12345678@GMAIL D KILLINGER	2289 LAUREL LEE	MAPLEWOOD	MN	55119	6517329326
PITTSBURGH ELEMENTARY SCHOOL	BARGLE12345678@GM L KUHL	4136 STILES STREET	PITTSBURGH	PA	15226	4125615136

29. Although the “Elementary Accounts” do not have an email address associated with them, in some instances, like those above, the contact name included the “BARGLE” email sequence and then a name (e.g. J Ward). These discrepancies give cause to believe that the accounts were created through the use of a computer script—that is, a list of commands that can be executed without user interaction—and that this script was improperly configured, leading to errors such as the entry of the BARGLE email sequence in the name field.

Online Adjustments

30. As mentioned above, if a customer forgets to provide his/her MaxPerks information when making a purchase at a store, he/she can go online to the MaxPerks website, log-in from his/her home computer, and add four pieces of information from the receipt (store number, register number, receipt number, and date of purchase) associated with the purchase they made. The customer’s MaxPerks account will then be credited for that sale. Below is a picture of where those items would be found on a typical OfficeMax receipt and where they

could be added to a MaxPerks account online:

ADD A RECEIPT close

Enter a receipt to receive credit for a purchase made in a store without your MaxPerks ID card.

Credit for purchases made in a store will appear in your account on the "My Rewards" page within 2 - 3 business days.

* = Required Information

* Store #:

* Register #:

* Receipt #:

* Transaction Date: (mm/dd/yyyy)

SUBMIT

You may submit receipts for purchases occurring in the last 90 days only. Purchases older than 90 days are not valid for MaxPerks credit.

store # receipt #

OfficeMax

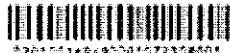
OfficeMax #001
1316A SOUTHERLAND ROAD
DOWNEY #0010 JC 60748
40879 40-6077

Tell us about your shopping experience
and enter to win 1 of 3 prizes. Visit
www.officemax.com/survey/rewards
to enter and to view these terms and
conditions of entering the survey.

0001141967950	\$9.29
GST Refractable 0.7 Tax At	
Subtotal	\$9.29
Tax 0.000	\$0.00
TOTAL	\$9.29
Cash	\$10.00
Change	\$0.71

21661510
0001 00001 40690 6 07/23/08
00100834 01:07:13 PM

ORDER BY PHONE 1-877-OFFICEMAX



020100169490001072308001

31. In order to execute the scheme, the fraudster would have to be able to claim purchases made by legitimate customers. To accomplish this, he would first go to an OfficeMax store around the country and make a purchase, thereby obtaining a legitimate receipt.

32. The fraudster would then log-in to one of the previously created MaxPerks accounts. Using the information from the receipt, the fraudster would be able to deduce previous and future purchases at OfficeMax by using the four pieces of information from his receipt. Since the store number and register number do not change, the fraudster is believed to have written a computer script that repeatedly decremented and/or incremented the receipt number by

one to claim previous and future purchases made at that store. Furthermore, the fraudster could take notice of how many registers were in the store and increment and/or decrement the register number accordingly to claim purchases at other registers.

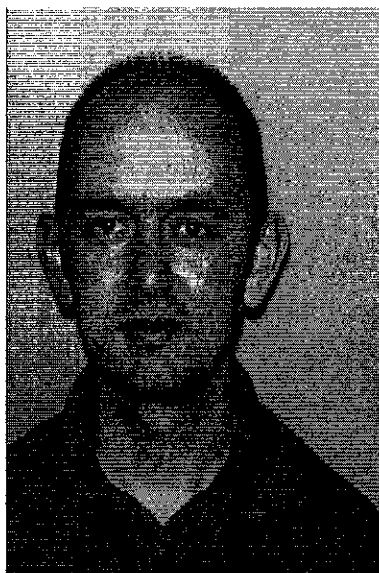
33. Since each account only allowed \$100 in rewards annually (corresponding to \$750 in purchases), the fraudster would use the numerous accounts he set up to claim transactions up to \$750 worth of purchases. At that point, the account was no longer used to claim transactions, since the account reached the annual reward limit of \$100.

34. Between May and September 2010, there were over 58,000 transactions adjusted online relating to the suspicious accounts. This is an average of 482 transactions per day. Assuming a keying time of 30 seconds per transaction, it would take about 4.2 hours per day to key that many transactions. This number excludes any adjustments that were not accepted by the system because they had already been awarded, were mis-keyed, or did not match a specific transaction. On one date there were 1,172 transactions keyed, which using this logic would require over 9.7 hours of continuous keying.

35. Taking into consideration the volume of adjustments done per day, the sequencing of the Gmail addresses that were registered, and the unique subscriber details provided for each account, it would be unlikely that someone manually entered this information. The most viable explanation is that a computer script was employed to parse through the different email account possibilities, placing periods in different places to create MaxPerks accounts, and then apply the MaxPerks online adjustments.

Identifying the Fraudster

36. Investigation had identified the individual who is believed to be the perpetrator of the fraud scheme as Matthew CHANNON, who resides at 7100 Gladden Ave, Albuquerque, NM. Below is a copy of his NM Driver's License Photo:



37. A review of the over 4,500 MaxPerks accounts believed to have been created by CHANNON identified several accounts that were set up using either a home address, email address, P.O. Box, and/or telephone number that is directly linked to CHANNON. Some of the examples of this are shown in the chart below:

Account #	Name	Address	City	State	Phone	Email
45422487	CSOL CORP	7100 GLADDEN AVE	ALBUQUERQU E	NM	505-242- 6289	stoopido@aol.com
648012993	CONVENIENT VIDEO	PO BOX 90504	ALBUQUERQUE	NM	408-598- 1528	cvid.us@gmail.com
629459324	OMICRON CONSULTANTS	7100 GLADDEN AVE	ALBUQUERQUE	NM	520-857- 0685	je.h.najehnsen@gmail.com

38. On March 30, 2011, the Honorable W. Daniel Schneider, United States Magistrate Judge for the District of New Mexico issued a search warrant authorizing a search of thirteen Google email ("GMAIL") accounts believed to be created and controlled by CHANNON, including, the BARGLE, TEECHUR, COACH, GARBLE sequences, hydrazok@gmail.com, jeahnajehnsen@gmail.com, matchannonconsulting@gmail.com, cvidus@gmail.com, [jqqqq@gmail.com](mailto:jrqqqq@gmail.com), mahashamaranka@gmail.com, amclay2@gmail.com, smoked@gmail.com, and furnituu@gmail.com.

39. During a review of those email accounts, there were emails received in all of the searched accounts which further confirmed that the accounts were CHANNON's. The cvidus@gmail.com account had numerous emails from Staples and OfficeMax that confirmed that the account was being used to accept proceeds from fraud. One example of how these accounts confirm that they are CHANNON's, in the cvidus@gmail.com account, CHANNON established a Netflix account associated with this email address with the following subscriber information:

Matt Channon
7100 GLADDEN AVE NE
PMB 8
ALBUQUERQUE, NM 87110-1464

40. There was also an eBay account setup with the cvidus@gmail.com account which on at least one occasion purchased an item and had it shipped to:

Matt Channon
7100 Gladden Av NE
Albuquerque, NM 87110

41. Information provided by Google provided the following subscriber information for the jeahnajehnsen@gmail.com account:

Name: Jehn Ajehnsen

Created on: 2009/11/11-03:40:24-UTC

Registration IP: 166.205.5.173, on 2009/11/11-03:40:24-UTC

42. During a review of the jeahnajehnsen@gmail.com account, on May 1, 2010, an email was received in this account showing that a car GPS device was purchased from Staples, which was to be mailed to the following address:

JEHNAJ EHNSSEN
7100 NE Gladden Ave., NE
PMB 288C
Albuquerque, NM 87110

It is believed that JEHNAJ EHNSSEN is a fictitious name that CHANNON used to make a purchase using his fraudulently obtained Staples rewards. Investigative databases confirm that there is no one with that name who resides at that address.

PayPal Debit Card

43. Through a review of transactions in which fraudulently acquired MaxPerks Reward certificates were used to make purchases, a personal debit card was identified that was used to pay the remaining balances on the transactions. The debit card is a PayPal debit card ending in 4445, which is registered to CHANNON. In other words, when a MaxPerks account did not have sufficient rewards to cover the full amount of the purchase, the personal debit card registered to CHANNON would be used to cover the difference.

44. The debit card registered to CHANNON has been directly connected to approximately 82 of the suspect MaxPerks accounts and to over 227 transactions in which fraudulently acquired MaxPerks Rewards and a debit card registered to CHANNON were both used. All of these accounts also have a significant number of online adjustments.

45. Below is a partial transaction record showing a purchase of \$161.04 in merchandise from OfficeMax in which three fraudulently acquired \$50 MaxPerks rewards certificates were used and then the remaining balance of \$11.04 was paid with the debit card registered to CHANNON:

Date/Time	Customer receipt	Audit receipt	Customer signature
9/20/2010 8:02:30 PM	01: Access Code: 202336		
9/20/2010 8:09:08 PM	0: STAN Code: 212100		
	0: Remaining Balance: \$0.00		
Type:	11: Gift Card		(\$50.00)
Sale	11: Entry Method:Keyed		
<input type="checkbox"/> Voided	11: Acct #*****5519		
<input type="checkbox"/> Training	0: Approved Authorization CD: 20050000		
<input type="checkbox"/> Offline	0: Access Code: 867885		
Total	0: STAN Code: 212100		
161.04	0: Remaining Balance: \$0.00		
	12: Gift Card		(\$50.00)
	12: Entry Method:Keyed		
	12: Acct #*****3717		
	0: Approved Authorization CD: 10000001		
	0: Access Code: 101666		
	0: STAN Code: 212100		
	0: Remaining Balance: \$0.00		
	13: Gift Card		(\$50.00)
	13: Entry Method:Keyed		
	13: Acct #*****5688		
	0: Approved Authorization CD: 20050007		
	14: Debit		(\$11.04)
	14: Auth Entry Method:Scanned		
	14: Acct #*****4445 Exp Date 5/31/2011		
	Card Holder: MATT		
	0: OOO Authorization CD:		
	0: PrintEvent PrintID = 111 EventID = RCO111 Description = iPhone App		
	End of Transaction: # 2121 9/20/2010 08:09 PM		
	0: Operator Sign Off: PFENNER		
	0: OPERATOR SIGNED ON: PFENNER :		

46. Records from OfficeMax show that on numerous occasions the debit card registered to CHANNON was used in stores outside of New Mexico to make purchases, including Arizona, Missouri, Texas, Colorado, Wisconsin, California, Illinois and Nevada. As seen in the transaction record below, a fraudulently acquired \$80 MaxPerks reward certificate was used to purchase merchandise in Phoenix, Arizona on June 9, 2010, and the remaining balance of \$15.71 was paid with the debit card registered to CHANNON:

Store: 743 Register: 1 Operator: NKRAUS Receipt Num: 6208	
Date/Time:	Customer receipt Audit receipt Customer signature
6/9/2010 12:57:14 PM	5: Store Coupon # 17079011060610 (20%) (\$21.90)
6/9/2010 12:59:28 PM	6: Store Coupon # 17079011060610 (20%) (\$21.90)
Type:	7: Store Coupon # 17079011060610 (20%) (\$21.90)
Sale	8: Store Coupon # 17079011060610 (20%) (\$21.90)
<input type="checkbox"/> Voided	9: Store Coupon # 17079011060610 (20%) (\$21.90)
<input type="checkbox"/> Training	0: Store Coupon # 17079011060610 (20%) (\$21.90)
<input type="checkbox"/> Offline	0: SUBTOTAL \$87.57
Total:	0: \$5.78
95.71	0: \$0.61
	0: \$1.75
	0: TOTAL \$95.71
	0: SUBTOTAL \$87.57
	0: \$5.78
	0: \$0.61
	0: \$1.75
	0: TOTAL \$95.71
	0: Access Code: 229835
	0: STAN Code: 620800
	0: Remaining Balance: \$0.00
	11: Gift Card (\$80.00)
	11: Entry Method: Keyed
	11: Acct # *****6202
	0: Approved Authorization CD: 20080005
	12: Debit (\$15.71)
	12: Auth Entry Method: Scanned
	12: Acct # *****4445 Exp Date 5/31/2011
	Card Holder: MATT
	0: DDD Authorization CD:
	0: PrintEvent PrintID = 96 EventID = RC096 Description = Fed Ex Sweepstakes
	End of Transaction: # 6208 6/9/2010 12:59 PM

47. Some of the email accounts that were identified by OfficeMax through the use of the PayPal debit card registered to CHANNON included mattchannonconsulting@gmail.com, mahashamaranka@gmail.com, jrqqqq@gmail.com and smokedb@gmail.com. Each of these account were associated with several purchases made using the debit card registered to CHANNON. The accounts were left open until June 20, 2011, and were still being used by CHANNON for fraud.

48. The mahashamaranka@gmail.com account has been used by CHANNON to profit from fraud as recently as May 25, 2011, at an OfficeMax store in San Francisco, CA. On at least five occasions, OfficeMax was able to obtain video of CHANNON using the mahashamaranka@gmail.com account at stores in Arizona, California, and New Mexico. With this account, CHANNON has received and used over \$1,700 worth of MaxPerks Rewards.

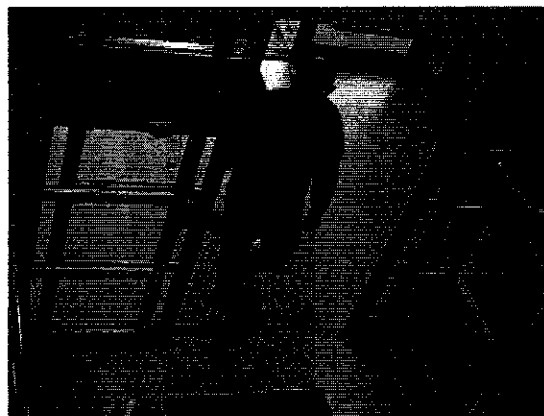
49. The mattchannonconsulting@gmail.com MaxPerks account was registered with an Albuquerque address and the phone number 505-344-4322, which is associated with

CHANNON. The smokedb@gmail.com MaxPerks account was registered with P.O. Box 90504, which is the same address provided for the MaxPerks Convenientvideo account.

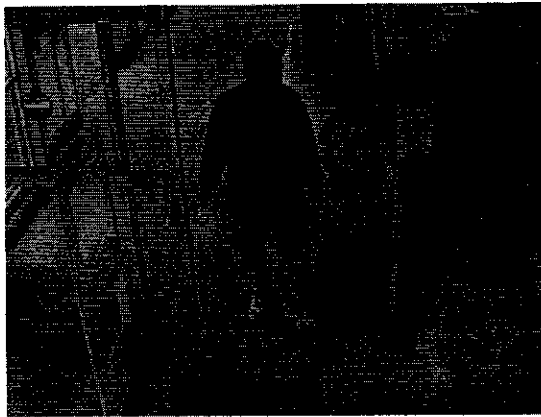
50. The mahashamaranka@gmail.com email address was used for nine different OfficeMax accounts, with periods (".") randomly placed between the alpha-numeric characters. Several of these accounts were directly connected to the debit card registered to CHANNON. All nine were left open by OfficeMax and are still being used.

Video Evidence

51. OfficeMax obtained video of CHANNON conducting fraudulent transactions on several occasions. The below photograph was taken on November 22, 2010, as he was entering an OfficeMax store in Albuquerque, NM to conduct a transaction reported to be fraudulent.



52. The below photograph was taken on November 22, 2010, as CHANNON entered a different OfficeMax store in Albuquerque, NM, to conduct a transaction reported to be fraudulent.



53. The below photograph is from a video of CHANNON making a transaction reported to be fraudulent at OfficeMax store in Tuscon, Arizona on December 21, 2010:



54. On several occasions, video evidence shows a female who is believed to be an accomplice to CHANNON. This female traveled to stores throughout the country and made purchases using the fraudulent MaxPerks Rewards certificates as well. On November 22, 2010 and November 23, 2010, the female was observed walking in to the OfficeMax stores in Albuquerque just prior to CHANNON entering the stores. She recycled ink on an account that

had previously been identified as CHANNON's by OfficeMax. Below are two of the screenshots that were taken from Albuquerque OfficeMax stores:



55. The female has been identified as Brandi Lucero ("LUCERO"). According to Lucero's driver's license information, LUCERO resides at 7100 Gladden Ave., Albuquerque, NM 87110, with CHANNON. Below is the driver's license photograph of LUCERO which confirms that she is the accomplice who was identified by OfficeMax:



56. The MaxPerks account to which LUCERO credited the returned ink was associated with amclay2@gmail.com, which is registered to an address in Tempe, Arizona. This MaxPerks account was previously associated with CHANNON because the debit card registered to CHANNON was once used in connection with the account.

Making an Initial Purchase

57. Information provided by OfficeMax shows that MaxPerks accounts associated with CHANNON were redeemed in at least 21 different states. Subpoena records from Southwest Airlines also confirm that CHANNON has traveled to many of these states in and around the time the fraudulent transactions were made.

58. A review of the online adjustments and video from OfficeMax stores shows on numerous occasions CHANNON would make a purchase. Then, shortly after the purchase, online adjustments from other customers purchases, both before and after CHANNON's, would begin to show up as being associated with CHANNON's MaxPerks accounts.

59. After discovering the fraud, OfficeMax shut down the majority of the suspicious MaxPerks accounts but decided to keep approximately 120 suspicious accounts open in order to

assist with the ongoing investigation. The accounts left open were the ones that did not fall under the four different email chains (BARGLE12345678, GARBLE12345678, COACH12345678, and TEECHUR12345678).

Recent Activity

60. More recently, OfficeMax has changed their online adjustments program to require that the actual amount of purchase be provided to claim a purchase. Since that change, on November 30, 2010, CHANNON was caught on video in an OfficeMax store in Albuquerque, NM, where he made a purchase while taking note of the amounts spent by other individuals who were ahead of him and/or behind him in line. Online adjustments confirmed that those customers' purchases were later claimed as purchases on suspected MaxPerks accounts associated with CHANNON.

61. In addition to observing the purchases of others, CHANNON has also devised a scheme using the approximately 120 accounts that were left open by OfficeMax to profit from recycling empty ink and toner cartridges. Based on information provided by eBay, between September 2009 and August 2010, eBay accounts associated with CHANNON were used to purchase over 14,000 empty ink jet cartridges.

62. The average price paid by these eBay accounts for a cartridge is \$0.355. Recycling the cartridge at OfficeMax yields a \$3.00 credit, which would have netted about \$38,000 in profit. Since each account is only allowed 20 ink cartridges per month, CHANNON used his 120 MaxPerks accounts to allow him to recycle 2400 cartridges per month (120 x 20). To receive payment for recycling the ink, a customer must spend an equal amount to receive the rewards. It appears that CHANNON had been purchasing debit cards from OfficeMax and associating them with the 120 accounts. Then, CHANNON would recycle ink on that same

account, up to \$60 per month, which resulted in OfficeMax issuing him a Reward Certificate for the amount spent.

63. To date, OfficeMax has identified approximately \$46,375 worth of ink recycling rewards that have been issued to CHANNON. According to OfficeMax, they believe that the cost to CHANNON for each \$60 Reward certificate that he received from ink recycling is no more than \$9. OfficeMax advised that this scheme is in violation of the policy agreement that every customer must agree to in order to obtain a MaxPerk account.

64. As recently as May 25, 2011, CHANNON was identified at OfficeMax stores in California, recycling ink with the MaxPerks accounts that were not shut down.

eBay/PayPal Records

65. As mentioned above, investigation has discovered that CHANNON was connected to several eBay accounts, which he used to sell items obtained with MaxPerks rewards.

Account ID	Name	Address	City	State	Email	Phone
doctor_zoidberg	Matt J Channon	7100 Gladden Av NE	Albuquerque	NM	hydrazok@gmail.com	505-344-4322
convenientvideo	Matthew J Channon	7100 Gladden Av NE	Albuquerque	NM	cvidu.s@gmail.com	408-598-1528
rmamyway	Chris Channon	12245 Yellowstone NE	Albuquerque	NM	cchannon@yahoo.com	505-292-5393
furnitu	Convenient Video	P O Box 90504	Albuquerque	NM	furnituu@gmail.com	505-344-4322

66. The "doctor_zoidberg" eBay account, which is connected to email account hydrazok@gmail.com, has sold approximately 1,200 items including ink cartridges, computer media (DVD-R's, CDR's, flash drives, etc.), printers, telephones, and computer equipment, most of which can be purchased at OfficeMax, Staples, and Office Depot stores. The total value of items sold was over \$45,000 USD from this account. Additionally, this account has made

numerous purchases including coupons for Staples and OfficeMax, ink cartridges, and computer equipment. According to transaction records, these coupons were used in addition to the fraudulently acquired MaxPerks Rewards to purchase items from OfficeMax at a discount.

67. On February 25, 2011, in an undercover capacity, the writer made a bid for Canon 210XL 211XL Ink Cartridges, which were being sold on eBay with the doctor_zoidberg account. On February 27, 2011, the writer was informed that the auction had been won by the writer and that the eBay item was in Albuquerque, NM.

68. The doctor_zoidberg account allowed payment to be received via the PayPal account associated with hydrazok@gmail.com. Therefore, the writer paid for the item and requested that it be shipped to an FBI controlled address in Dallas, TX. After paying for the item on PayPal, the writer received a receipt showing that the Payment was to Channon Silichem, which had a customer service email address of hydrazoic@aol.com. In addition to the receipt from PayPal, the writer received a receipt from eBay showing that the item had been won from Matt J. Channon, Albuquerque, NM 87110.

69. Information provided by Google provided the following subscriber information for the hydrazok@gmail.com account:

Name: Matt Channon		
Created on: 2009/11/04-22:16:39-UTC		
IP: 76.113.79.124, on 2009/11/04-22:16:39-UTC		
Date/Time	Event	IP
2010/12/27-14:49:03-UTC	Logout	174.56.56.220
2010/12/27-14:23:57-UTC	Login	174.56.56.220
2010/12/26-16:52:52-UTC	Logout	174.56.56.220
2010/12/26-15:24:51-UTC	Login	174.56.56.220
2010/12/25-22:23:50-UTC	Login	166.205.11.35

70. The "convenientvideo" eBay account, which is connected to email account cvidu.s@gmail.com and is registered with CHANNON's name and address, has purchased

thousands of empty ink cartridges and OfficeMax coupons. Furthermore, on September 22, 2010, this account placed a \$300 OfficeMax MaxPerks Rewards Certificate Gift Card up for auction on eBay. The Furnitu eBay account purchased this certificate. It is believed that CHANNON put the gift card up for auction, but in an attempt to prevent someone from purchasing it for less than the desired price, he purchased it from himself using the Furnitu account.

71. As mentioned previously, the cvidus@gmail.com account was used to create an eBay account and a MaxPerks Rewards account. Information provided by Google included the following subscriber information for the cvidus@gmail.com account:

Name: Convenient Video
Created on: 2009/09/04-01:35:47-UTC
IP: 76.18.86.2, on 2009/09/04-01:35:47-UTC
Other Usernames: cvid.us@gmail.com

72. From the "rmamyway" eBay account, which is connected to email account cchannon@yahoo.com, over \$31,000 worth of items have been sold, including a significant number of cameras and camera equipment.

73. From the "furnitu" eBay account, which is associated with furnituu@gmail.com, over \$4,700 worth of items have been sold, including Office Depot Rewards Certificates valued at \$1,647.77, OfficeMax MaxPerks Rewards certificates valued at \$3,122, and Staples Rewards Certificates valued at \$2,100. The eBay subscriber information for the furnitu account includes the following:

User ID: furnitu
Full Name: Convenient Video
Contact Info: Convenient Video, P O Box 90504, Albuquerque, NM, 87199, 505-344-4322 5
Shipping Address: M. J. Channon, 1829 Commercial Street N.E., Albuquerque, NM, 87102.

74. Information provided by Google provided the following subscriber information for the furnituu@gmail.com account:

Name: Furnit U
Created on: 2009/11/22-09:23:12-UTC
IP: 166.205.137.71, on 2009/11/22-09:23:12-UTC

Date/Time	Event	IP
2010/12/18-13:12:21-UTC	Logout	174.56.56.220
2010/12/18-13:11:51-UTC	Login	174.56.56.220

This IP address, 174.56.56.220, is the same used to log-in to the hydrazok@gmail.com email account.

Prepaid Gift Cards

75. From November 2009 through September 2010, the Furnitu and the doctor_zoidberg accounts logged into eBay from an IP address 98.230.199.128. That IP address is registered to Comcast Cable and appears to be a customer in the Albuquerque, NM area. CHANNON was a Comcast subscriber at that time. In October 2010, CHANNON's home internet service changed to Qwest, and the Furnitu and the doctor_zoidberg began logging in from IP addresses associated with Qwest instead. Furthermore, the first bill that CHANNON received from Qwest was paid using American Express Debit Card number 3743-2869-1820-263.

76. The American Express (AMEX) Debit Card used to pay CHANNON's Qwest bill, 3743-2869-1820-263, was purchased in an OfficeMax store in Albuquerque, NM with fraudulently acquired MaxPerks Rewards certificates. That same card was also used on October 21, 2010, to make purchases at a Staples store in Framingham, MA for \$32.82. Prior to making the purchase, a balance-inquiry call was placed from telephone number 505-888-6288 to the American Express IVR number on the back of the debit card.

77. In addition to the above-mentioned AMEX card, on October 23, 2010, MaxPerks rewards from accounts associated with CHANNON purchased three other AMEX Gift Cards, numbers 3790-1446-3184-790, 3743-2876-6943-727, and 3790-1446-3185-078. A review of the transaction detail for those gift cards show that these cards were used to make payments at establishments in the Albuquerque area.

78. According to information provided by Qwest, CHANNON's Qwest account includes the following subscriber information:

Name: Matt Channon
Address: 7100 Gladden Ave NE, Albuquerque, NM 87110
Phone: 505-888-6288

As mentioned above, the 505-888-6288 number is the number used to call American Express to determine the balance on a fraudulently acquired gift card.

Shipping Packages

79. On numerous occasions, CHANNON is believed to have visited OfficeMax stores around the country, including Texas, Illinois, Oregon, Washington, Pennsylvania, and California, and purchased items with the suspicious MaxPerks Rewards at an OfficeMax store. Then, using the MaxPerks Rewards as payment, the items would be shipped via FedEx, a service offered by OfficeMax, to CHANNON's residence in Albuquerque, NM.

80. As recently as January 26, 2011, a person using the name of MATTHEW CHANNON has used the FedEx services at OfficeMax to send packages, paid for with the suspicious MaxPerks Rewards.

81. Between December 28, 2009 and January 18, 2010, someone using the name Chris Channon ("CHRIS") sent five FedEx Packages from an OfficeMax store in Albuquerque, NM. Four of the five were paid for with a gift card ending in 9211 and a pre-paid American

Express card ending in 3557, while the other item that was shipped from CHRIS was paid for with the PayPal debit card registered to CHANNON ending in 4445. The address used by the sender was 12245 Yellowstone Rd., NE, Albuquerque, NM, which is the residence of CHRIS, who is believed to be a relative of CHANNON's.

Channon's Background

82. The writer conducted a "Google search" on www.Google.com for 'Convenient Video' and discovered the following:

Convenient Video, 7100 Gladden Ave NE, 87110, telephone 505-888-6288
Principal: Matthew Channon.

The 505-888-6288 number was also used to register the Qwest service at his residence and to call the American Express IVR service to determine the balance of a card he purchased with MaxPerks Rewards.

83. CHANNON's "Linked-in" profile shows he has extensive computer knowledge.

84. CHANNON obtained a Masters in Computer and Electrical Engineering at Georgia Tech and Bachelors in Material Engineering at New Mexico Tech.

85. CHANNON maintains a website for a solar power business at www.silichem.com, which includes the following contact information on the website: 7100 Gladden Ave., Albuquerque, NM 87110, telephone number 408-598-1528. The 408-598-1528 number is the same one he used to register the "Convenient Video" eBay and MaxPerk accounts.

86. The Silichem.com account was registered with Tucows.com, a domain registrar, with the following information:

Matt Channon
hydrazo.k@gmail.com
7100 Gladden Ave NE
Albuquerque, NM 87110

505-344-4322

As mentioned previously, the hydrazok@gmail.com account was used to register the doctor_zoidberg eBay account. Additionally, the 505-344-4322 number was also used for the doctor_zoidberg and furnitu eBay accounts.

Staples

87. When Staples was informed of the potential fraud, Staples reviewed its database and discovered over \$10,000 in losses connected to CHANNON, who is believed to have executed a similar scheme related to their rewards program and the recycling of ink.

88. Investigation conducted by Staples identified 89 Staples Rewards accounts that are believed to be CHANNON's, including four that were directly connected to CHANNON, either by name, address, or telephone number, which were:

Member #	2189783844	2062562935	2121820126	2090794708
Name	Matt Channon	Matt Channon	C. T. Teaching	Convenient Video
Address	7100 GLADDEN AVE NE	PO BOX 37451	PMB 1105 7100 GLADDEN AVE NE	PO BOX 90504
Phone	505-344-4322	505-344-4322		408-598-1528
Email	<u>stoopido@aol.com</u>	<u>mattchannonconsulting@gmail.com</u>	<u>j.rqqqq@gmail.com</u>	<u>cvid.us@gmail.com</u>

89. A review of all transactions associated with these four Staples Rewards Accounts discovered 10 Credit Card Accounts and 1 Debit Card. A review the transaction history for each of the cards identified an additional 85 rewards accounts linked to CHANNON.

90. The cards identified by Staples that appear to have been used by CHANNON include the following:

- PayPal debit card 4445

- Mastercards ending in 1482, 1841, 2248, and 7503
- Visa Cards ending in 1710 and 1945
- American Express Cards ending in 0533, 0577, 1116, and 3811

As mentioned previously, the PayPal debit card ending in 4445 is the same card that was used to purchase items from OfficeMax.

91. Based on the transaction history of the 89 Staples Rewards accounts it appears that CHANNON is primarily recycling ink and then using the Ink Recycling Rewards Checks, along with Staples Coupons, to purchase electronic items at a reduced price. A total of 3,728 cartridge recycles were associated with the 89 rewards accounts, resulting in the issuance of \$10,703 worth of Ink Recycling Rewards Checks since August 2009.

92. Only one Staples Rewards Account is permitted per customer, per household. Customers are allowed to recycle up to 10 Ink/Toner Cartridges per month. Customers receive \$2 per cartridge (formerly \$3 per cartridge), payable monthly in the form of an Ink Recycling Rewards Check that can be redeemed at any Staples Store.

Office Depot

93. As mentioned above, eBay accounts associated with CHANNON were used to sell over \$1,600 worth of Office Depot Rewards Cards. Office Depot found four accounts, including [jqqqq@gmail.com](mailto:jrqqqq@gmail.com) and smokedb@gmail.com, which have paid over \$2,200 in Office Depot Rewards. Office Depot identified those four accounts because all four were associated with the PayPal Debit Card registered to CHANNON ending in 4445.

94. According to Office Depot, in or around April 2011, the smokedb@gmail.com account was scheduled to pay \$485 in Rewards, but Office Depot was not able to identify any purchases made by this account which would justify the Reward. This suggests that CHANNON may be using an additional scheme at Office Depot.

TECHNICAL TERMS

95. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. Storage medium: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, floppy disks, flash memory, CD-ROMs, and several other types of magnetic or optical media not listed here.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

96. As described above and in Attachment B, this application seeks permission to search for records that might be found on the PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage

media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

97. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files.

Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on review of the evidence related to this investigation, I am aware that computer equipment was used to generate and store documents and records used in the above mentioned fraud schemes.

98. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, registry information, configuration files, user profiles, e-mail, e-mail address books, “chat,” instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic

programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. When an individual uses a computer to commit fraud, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

99. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires agents to seize physical storage media and later review the media consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it

will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

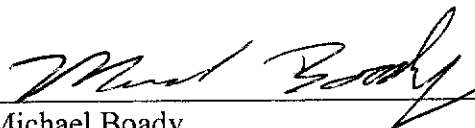
100. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), when officers executing the warrant conclude that it would be impractical to review the media on-site, the warrant I am applying for would permit officers either to seize or to image-copy storage media that reasonably appear to contain some or all of the evidence described in the warrant, and then later examine the seized storage media or image copies consistent with the warrant. The examination may require searching authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

hard drive to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

101. I submit that this affidavit supports probable cause for a warrant to search the PREMISES described in Attachment A and seize the items described in Attachment B.

Respectfully submitted,



Michael Boady
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me
on June 27, 2011:



UNITED STATES MAGISTRATE JUDGE