

CASE REPORT

NATIONAL GALLERY DC

Tracy's iPhone [2012-07-15-National-Gallery]

TABLE OF CONTENTS

Case Report	1
National Gallery DC	1
Executive Summary	3
Details of Tracy's iPhone.....	3
Evidence to establish Personas.....	4
Evidence relating to theft of valuable stamps	5
Evidence relating to Defacement of Museum Art.....	5
Plot Timeline.....	6
Email Content.....	6
SMS Message Content.....	11
Wi-Fi/GPS location information.....	12
Conclusion	14
Supplemental Materials	15

EXECUTIVE SUMMARY

On January 21, 2016, DigiTech Inc. was called in to assist with the National Gallery, Washington DC (NGDC) case involving the conspiracy associated with the theft of valuable stamps and defacing of museum of art at the NGDC.

- Tracy is a suspect in the above-mentioned conspiracy.
- As part of the investigation, Tracy's iPhone was taken into custody.
- DigiTech Inc. was tasked with investigating evidence relevant to the above-mentioned conspiracy.

As described fully in this report, DigiTech, Inc. made the following findings:

1. There was collusion between Tracy, Pat, and King to steal stamps from the NGDC.
2. Tracy had provided internal NDGC information to Carry for a flash mob. It was a scheme to damage foreign artwork.

DETAILS OF TRACY'S IPHONE

Name	Findings	Location in iPhone image file
Model	iPhone1,2	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
Host Name	Tracy Sumtwelve's iPhone	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log.1
OS Version	iPhone OS 4.2.1 (8C148)	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
Install Time	Created: 6/6/2012 12:03:28 -0700	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log
User Email	tracy.sumtwelve@nationalgallerydc.org tracysumtwelve@gmail.com	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail
Phone Number	1 (703) 340-9661	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
Serial Number	86004482Y7H	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/AppleSupport/general.log

ICCID	89014103255195342366	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/logs/lockdownd.log
IMEI	012021003735398	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/root/Library/Lockdown/activation_records/wildcard_record.plist

Hashes

MD5 34c4888f095dc3241330462923f6fea5

SHA256 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607

EVIDENCE TO ESTABLISH PERSONAS

This section establishes aliases, phone numbers, emails addresses associated with each person, and relationships between each individual.

Tracy:

Phone Number: (703) 340-9961
 Email: tracysumtwelve@gmail.com
 Work email: tracy.sumtwelve@nationalgallerydc.org
 Alias email: coralbluetwo@hotmail.com
 Relationship: Accused

Pat:

Phone Number: (571) 308-3236
 Email: perryatsum@yahoo.com
patsumtwelve@gmail.com
 Relationship: Tracy's brother & accomplish

Terry:

Phone Number: (703) 829-6071
 Email:
 Relationship: Daughter of Tracy & Joe

Joe:

Phone Number:
 Email: joe.sum.twelve@gmail.com
 Relationship: Tracy's ex-husband and Terry's father.

Carry:

Phone Number: (202) 725-2124

Email: carrysum2012@yahoo.com
Relationship: Acquaintance of Tracy

King:
Email: throne1966@hotmail.com
Relationship: Acquaintance of Pat

Evidence relating to theft of valuable stamps

This sub-section provides details regarding the evidence found as it relates to the theft of valuable stamps.

Tracy, Pat, and King were discussing with each other how to steal valuable stamps from the NGDC. Tracy's phone contained images of stamps that they were interested in stealing.

Pat emailed King telling him about the planned stamp heist at NGDC and is asking for his assistance. This is a blackmail attempt by implying King's parole could be compromised if he doesn't assist with the scheme.

King replies with an attached document listing the tools he will need.

Pat forwards the email from King to Tracy.

Pat texts Tracy letting her know that her friend (actually Tracy) will need to change the attached file to a PDF format.

Tracy emails herself ZIP file containing three pdf files. They are memos about stamp insurance; the specific stamps and the insurance amount for each.

Evidence relating to Defacement of Museum Art

This sub-section provides details regarding the evidence found as it relates to the Defacement of Museum art.

Tracy was communicating with Carry to assist with a “flash mob” (a ruse to deface artwork at NGDC). A later message sets up another meeting with Carry so that Tracy can bring Carry’s tablet in with her. Tracy asks Carry how it is going via text message.

PLOT TIMELINE

Tuesday, June 19, 2012	Pat sends Tracy information about using a virtual machine and installing Virtual Box.
Thursday, July 5, 2012	SMS conversation between Tracy and Carry about meeting up at Bubba’s grill.
Friday, July 6, 2012	Tracy meets Carry at Bubba’s grill.
Friday, July 6, 2012 ----	Messages between Tracy, Pat, and King about what tools are needed for the stamp heist.
Tuesday, July 10, 2012	
Sunday, July 08, 2012	Tracy photographs the stamps that they are interested in stealing.
Monday, July 09, 2012	Tracy sends herself copies of insurance memos for specific stamps.
Wednesday, July 11, 2012	Tracy meets Carry again to bring the tablet in with her.
Thursday, July 12, 2012	Tracy asks Carry about the status of the “flash mob”.

EMAIL CONTENT

/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/Protected Index

Master Timeline of NGDC				
Artifact #	Timestamp	Header Information	Key Information	Evidence

				Location
1	Tue, 19 Jun 2012 13:06:33 - 0700 (PDT)	patsumtwelve@gmail.com TracySumtwelve@gmail.com Subject: Paris Speak and answer	Pat -> Tracy [Translated from French] Considering proposal and response is yes. Pat comments that Tracy said having an alias. Requests email address and will provide further instructions.	Mailbox
2	6/19/2012 20:26:47	perrypatsum@yahoo.com TracySumtwelve@gmail.com Subject: Look me up sometime	Perry -> Tracy Checked in with Pat (brother) and should email with her alias	
3.	6/19/2012 21:38:59	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Crazydave by the VMs Attachment: Crazydave1.mp3	Pat (Perry) emails Tracy (Coral) with instructions to install a Virtual Machine embedded (around 1:23) in an audio file.	/img_tracy-phone-2012-07-15-final.E01/vol_v ol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/3896FC6F-A083-4D39-B0A2-CE68368D44CA.emlx
4.	6/19/2012 21:39:34	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Re: ???	Pat (Perry) replies to Tracy (Coral) confirming that he was getting her emails.	Mailbox
5.	6/21/2012 17:43:15	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Re: Crazydave by the VMs	Pat (Perry) replies to Tracy (Coral) on a email thread about Virtual Machine installation saying that she should listen to some other songs as well. In the email thread Tracy (Coral) confirms that the instructions sent earlier in the audio file helped her.	
6.	6/28/2012	perrypatsum@yahoo.com coralbluetwo@hotmail.com	Pat (Perry) emails Tracy (Coral) asking her to communicate using aliases and the VM setup to keep them safer. He	Mailbox

	19:31:33	Subject: Whats going on	<p>also indicates that they might have to get into riskier/illegal business since both of them were facing financial hardships.</p> <p>He tells her that few of his workplace friends were good at these businesses and that he will inform her should something pop-up; in the meantime they should keep discussing some ideas for the same.</p>	
7.	6/29/2012 14:21:56	<p>perrypatsum@yahoo.com coralbluetwo@hotmail.com</p> <p>Subject: Re: Whats going on</p>	<p>This is an email thread between Pat (Perry) and Tracy (Coral) discussing ideas for making some money.</p> <p>To Pat's suggestion that they use the Virtual Machines and aliases to communicate and keep looking for ways to make money, Tracy replies that she will keep her eyes open for opportunities and insists that Pat try to get in on some business soon, since her kid didn't want to change schools. She also indicates that she is paying attention to documents especially insurance papers so that she could identify something of potential. Pat assures that he will make something happen although he is nervous because IA has been sniffing around.</p>	
8.	6/29/2012 14:31:36	<p>perrypatsum@yahoo.com tracysumtwelve@gmail.com</p> <p>Subject: hey sis</p>	<p>Pat (Perry) emails Tracy addressing her as 'sister' and enquires about Terry. Asks her to check in with Coral with whom he has been planning some things. He also suggests all of them going together for dinner as friends. He asks Tracy to check in with Coral.</p>	
9.	6/29/2012 15:21:35	<p>perrypatsum@yahoo.com coralbluetwo@hotmail.com</p> <p>Subject: Re: Whats going on</p>	<p>Pat (Perry) replies to the email thread allaying Tracy's (Coral) concern about IA sniffing around him. Tracy in her earlier email in the thread says that although nothing interesting has turned up yet she expects something soon. Pat in his email mentions that they can certainly get the job done if something like what they had earlier discussed pops up.</p>	

10.	7/2/2012 16:13:18	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) mentioning that some interesting foreign exhibit is going to happen and that from assessing the paperwork she feels that it would be a big deal. Pat (Perry) replies back feeling hopeful about this being the opportunity they were looking for.	Mailbox
11.	7/2/2012 20:00:31	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Re: Some good news	Email thread: Some good news Following up on the earlier email about the exhibit, Tracy (Coral) mentions going through documents related to the exhibit from which she found that the exhibit is worth a lot of money but the shipping cost is very low comparatively. Pat (Perry) emails back saying that such a thing may mean that the exhibit is something small which would be a very good thing for them.	
12.	7/3/2012 13:29:37	joe.sum.twelve@gmail.com tracysumtwelve@gmail.com Subject: Re: Regarding Terry	Email Thread: Regarding Terry Tracy emails Joe asking whether he could help her with Terry's tuition this year since it is becoming too expensive for her. Joe replies back saying that he won't be paying Terry's tuition if she is not living with him.	
13.	7/3/2012 14:53:04	perrypatsum@yahoo.com coralbluetwo@hotmail.com Subject: Re: Some good news	Email Thread: Some good news Tracy (Coral) emails Pat (Perry) saying that the exhibit is rare and highly valuable stamp collection and that may be this is their opportunity. Pat (Perry) replies to Tracy (Coral) asking her to collect as much information as possible about the stamp exhibit and that in the meantime he would look into options for pulling off the heist.	
14.	7/5/2012 15:51:31	carrysum2012@yahoo.com tracysumtwelve@gmail.com Subject: Long time no see...	Carry reaches out to Tracy asking her if they could meet-up for lunch and suggests this Friday. She also mentions that through Facebook she realized that Tracy was having a hard time recently.	Mailbox

15.	7/6/2012 15:27:51	patsumtwelve@gmail.com tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy emailed Pat saying that she spoke with Coral and that Coral got some great news about her job and suggested that Pat catch up with Coral. Pat replied back saying that he knows a guy called King.	
16.	7/6/2012 15:49:31	patsumtwelve@gmail.com throne1966@hotmail.com Cc:coralbluetwo@hotmail.com Subject: can't pass up	Pat emails King with Tracy (Coral) in cc, saying that he has a lucrative proposition, a heist at national gallery. Compels King to help or his (King's) parole might be put in jeopardy.	
17.	7/6/2012 17:59:24	patsumtwelve@gmail.com tracysumtwelve@gmail.com Subject: Re: Good News	Email Thread: Good News Tracy suggests they (King, Tracy and Pat) should hang out sometime Pat emails Tracy with account login information for: coralblue@hotmail.com Password: legalBee	
18.	7/9/2012 14:44:11	tracysumtwelve@gmail.com coralbluetwo@hotmail.com Subject: things	documents.zip is a password protected compressed ZIP folder containing 3 insurance documents related to stamps. docs.zip is an encrypted ZIP folder containing 3 insurance documents related to stamps.	/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Library/Mail/POP-coralbluetwo@hotmail.com@pop3.live.com/INBOX.mbox/Messages/8A3BD06F-CDB1-4453-9C69-77E06823F2AE.emlx
19.	7/9/2012 18:18:47	carrysum2012@yahoo.com tracysumtwelve@gmail.com Subject: Re: Long time no see..	Email Thread: Long time no see... Tracy thanked Carry for the lunch. Carry emails Tracy asking for help to sneak a tablet in for a flash mob event they spoke about earlier. Implied that Tracy would be compensated in some	Mailbox

			way for the help.	
20.	7/10/2012 13:48:40	carrysum2012@yahoo.com tracysumtwelve@gmail.com Subject: Re: Long time no see...	Email Thread: Long time no see... Tracy agrees to help Carry sneak in the tablet. Asks when Carry would like to get in to take a look around the gallery. Carry replies saying that this would be a big help and asks if she could come around 9 tomorrow.	

SMS MESSAGE CONTENT

27.	6/12/2012 21:25:04	F: Pat T: Tracy	Pat asks Tracy about her plans for the weekend	SMS
28.	6/13/2012 17:30:28	F: Terry T: Tracy	I'm going out with dad after school for pizza! Thought I'd let you know if you planned to cook. T	SMS
29.	6/13/2012 18:30:38	F: Tracy T: Pat	Tracy replies to Pats message saying that she has no big plans and enquires about his plans.	SMS
30.	6/13/2012 18:33:46	F: Tracy T: Terry	Ok, sounds good.	SMS
31.	7/3/2012 14:04:32	F: Terry T: Tracy	Terry replies back saying that she doesn't want to switch schools and would rather stay with her dad and continue at Prufrock	SMS
32.	7/5/2012 18:18:23	F: Carry T: Tracy	Carry sets up the time and location as 1pm at Bubba's grill for meeting with Tracy	SMS
33.	7/5/2012 18:20:26	F: Tracy T: Carry	Tracy confirms the meeting time and location	SMS
34.	7/6/2012 15:02:19	F: Tracy T: Pat	Tracy asks Pat to give her a call	SMS
35.	7/6/2012 15:08:37	F: Pat T: Tracy	Pat says he is busy and suggests calling later	SMS
36.	7/6/2012 15:11:54	F: Tracy T: Pat	Tracy says its important and insists that pat call her soon	SMS

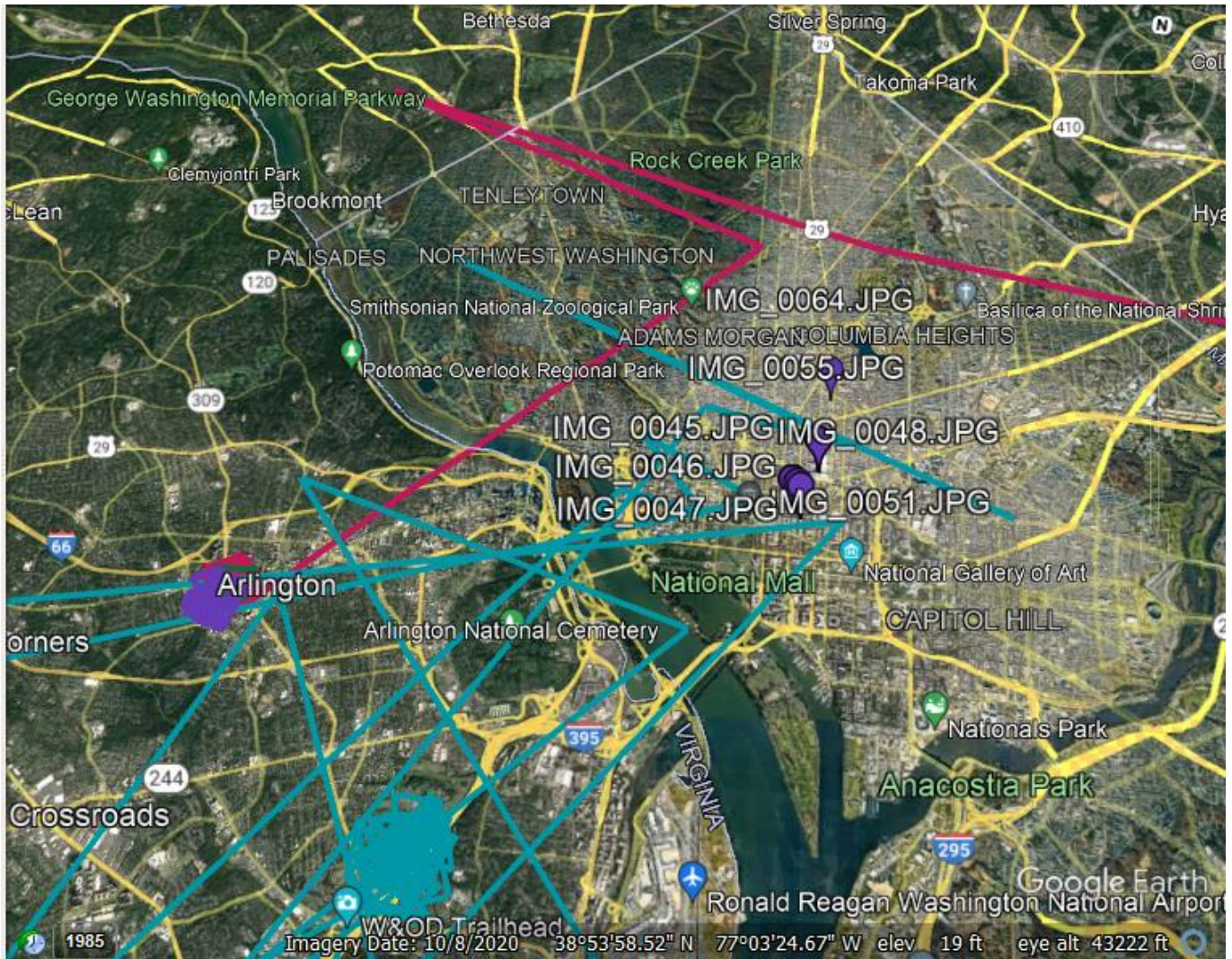
37.	7/6/2012 15:13:31	F: Pat T: Tracy	Pat says he will call in 5 min	SMS
38.	7/6/2012 15:18:50	F: Pat T: Tracy	Pat calls Tracy and they speak for 4 min 4 secs.	SMS
39.	7/6/2012 16:27:16	F: Carry T: Tracy	Carry messages saying she has a table inside	SMS
40.	7/6/2012 16:27:50	F: Tracy T: Carry	Tracy replies back saying that she will be there.	SMS
41.	7/10/2012 15:26:19	F: Pat T: Tracy	Pat messages Tracy telling her about the email and informing that the attachment needs to be changed to pdf. He asks Tracy to tell this information to Coral.	SMS
42.	7/10/2012 15:58:04	F: Tracy T: Pat	Tracy acknowledges the email and message.	SMS
43.	7/10/2012 16:37:09	F: Tracy T: Pat *Failed	Tracy tried to share the following location with Pat over MMS message but it failed. Location: 2600-2700 24th Rd S, Arlington, VA 22206	SMS
44.	7/10/2012 17:18:38	F: Tracy T: Terry	Tracy messages Terry for Lunch	SMS
45.	7/10/2012 18:19:24	F: Tracy T: Terry	Tracy messages Terry that she is back at work.	SMS
46.	7/10/2012 18:58:24	F: Terry T: Tracy	Terry messages Tracy saying she is busy and suggests meeting up over the weekend if her dad isn't busy.	SMS
47.	7/11/2012 12:41:45	F: Carry T: Tracy	Carry messages Tracy informing that she is almost there (National Gallery)	SMS
48.	7/11/2012 12:49:08	F: Tracy T: Carry	Tracy replies to Carry asking her to meet out front. She says that she will take the tablet in.	SMS
49.	7/13/2012 1:02:10	F: Terry T: Tracy	I really want to go to Dad's this weekend. He said he'll take me shopping for school	SMS

WI-FI/GPS LOCATION INFORMATION

/img_tracy-phone-2012-07-15-final.E01/vol_vol5/root/Library/Caches/locationd/consolidated.db

iphone-tracker.py (<https://gist.github.com/Schnouki/934357>) was used to massage the cell location data into a KML (Keyhole Markup Language) that could be fed into Google Earth and

plotted. Added in the locations of photos in /img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Media/DCIM/100APPLE that contained GPS location information in the EXIF Metadata. Uploading resultant `iPhone consolidated.db map.kml` as part of this report.



There is also an interactive Google Map with the above data points available at:

<https://www.google.com/maps/d/viewer?hl=en&hl=en&mid=1nC93bIMe2xZjd0dtuipIn0Kzt7XNtLix&ll=38.99275324256194%2C-77.06172395270083&z=11>

CONCLUSION

Evidence found on Tracy's iPhone indicated the following:

- Tracy used the alias Coral and Pat used the alias Perry.
- Tracy is under considerable financial strain from the divorce and paying for her daughter's tuition at Prufrock.
- From various correspondence, Tracy colluded with Pat and King to steal valuable stamps from the NGDC.
- The investigation also uncovered Tracy's willingness to give sensitive information to help Carry's "flash mob" project. Monetary compensation is implied.
- The stamp scheme was well planned with a list of required tools, copies of insurance memos, and photos of the stamps in question.

SUPPLEMENTAL MATERIALS



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

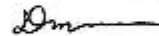
TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 25. Armed Forces Reserve	\$43,000.00
Lot # 26. Stamp of Kazakstan2	\$29,000.00
Lot# 27. BradyCo.	\$12,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann



President National Gallery DC

For The Internal use of National Gallery and MylStamp Collections Only.



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery DC, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 11. Woman's Profile	\$31,000.00
Lot # 12. Stamp of Kazakhstan	\$29,000.00
Lot# 13. 1929 Nepal	\$27,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MylStamp Collections Only.



NATIONAL GALLERY DC
WASHINGTON



Memorandum of Insurance Assurance:

TO: MylStamp Collections

In Regards to items owned or on loan to the National Gallery of Art, Washington from MylStamp Collections from the period of May 12, 2012 to May 12, 2013, all items in aforementioned list will be in the custody of National Gallery DC and therefore fiscal responsibility of said Items is carried by the same. As per agreement between both parties the following items are covered by AwesomeInsurance Inc. Policy x23654 for the following amounts under any circumstances leading to the degradation of said items excepting normal wear of display.

Lot # 1. Douglas MacArther	\$35,000.00
Lot # 2. Nederland	\$30,000.00
Lot# 3. Mongolia	\$24,000.00

Terms do not cover period of transport from or to the National Gallery.

D'Mann

President National Gallery DC

For The Internal use of National Gallery and MylStamp Collections Only.

- A rope and javelin (using alternative means to break in)
- tactical turtle necks (what i will be wearing)
- spray paint (for the cameras)
- vibram five finger shoes (in order to walk silently)
- pack of smokes (detecting lasers)
- smoke grenades (use as a means of escape if caught)

/img_tracy-phone-2012-07-15-final.E01/vol_vol5/mobile/Media/DCIM/100APPLE



IMG_0042.JPG



IMG_0043.JPG



IMG_0044.JPG



IMG_0045.JPG



IMG_0046.JPG



IMG_0047.JPG



IMG_0048.JPG



IMG_0049.JPG



IMG_0050.JPG



IMG_0051.JPG



IMG_0052.JPG



IMG_0053.JPG



IMG_0054.JPG



IMG_0055.JPG



IMG_0056.JPG



IMG_0057.JPG



IMG_0058.JPG



IMG_0059.JPG



IMG_0060.JPG



IMG_0061.JPG



IMG_0062.JPG



IMG_0063.JPG



IMG_0064.JPG



IMG_0065.JPG



IMG_0066.JPG



IMG_0067.JPG



IMG_0068.JPG



IMG_0069.JPG



IMG_0070.JPG



IMG_0071.JPG

Pictures of stamps referenced in the *Memorandum of Insurance Assurance* documents:







