



Cybersecurity

21.3 The Final Report

Case Report Pure Gold Credit Union

Table of Contents

[Case Report](#)

[Pure Gold CU](#)

[Peter's iPhone](#)

[Table of Contents](#)

[Executive Summary](#)

[Equipment and Tools](#)

[Details of Peter's iPhone](#)

[Evidence to Establish Personas](#)

[Plot Timeline](#)

[Conclusion](#)

[Appendix A: Correspondence Evidence](#)

[Appendix B: GPS Location Information](#)

Executive Summary

On January 21, 2016, Digitech Inc. was called in to assist Pure Gold Credit Union (PGCU)) case involving the conspiracy associated with the theft of funds.

- Peter is a suspect in the aforementioned conspiracy.
- As part of the investigation, Peter's iPhone was taken into custody.
- Digitech, Inc. was tasked with investigating evidence relevant to the aforementioned conspiracy.

As described fully in the report, Digitech, Inc. made the following findings.

Through our research we found evidence strongly suggesting a conspiracy between PGCU employees to fraudulently withdraw funds. Upon further investigation, we identify Peter Barnes, Rosie Lloyd and alias Hockeyfan474 as conspirators.

Equipment and Tools

Kali Linux Terminal

Sleuth Kit Autopsy Forensic Application

SQLite Browser

MD5 and SHA-256 hashes to ensure the integrity of the evidence

Evidence Tagging (+CAT-6 Items of Interest)

Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone12	activation_record.plist
Host Name	Peters iPhone	data_ark.plist
OS Version	V16.5.1	data_ark.plist
User Email	peterbarnes12792@icloud.com	accounts3.sqlite
Phone Number	615-571-9608	CellularUsage.db
Serial Number	FFNHHK2RPLJM	activation_record.plist
ICCID	89148000009489719791	activation_record.plist

IMEI	352853889946501	activation_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided by junior investigator
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6 577ccb534ca0d1e83ffd27683e621607	Provided by junior investigator

Details of Rosie's iPhone

Name	Findings	Location/File in iPhone image file
User Email	rosielloyd071292@icloud.com	Mail/Protected Index
Phone Number	615-427-8267	Mail/Protected Index

Evidence to Establish Personas

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

Peter Barnes, Bank Lead Teller at Pure Gold Credit Union, Dallas Branch

Phone Number: 615-571-9608
Email: peterbarnes12792@icloud.com
Relationship: primary accused

Rosie Lloyd, Bank Financial Advisor at Pure Gold Credit Union, Dallas Branch

Phone Number: 615-427-8267
Email: rosielloyd071292@icloud.com
Relationship: co-worker, co-conspirator

Mr. X; hockeyfan4747

Email: hockeyfan4747@proton.me
Relationship: co-conspirator, PGCU employee

List any other contacts here - derived from primary information stored in iPhone:

Douglas J. Weinstein

Phone Number: 234-987-6523

Email:

Relationship: Old high school friend

John Grant

Phone Number: 452-987-5625

Email: john.grant@gmail.com

John Keen

Phone Number: 615-555-6543

Mark Fletch

Phone Number: 529-555-4523

Email: mark.fletch@yahoo.com

Paul Thacker

Phone Number: 629-555-1298

Remington Stelle

Phone Number: 529-654-123

Tameka Brady

Phone Number: 324-555-2345

Email: tameka.brady@proton.mail

Evidence relating to theft of PGCU funds

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

The timeline of email exchanges and texts (appendix A) outline a conspiracy to fraudulently withdraw funds from PGCU. The conspirators consist of Peter Barnes, Rosie Lloyd and alias Hockeyfan474. Upon thorough inspection of Peter's phone, we also find search engine searches for fraud and video confirmation of the withdrawal of funds, again aligning with the timeline of events and communication exchanges.

Plot Timeline

Master Timeline of NGDC				
ID	Timestamp (UTC)	Header Information	Key Information	Evidence Location
10.elmx	Thu, 12 Oct 2023 00: 47: 25 +0000 (UTC)	Subject: Dinner Date Peter Barnes, peterbarnes12792@icloud.com Rosie Lloyd rosielloyd071292@icloud.com	Peter and Rosie confirmed a meet-up to talk about non-work and both feel like they are not being paid enough and that execs are overpaid. "Hey Rosie, great hanging out with you this weekend! Always good to hand out and talk about non work things"	Mail/Protected Index
12.elmx	Thu, 12 Oct 2023 22: 59: 41 +0000 (UTC)	Subject: Re: Dinner Date Peter Barnes, peterbarnes12792@icloud.com Rosie Lloyd rosielloyd071292@icloud.com	Peter shares Rosie's sentiment and says they should meet up again soon.	Mail/Protected Index
13.elmx	Fri, 20 Oct 2023 02: 43: 37 +0000 UTC	Subject: Question hockeyfan474@proton.me Peter Barnes, peterbarnes12792@icloud.com	"So, is Rosie in?" Hockeyfan emails Peter	Mail/Protected Index
14.elmx	Fri, 20 Oct 2023 02: 02: 43 +0000 (UTC)	Subject: Idea Peter Barnes, peterbarnes12792@icloud.com Rosie Lloyd rosielloyd071292@icloud.com	Peter confirms that he and Rosie met up. Peter proposed an idea. Rosie is intrigued, asks if X can be trusted to help.	Mail/Protected Index
16.elmx	Fri, 20 Oct 2023 02: 11: 14 +0000 (UTC)	Subject: Re: Idea Peter Barnes, peterbarnes12792@icloud.com Rosie Lloyd rosielloyd071292@icloud.com	Peter says X can be trusted and was the one who came up with the idea. Peter says he's ready to put plan into action but needs Rosie help. Peter asks Rosie if she's ready.	Mail/Protected Index

			Rosie confirms she's ready and just needs copies of forged withdrawal receipts so she can get the plan going.	
18.elmx	Fri, 20 Oct 2023 02: 22: 57 +0000 (UTC)	Subject: Re: Idea Peter Barnes, peterbarnes12792@icloud.com Rosie Lloyd rosielloyd071292@icloud.com	Peter confirms he'll get forged documents over to Rosie and asks Rosie to delete their email trail/ "evidence". Rosie confirms she'll delete the trail	Mail/Protected Index
20.elmx	Fri, 20 Oct 2023 02: 38: 10 +0000 (UTC)	Subject: Question Peter Barnes, peterbarnes12792@icloud.com hockeyfan474@proton.me	Peter emails hockeyfan and confirms that they're set to execute the plan and that Rosie is in. Hockeyfan responds "excellent!"	Mail/Protected Index
16.sms.db		iMessage Destination Caller ID: 615-571-9608	"Yup, see you then."	SMS/sms.db
17.smb.db		SMS Destination Caller ID: 615-571-9608	"Check your email"	SMS/sms.db
18.smb.db		SMS Destination Caller ID: 615-571-9608	"OK, will do"	SMS/sms.db
22.smb.db		iMessage Destination Caller ID: 615-571-9608	"I did it today, can't believe it. Going to the mall later, wanna join me me? Also, I sent you a picture."	SMS/sms.db
23.smb.db		iMessage Destination Caller ID: 615-571-9608	"Let's get off texts please, just email me to that email address."	SMS/sms.db
30.smb.db		SMS Destination Caller ID: 615-571-9608	"Just left you a VM, listen to it and get back to me!"	SMS/sms.db
31.smb.db		SMS Destination Caller ID: 615-571-9608	"Ok"	SMS/sms.db

Conclusion

Evidence found on Peter's iPhone indicated the following:

- Hockeyfan474 planned conspiracy to withdraw funds from PGCU
- Hockeyfan474 proposed plan to Peter and to involve Rosie
- Peter asked Rosie if she wanted to be included in plan and said that Hockeyfan474 was a trusted co-conspirator
- Rosie agreed to participate in plan
- Peter provided Rosie with falsified withdrawal receipts
- Someone (???) fraudulently withdraw funds
- +16158070242 left peter (+16155719608) voicemail

Bonus Conclusion

Did you determine who is Mr. X? If so, who is it, and how did you figure this out?

- Hockeyfan474 is Mr. X. Hockeyfan474 asked Peter, via email, if Rosie was involved and once confirmed said "excellent". The timeline of emailed strongly suggests that Peter reached out to Rosie to confirm her participation in response to X asking him to confirm their plans.

Appendix A: Correspondence Evidence

Email Sequence:

9 Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non work things. Peter
10 Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non work things. Peter Barnes
11 Hey Peter, Likewise, was so great to get a chance to hang out, outside of work. Sounds like we both feel that we aren't being paid enough, and on top of that all the Gold Credit Union executives are pulling up in sports cars. Its really frustrating :(. Rosie Llyod
12 I hear you, I'm really frustrated as well. Lets get together after work tonight, wanted to run something by you. Peter Barnes
13 So, is Rosie in? Sent with Proton Mail secure email.
14 Great getting together again last night, what did you think of the 'idea' I ran by you? Peter Barnes
15 Honestly, I am intrigued. Was up all night thinking about it, and how we can pull it off. Are you sure "X" can help us out? Do you trust X ? How about Michaela Rokas ? Rosie Llyod
16 I trust X, it was actually X that brought this idea to me a while back. I thought they were kidding, but X kept asking. Now after seeing the exec's getting rich while I have trouble paying my bills, I am ready to put this into action. But I need your help to make this work. You know what to do next? Peter Barnes
17 Yup, you explained it well last night. Just get me the copies of the forged withdrawal receipts so I can get this going. Also, what about Catarina Mona and Lanzo, I think her last name is Agneza ? Rosie Llyod
18 OK, but please try to keep details about this plan off our email, you may also want to delete these emails to remove any traces of evidence. You are being a little reckless and going to get us caught. They are ok, I get along with them for the most part. Peter Barnes
19 Ok, I'll do that, and don't worry so much. Rosie Llyod
20 Yes, we are good, should get this going this Friday Peter Barnes
21 Excellent! Sent with Proton Mail secure email. ----- Original Message -----
22 Can we schedule talk sometime. Under friends? Under this email? When is Peter's YOUR SERVICE END DATE TO A WEEK AWAY. NAME

Text Sequence I:

[illegible]

Test Sequence 2:

[illegible]

Search Engine Queries:

Data Content

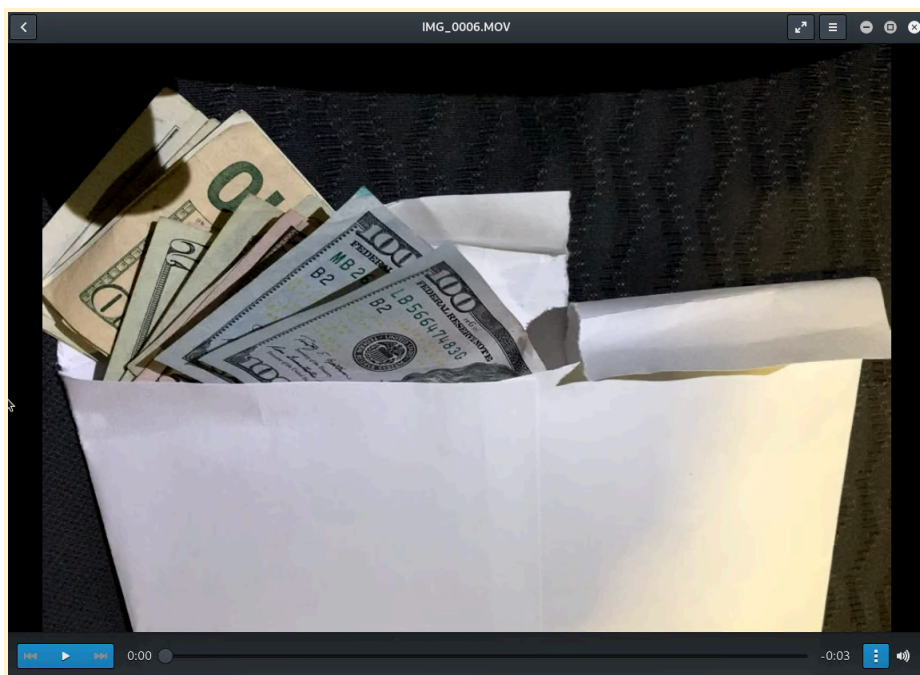
Hex Strings Indexed Text Message File Metadata Results Annotations Other Occurrences

Matches on page: - of - Match Page: 1 of 1 Page Text Source: File Text

```
14 8
15 8
16 9
17 9 7.1944294E8 cnn - Google Search 1 0 0 0 7 1 0
18 9 7.1944294E8 cnn - Google Search 1 0 0 0 7 2 0
19 10 7.1944294E8 Breaking News, Latest News and Videos | CNN 1 0 0 0 7 0 100
20 11 7.1944294E8 Google 1 0 0 0 7 0 100
21 11 7.1944294E8 Google 1 0 0 0 7 2 0
22 12 7.1944294E8 Google 1 0 0 0 7 1 0
23 11 7.1944294E8 Google 1 0 0 0 7 3 0
24 13 7.1944479E8 forensic accounting - Google Search 1 0 0 0 7 0 100
25 13 7.1944479E8 forensic accounting - Google Search 1 0 0 0 7 3 0
26 14 7.19445E8 Forensic accounting - Wikipedia 1 0 0 0 7 0 100
27 11 7.194451E8 Google 1 0 0 0 7 2 0
28 11 7.194451E8 Google 1 0 0 0 7 2 0
29 12 7.194451E8 Google 1 0 0 0 7 3 0
30 11 7.194451E8 Google 1 0 0 0 7 3 0
31 15 7.194452E8 forensic accounting how to not get detected - Google Search 1 0 0 0 7 0 100
32 15 7.1944493E8 forensic accounting how to not get detected - Google Search 1 0 0 0 7 3 0
33 16 7.194452E8 Forensic Accounting Advice - How to Minimize The Risk of Fraud in Your Business 1 0 0 0 7 0 100
34 11 7.194452E8 Google 1 0 0 0 7 2 0
35 11 7.194454E8 Google 1 0 0 0 7 2 0
36 12 7.194454E8 Google 1 0 0 0 7 3 0
37 11 7.194454E8 Google 1 0 0 0 7 3 0
38 17 7.194459E8 money laundering 101 - Google Search 1 0 0 0 7 0 100
39 17 7.194459E8 money laundering 101 - Google Search 1 0 0 0 7 3 0
40 18 7.194459E8 Money Laundering 101: Understanding The Basics | IPS 1 0 0 0 7 0 100
```

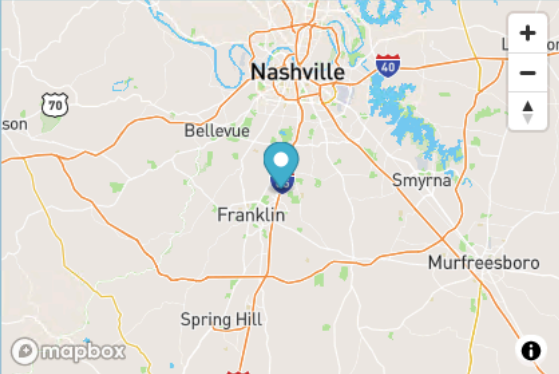
history tombstones

Video Evidence on withdrawal:



Appendix B: GPS Evidence

GPS location of Peter's phone, when Video Evidence captured:

Camera Make and Model	All Photo EXIF Data Save & Share EXIF
Apple - iPhone SE (2nd generation)	<input checked="" type="checkbox"/> Hide Serial Numbers
Camera Location Details	
Photo GPS Location: <u>35.97045,-86.80738888888888</u>	
	
Image Preview	
Preview not available	
	Make Apple
	Model iPhone SE (2nd generation)
	Orientation bottom-right
	XResolution 72
	YResolution 72
	ResolutionUnit inches
	Software 16.5
	DateTime 2023:10:20 19:53:39
	HostComputer iPhone SE (2nd generation)
	TileWidth 512
	TileLength 512
	Exif IFD Pointer 274
	GPS Info IFD Pointer 2148
	ExposureTime 1/46
	FNumber f/1.8
	ExposureProgram Normal program
	ISO Speed Ratings 320