



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.

Information was gathered from Peter Barnes' and Rosie Lloyd's confiscated mobile devices. Each device contained a list of emails, browser history, SMS and SMS attachments which ultimately proved their involvement and Oliver Bell's involvement in the theft of PGCU's funds.

From our findings Peter Barnes initiated the operations with Oliver and convinced Rosie via email and SMS communications to become involved too. The evidence provided shows that there was a collective motive surrounding the theft, that is that they were unhappy with their income in comparison to executives higher up. As a result of this they planned to steal money via money laundering and fraudulent means, with Oliver having the ability to remove any trace of the transactions via the deletion of audit records.

Throughout the course of the operation, Rosie was responsible for organizing the forged receipts which in turn would allow them to clear money from PGCU. This was seen through email communications.

The three individuals were able to steal 125 thousand dollars from PGCU before Digitech Inc was informed and operations ceased.

Equipment and Tools

We used a variety of tools to aid in our investigation which included:

- Kali Linux
- Autopsy
- SQLITE Browser
- Windows Media Player
- <https://onlineexifviewer.com/> was used to analyze .HEIC files

Details of Peter's iPhone

Model: iPhone 12,8

Host Name: Peters iPhone

OS Version: iPhone iOS 16.5.1

Phone Number: +16155719608

Serial Number: FFNHH2RPLJM

ICCID: 89148000009489719791

IMEI: 35285388994650

MD5 Hash: 34c4888f095dc3241330462923f6fea5

SHA256 Hash: 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607

Details of Rosie's iPhone

Model: iPhone 12,8

Host Name: Rosies iPhone

OS Version: iPhone iOS 16.5

Phone Number: +16154278267

Serial Number: FFPHGILYPLJM

ICCID: 89148000009489732844

IMEI: 359844405812767

Evidence to Establish Personas

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

Peter:

Phone Number: +16155719608

Email: peterbarnes12792@icloud.com

Relationship: Accused

Rosie:

Phone Number: +16154278267

Email: rosielloyd71292@icloud.com

Relationship: Accused (co-conspirator)

X (Oliver Bell):

Phone Number: +16158070242

Email: hockeyfan4747@proton.me

Relationship: Co-conspirator, (ring leader)

Email and mobile information was found on both Peter's and Rosie's devices, connecting them and Oliver Bell to the personal details listed above. These details specifically were found within the sms.db and mail directories on the mentioned devices.

Evidence relating to theft of PGCU funds

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

SMS evidence on Peter Barnes' phone proves that Rosie Lloyd successfully stole money from PGCU with the help of Peter Barnes. Rosie's SMS message states:

"I did it today, can't believe it. Going to the mall later, wanna join me ? Also, I sent you a picture".

The picture was located on Peter Barnes' phone as an attachment, as shown in Appendix A and its location correlates to Rosie's known location at the mall, as shown in Appendix B.

Oliver Bell's voicemail on Peter's phone also incriminates all three parties, as he states Rosie and Peter have cleared 125 thousand dollars worth of PGCU funds, and Oliver has successfully been deleting audit records in order to keep their operations hidden.

Plot Timeline

7-8 October 2023

Peter and Rosie catch up out of work hours

07:47 PM [11 October 2023]

Peter emailed Rosie, speaking about their recent catch-up together:

"Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non work things. Peter"

05:36 PM [12 October 2023]

Rosie responds to Peter's email, highlighting their frustration towards PGCU executives and income grievances:

"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 paid enough, and on top of that all the Gold Credit Union executives are pulling up in sports cars. It's really frustrating :(

Rosie Lloyd"

10:59 PM [12 October 2023]

Peter sends an email to Rosie, hinting at a potential proposal that both parties could get involved in:

"I hear you, Im really frustrated as well. Lets get together after work tonight, wanted to run something by you."

12 October 2023

Peter and Rosie met up after work

01:31 AM [19 October 2023]

Peter receives an email from hockeyfan4747@proton.me, who we believe is Mr. X:

"So, is Rosie in?"

09:02 PM [19 October 2023]

Peter sends an email to Rosie, asking what she thought of his plan:

"Great getting together again last night, what did you think of the 'idea' I ran by you? Peter Barnes"

09:07 PM [19 October 2023]

Rosie responds to Peter last email:

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 ?"

09:11 PM [19 October 2023]

Peter's email response to Rosie indicates his previous history with X and their malicious ideas:

"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?"

09:20 PM [19 October 2023]

Rosie replies to Peter, stating she is ready to aid in the involvement of the theft of funds:

"Yup, you explained it all 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 ?"

09:22 PM [19 October 2023]

Peter's responses to Rosie highlights his concerns regarding Rosie's recklessness when communicating over email. He also advises her to delete emails as they can be used as evidence in case they are caught:

"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"

09:33 PM [19 October 2023]

Rosie's email response to Peter:

"Ok, I'll do that, and don't worry so much."

09:38 PM [19 October 2023]

Peter emails Mr. X, stating that Rosie is in and they are ready to execute their plan to steal funds from PGCU:

"Yes, we are good, should get this going this Friday. Peter Barnes"

19 October 2023

Mr. X responds to Peter's previous email:

"Excellent!"

20 October 2023

Rosie successfully clears money from PGCU

07:53 PM [20 October 2023]

Rosie sends an SMS attachment to Peter, clearly showing a bundle of cash within an envelope.

06:36 PM [25 October 2023]

Peter receives voicemail message from Mr. X aka Oliver Bell

Conclusion

Evidence found on Peter's iPhone indicated the following:

We searched through Peter Barnes' browser history and found multiple sites which connect him to the operation. Some of these searches could potentially assist him with the theft of PGCU funds. These included:

- Guide on money laundering
- Information on forensic accounting and how to remain undetected

Emails and SMS messages between Peter and Rosie prove that both suspects were unhappy with their pay and did not appreciate PGCU executives earning more than themselves. Peter was able to encourage Rosie to become involved in the theft, as highlighted over email and ultimately aid in the operation.

Email and SMS messages from Rosie also incriminate her and prove that she was able to successfully acquire and use forged withdrawal receipts in order to steal money from PGCU.

A voicemail from “X”, now known as Oliver Bell, was found which incriminated Oliver Bell and proves that he is involved. Within the audio file, he states that he’s impressed that Peter and Rosie have collectively stolen 125 thousand dollars from PGCU and reminds Peter that he is still entitled to 20% of all the stolen funds. This is requested via an envelope of cash, delivered to Oliver’s and left at his back door. Oliver also stated that he has been to cover up their activities by deleting audit records so they aren’t caught.

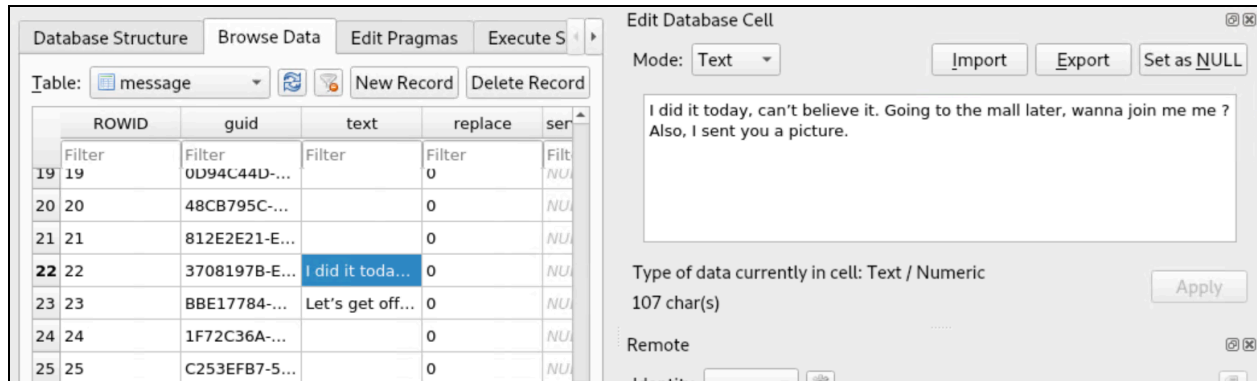
Bonus Conclusion

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

We have determined that Mr. X is Oliver Bell, the District Manager at Pure Gold Credit Union. This information was gathered through accessing a saved voicemail message on Peter’s phone. Oliver mentions that Peter and Rosie have collectively cleared 125 thousand dollars, and highlighted the importance that he still gets 20% of all stolen funds. Within the voicemail, Oliver mentions he will continue clearing the audit records in order to keep their malicious activities under the radar so Evelyn, the Branch Manager, doesn’t find out. Oliver’s final remarks request Peter to deliver his cut of the funds to his back door, in the form of cash within an envelope.

Appendix A: Correspondence Evidence

The screenshot below displays an SMS message from Rosiie to Peter, outlining that she has indeed successfully stolen from PGCU.



The following attachment was sent by Rosie to Peter via SMS communications. The data was analyzed, showing us a .MOV file showing a bundle of cash.



The following screenshot shows Oliver Bell's (X) SMS message to Peter Barnes, mentioning he has left a voice message for him to listen to.

ROWID	guid	text	replace	ser
19	0D94C44D-...		0	NU
20	48CB795C-...		0	NU
21	812E2E21-E...		0	NU
22	3708197B-E...	I did it toda...	0	NU
23	BBE17784-...	Let's get off...	0	NU
24	1F72C36A-...		0	NU
25	C253EFB7-5...		0	NU
26	4ACC8E64-...		0	NU
27	9A115BE9-...		0	NU
28	F7E8D719-...		0	NU
29	D1FCE1FD-...		0	NU
30	3E979855-C...	Just left you...	0	NU
31	0289E731-E...	Ok	0	NU

Just left you a VM, listen to it and get back to me!

Type of data currently in cell: Text / Numeric
52 char(s)

Remote

Identity

Name	Commit	Last modified	Size
------	--------	---------------	------

The following voice message left by Oliver Bell can be listened to [here](#).

The two following screenshots show two emails sent to Peter Barnes from Rosie Lloyd:

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 Lloyd

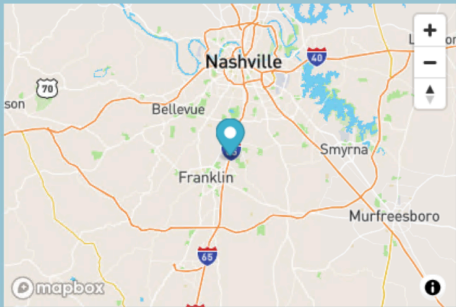
On Oct 19, 2023, at 9:07 PM, Rosie Lloyd <rosielloyd071292@icloud.com> wrote:

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 Lloyd

Appendix B: GPS Location Information

Upon reviewing the HEIC file available on Peter's phone, we concluded that the .MOV was captured in Brentwood, Tennessee.

Camera Make and Model
Apple - iPhone SE (2nd generation)
Camera Location Details
Photo GPS Location: 35.97045,-86.80738888888888

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
ISOSpeedRatings	320
ExifVersion	0232
DateTimeOriginal	2023:10:20 19:53:39
DateTimeDigitized	2023:10:20 19:53:39