



## 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.

Peter & Rosie are key culprits in money laundering from the Pure Gold Credit Union. They conspired together as disgruntled employees, jealous of executives, to create false documents in order to withdraw money from the Credit Union.

## Equipment and Tools

Within a Kali linux instance, we used the tools Autopsy to view and gather case data from the phone image files, stlitebrowser to open any database files, xdg-open (for the video files), <https://onlineexifviewer.com/> for viewing the native iPhone HEIC images and an audio player to listen to the audio files

## Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone SE (2nd Generation)	/LogicalFileSet1/PeteriPhoneImage/SMS/Attachments/33/03/00E33F22-7F93-41B1-80DB-D9CFAD02E410/00E33F22-7F93-41B1-80DB-D9CFAD02E410.pvt/IMG_0006.HEIC
Host Name	Peters iPhone	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/data_ark.plist

OS Version	16.5.1	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/data_ark.plist
User Email	<a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/Accounts3.sqlite
Phone #	1-615-571-9608	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/CellularUsage.db
Serial #	FFNHHK2RPLJM	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/activation_record.plist
ICCID	89148000009489719791	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/activation_record.plist
IMEI	352853889135063	/LocalFileSet1/PeteriPhoneImage/Files for identifiers/activation_record.plist
MD5 Hash	34c4888f095dc3241330462923f6fea5	Provided by the junior investigator.
SHA256 Hash	71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607	Provided by the junior investigator.

## Details of Rosie's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone SE (2nd Generation)	/LogicalFileSet3/RosieiPhoneImage/SMS/Attachments/a8/08/B35F722B-8B47-4AF6-BA7D-6A5DC5753F20/B35F722B-8B47-4AF6-BA7D-6A5DC5753F20.pvt/IMG_0006.HEIC
Host Name	Rosie's iPhone	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/data_ark.plist
OS Version	16.5	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/data_ark.plist
User Email	<a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a>	/LocalFileSet3/RosieiPhoneImage/Files for

		identifiers/Accounts3.sqlite
Phone Number	1-615-427-8267	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/CellularUsage.db
Serial Number	FFPHG1LYPLJM	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/activation_record.plist
ICCID	89148000009489732844	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/activation_record.plist
IMEI	35984440581276	/LocalFileSet3/RosieiPhoneImage/Files for identifiers/activation_record.plist

Video and photo evidence of money taken after the event of the laundering



## Evidence to Establish Personas

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

Peter:

Phone Number: 1-615-571-9608

Email: [peterbarnes12792@icloud.com](mailto:peterbarnes12792@icloud.com)

Relationship: Accused

Rosie:

Phone Number: 1-615-427-8267

Email: [rosielloyd071292@icloud.com](mailto:rosielloyd071292@icloud.com)

Relationship: Co-Conspirator

List any other contacts here

Oliver Bell (Mr.X):

Phone Number: 1-615-807-0242

Email: [hockeyfan4747@protonmail.com](mailto:hockeyfan4747@protonmail.com)

Relationship: Co-Conspirator

## Evidence relating to theft of PGCU funds

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

Peter and Rosie agree over email

1. Artifact ID- 9223372036854775542 a short video of an envelope of cash.
2. Artifact ID- 9223372036854775538 Peter and Rosie email chain. They discuss being unhappy with pay disparity between themselves and higher ups in the company. They make a plan to meet after work to discuss something
3. Artifact ID- 9223372036854775576 An email from [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me) (suspected to be Oliver) he asks if Rosie is in
4. Artifact ID- 9223372036854775480 Rosie asks if "X" (Oliver) and Michaela Rokas will assist in their plan.
5. Artifact ID- 9223372036854775553 Rosie and Peter email chain. Peter confirms X is an accomplice and came up with the plan. They confirm they are ready to go forward with their plan
6. Artifact ID- 9223372036854775498 peter/rosie email chain. Peter is concerned about communicating over email.
7. Artifact ID- 9223372036854775533 peter/hockeyfan email chain confirming friday as the day for executing the plan.

1	20 Oct 2023 2:33:47 GMT	From <a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a> TO: <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a> Received: mailgateway 24018B119	Rosie & Peter discussing to take the email chain offline to hide evidence	Email 19 <a href="mailto:partial.emixpeterbarnes12782@icloud.com">partial.emixpeterbarnes12782@icloud.com</a>
---	----------------------------------	---	---	--

2	12 OCT 2023 5:36 PM GMT	From <a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a> TO <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Rosie is upset about her pay and the executives having expensive cars	Email 12
3	Wed Oct 18 2023 8:31PM	To hockeyfan4747@proton.me From: <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Confirming their plan for Friday october 20th 2023 to do the money laundering	Email 20
4	Wed Oct 18 2023 8:31PM	To hockeyfan4747@proton.me From: <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Confirms rosie is in on it	Email 21
5	Thu Oct 19 2023 9:07PM	From: <a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a> To: <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Questions reliability of third suspect 'X', suggests participation of Michael Rokas	Email 17
6	Thu Oct 19 2023 9:11PM	From: <a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a> To: <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Mentions modus operandi, using forged receipts from Catarina Mona and Lanzo Agneza	Email 17
7	Fri 20 Oct 2023	To <a href="mailto:rosielloyd071292@icloud.com">rosielloyd071292@icloud.com</a> From <a href="mailto:peterbarnes12792@icloud.com">peterbarnes12792@icloud.com</a>	Mysteryman X, and Michaela Rokas are brought up and may be implicit  Peter and rosie talk about being ready to go through with the "plan"	Email 16
8		To: +16155719608 From: +16155719608	"Yup, see you then"	Text 16 - iMessage
9		To: 16155719608	"Check your email"	Text 17 - SMS
10		To 61555719608	"Let's get off texts please, just email me to that email address" -iMessage	Text 23
11		Google Search Forensic Accounting	Was searching methods of forensic accounting > website Fullerllp.com/blog/advice-from-a-to-ronto-forensic-accounting-firm-how-to-minimize-the-risk-of-fraud-in-yo	Safari History Item 12 -13

			u-business/	
12		Google Search Money "Launderong" (laundering)	Search result www.ipsservicesinc.com/money-laundering-101-understanding-the-basics	Safari History Item 14 -15
13		Voicemail From Oliver Bell 1-615-807-0242 To Peter Barnes 1-615-571-9608	Peter and Rosie clear of 125k with "Oliver" (Mr.X) receiving 20%. Oliver forging audit records to keep Evelyn off their backs - Oliver Bell - District Manager at pure gold Credit Union / Midwest Region	Voicemail 1

## Plot Timeline

Roughly 10-12-2023 approx 5:36PM - Rosie and Peter meet after work and had a conversation about laundering the money. (confirmed on Rosie and Peter's iMail data)

10-19-2023 approx 9:02PM - Peter confirms his "plan" with Rosie by asking what she thinks of it - Rosie responds that she is intrigued by it and they if they can trust Michaela Rokas and Mr. X

10-20-2023 (sometime during business hours) - Rosie, Peter and Oliver executed their plan to forge Audit records and other documents to withdraw 125K from Pure Gold Credit Union.

10-23-2023 - 7:53PM - Rosie and Peter shared an image of an envelope with cash with a geolocation of 35.97045,-85.80738888888888 (just south of Nashville, Tennessee). This aligns with the voicemail from Oliver Bell asking for cash for his 20% cut

## Conclusion

Evidence found on Peter's iPhone indicated the following:

- [Peter and Rosie successfully worked together to steal money from the credit Union. Oliver Bell assisted by deleting audit records for a percentage.]



## Bonus Conclusion

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

- According to several Emails/ SMS records - Mr.X is another disgruntled employee who has been plotting against PGCU for a long time. Upon listening to the Voicemail on Peter's iPhone, Oliver (Oliver Bell) is recovering 20% from their 125K fraud and will be fabricating audits to keep Evelyn of Rosie and Peter's back

## Appendix A: Correspondence Evidence

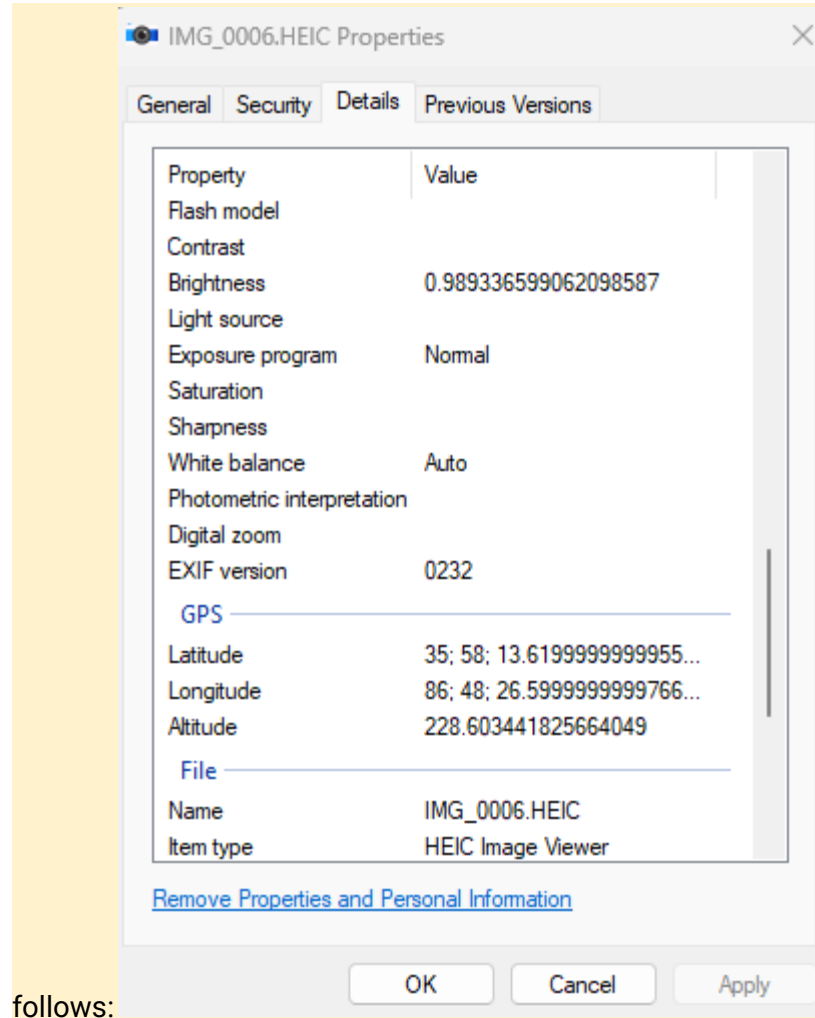
List any sms attachments and pictures found here



1. IMG\_0006.MOV found on Peter and Rosie's phone- a stack of cash meant for Oliver Bell (Mr.X)

## Appendix B: GPS Location Information

From the IMG\_0006.HEIC image shared on both Rosie and Peter's phones, the GPS data is as



follows:

We also visited an online EXIF viewer, [onlineexifviewer.com](https://onlineexifviewer.com), and uploaded the file to check for the GPS coordinates.

Camera Make and Model

Apple - iPhone SE (2nd generation)

Camera Location Details

Photo GPS Location: [35.97045,-86.80738888888888](#)

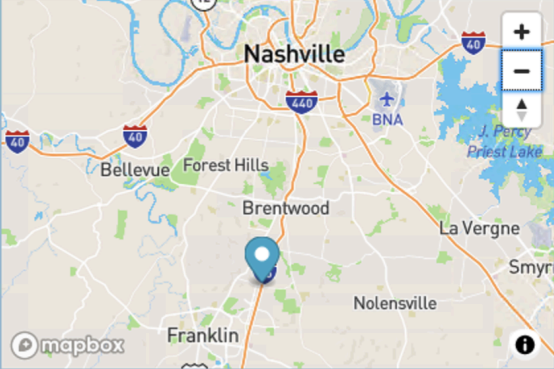


Image Preview

Preview not available

All Photo EXIF Data

[Save & Share EXIF](#)

☒ Hide Serial Numbers

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)
Exif IFD Pointer	250
GPS Info IFD Pointer	2124
ExposureTime	1/46
FNumber	f/1.8
ExposureProgram	Normal program
ISOSpeedRatings	320
ExifVersion	0232