



Cybersecurity

The Final Report

Case Report

Pure Gold Credit Union

Submitted by CK Security Solutions

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, CK Security Solutions 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 a thorough analysis of digital evidence, Digitech, Inc. identified Peter Barnes and Rosie Lloyd as co-conspirators in the theft. Key evidence included a series of suspicious emails and SMS/iPhone messages exchanged between Peter and Rosie, which detailed their plans to misappropriate funds from PGCU. These communications were instrumental in establishing the connection between the two individuals and their coordinated efforts.

Furthermore, the investigation uncovered evidence implicating Oliver Bell, the District Manager at PGCU, as the ringleader of the conspiracy (also referred to as Mr. X). A voicemail and a photo found on Peter's iPhone provided critical information that tied Mr. Bell to the scheme.

The findings detailed in this report highlight the effective use of digital forensic techniques in uncovering key evidence and identifying individuals involved in the conspiracy. Digitech, Inc. successfully provided PGCU with the necessary insights to address this breach of trust and security.

Equipment and Tools

- Kali Linux
- Autopsy 4.10.0
- SQLite browser
- Google maps

Details of Peter's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone 12.8	Activation Record
Host Name	Peter's Phone	Activation Record
OS Version	iOS 16.5	Activation Record
User Email	peterbarnes12792@icloud.com	Mail files
Phone Number	+16155719608	Cellular Usage
Serial Number	FFNHHK2RPLJM	Activation Record
ICCID	89148000009489719791	Activation Record
IMEI	311480010283519	Activation Record
MD5 Hash	cbcc58b538466287895220d1a763d5ed	n/a
SHA256 Hash	0c559080e112633baaf1b60a15b2873534f2822b54ac1ba707421688323a6b37	n/a

Details of Rosie's iPhone

Name	Findings	Location/File in iPhone image file
Model	iPhone 12.8	Activation Record
Host Name	Rosie's iPhone	Activation Record
OS Version	iOS 16.5	Activation Record
User Email	rosielloyd071292@icloud.com	Mail files
Phone Number	+16154278267	Cellular Usage
Serial Number	FFNHHK2RPLJM	Activation Record
ICCID	89148000009489732844	Activation Record
IMEI	359844405812767	Activation Record
MD5 Hash	e666cd1232ead8f76c0a42910f54b7d5	n/a
SHA256 Hash	0aa14fa06a416fd59c1e6586c888dd3511b1a98c7a01915233181866bedd7671	n/a

Evidence to Establish Personas

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

Peter Barnes:

Phone Number: +16155719608
Email: peterbarnes12792@icloud.com
Relationship: Accused, reports to Evelyn Lane

Rosie Lloyd:

Phone Number: +16154278267
Email: rosielloyd071292@icloud.com
Relationship: Accused, Co-conspirator with Peter, close friends with Peter, reports directly to Evelyn Lane

Oliver Bell:

Phone Number: +16158070242
Suspected Email: hockeyfan4747@proton.me
Alias: Mr. X
Relationship: Accused Ringleader and District Manager

Evelyn Lane:

Phone Number: n/a
Email: n/a
Relationship: Branch Manager, who found the missing funds and started the investigation into Peter. Reports directly to Oliver Bell

The data collected from Peter Barnes' phone shows multiple emails exchanged with Rosie Lloyd, confirming their close personal and professional relationship. Rosie and Peter are working together to embezzle funds from PGCU.

In one of the investigated SMS messages between Peter and an unknown number, there is reference to use the alias email given. This third email address, hockeyfan4747@proton.me, is suspected to be linked to Oliver Bell, alias Mr. X, who is leading the scheme. Peter and Rosie discuss their trust in Mr. X and confirm he is the mastermind behind the plan. Rosie and Peter

report directly to Evelyn Lane, the Branch Manager, who discovered the missing funds and initiated the investigation.

Evidence relating to theft of PGCU funds

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

Artifact #10

- **Timestamp:** 6 October
- **Header Information:** Peter's browser history.
- **Key Information:** Peter's search for "forensic accounting" and "how to not get detected" suggests an awareness of the risks involved in the theft and an attempt to avoid detection.

Artifact #1

- **Timestamp:** 12 October
- **Header Information:** Emails back and forth between Rosie and Peter. They are disgruntled due to the disparity in pay compared to executives.
- **Key Information:** Rose and Peter are increasingly upset over the differences in lifestyle between them and the executives, with executives driving sports cars while employees struggle financially.

Artifact #8

- **Timestamp:** 18 October
- **Header Information:** Email from "Hockeyfan4747" (possibly Oliver) to Peter Barnes.
- **Key Information:** The email discusses the plan and confirms that everything is set for Friday including confirming Rosie's involvement. This shows a degree of secrecy and intent to execute the heist.

Artifact #9

- **Timestamp:** 20 October
- **Header Information:** Email from Peter Barnes to Rosie Lloyd.
- **Key Information:** Peter warns Rosie to be careful about leaving evidence in emails and mentions their co-conspirators, including X. This email reveals further planning and intent for the heist.

Artifact #11

- **Timestamp:** 20 October
- **Header Information:** SMS message analysis.
- **Key Information:** Further analysis of SMS messages revealed more suspicious communications, including plans to move the operation onto emails and phone calls.

Artifact #5

- **Timestamp:** 20 October
- **Header Information:** Photo of cash taken near Nashville, Texas, delivered from Peter via SMS.
- **Key Information:** Oliver requested an envelope with cash to be delivered. This photo suggests that stolen funds were being moved.

Artifact #12

- **Timestamp:** 20 October
- **Header Information:** SMS message identifying Oliver.
- **Key Information:** Oliver's phone number is identified in the SMS database of Peter's iPhone, linking him to Peter and confirming his involvement.

Artifact #3

- **Timestamp:** 22 October
- **Header Information:** Rosie's browser history.
- **Key Information:** Searches about purchasing cars for cash, which may be related to laundering stolen funds.

Artifact #4

- **Timestamp:** 22 October
- **Header Information:** Rosie's browser history. "Best places to store cash"
- **Key Information:** Evidence of planning to conceal stolen funds, possibly to avoid detection.

Artifact #6

- **Timestamp:** 25 October
- **Header Information:** Voicemail confirming involvement.
- **Key Information:** Voicemail from Oliver to Peter confirms the heist has been successful and that Oliver is involved in the theft, taking 20% of the stolen funds. Oliver is identified as "Mr. X."

Artifact #7

- **Timestamp:** 25 October
- **Header Information:** Voicemail sender and receiver phone numbers.
- **Key Information:** The voicemail sender's phone number (+16158070242) and receiver's phone number (+16155719608) were recorded in the voicemail database, confirming the identities of the individuals involved.

Plot Timeline

Date	Information
6 October	Browser Search History: Peter's search for "forensic accounting" and "how to not get detected" suggests an awareness of the risks involved in the theft and an attempt to avoid detection
12 October	Emails: Peter and Rosie are increasingly upset over the differences in lifestyle between them and the executives, with executives driving sports cars while employees struggle financially.
18 October	Emails: Email between Peter and "Hockeyfan4747" (possibly Oliver) discusses the plan and confirms that everything is set for Friday. This shows a degree of secrecy and intent to execute the heist.
20 October	Emails: Peter warns Rosie to be careful about leaving evidence in emails and mentions their co-conspirators, including X. This email reveals further planning and intent for the heist.

20 October	SMS: Analysis of SMS messages revealed more suspicious communications, including plans to move the operation onto emails and phone calls.
20 October	SMS: Oliver requested an envelope with cash to be delivered. This photo attachment suggests that stolen funds were being moved.
20 October	SMS: Oliver's phone number is identified in the SMS database of Peter's iPhone, linking him to Peter and confirming his involvement.
22 October	Browser Search History: Searches about purchasing cars for cash, which may be related to laundering stolen funds.
22 October	Browser Search History: Evidence of planning to conceal stolen funds, possibly to avoid detection.
25 October	Phone records: Voicemail from Oliver to Peter confirms the heist has been successful and that Oliver is involved in the theft, taking 20% of the stolen funds. Oliver is identified as "Mr. X."
25 October	Phone records: The voicemail sender's phone number (+16158070242) and receiver's phone number (+16155719608) were recorded in the voicemail database, confirming the identities of the individuals involved.

Conclusion

Evidence found on Peter's iPhone indicated the following:

The analysis of Peter Barnes's iPhone has revealed compelling evidence of his central role in the theft of PGCU funds, alongside co-conspirators Rosie Lloyd and Oliver ("Mr. X"). The digital artifacts extracted from his device—spanning SMS messages, emails, browser history, and voicemails—paint a clear picture of premeditated fraud, with a focus on financial gain and evasion of detection.

Key Findings:

1. **Motivation and Planning:** Peter's emails and browser history indicate his discontent with the financial disparity between employees and executives, fueling his willingness to commit theft. His search for "forensic accounting" and methods to avoid detection demonstrate an awareness of the risks and a calculated approach to the crime.
2. **Communication and Coordination:**
 - SMS and email communications between Peter, Rosie, and Oliver outline the development and execution of the plan. These messages confirm the involvement of all parties, including Oliver's role as a key conspirator (identified as "Mr. X").
 - The voicemail from Oliver to Peter further solidifies Oliver's direct participation, with explicit acknowledgment of his share in the stolen funds.
3. **Evidence of Execution:** The photo of cash taken near the Nashville, Texas branch corroborates the transfer of stolen funds. Additionally, Rosie's browser history searches for purchasing cars for cash and storing money reflect steps to conceal and utilize the illicit gains.
4. **Conspirator Network:** Emails confirm Peter's efforts to include and manage co-conspirators, such as Rosie and Oliver, while also expressing concerns about minimizing evidence and maintaining secrecy.

Conclusion: The evidence extracted from Peter Barnes's iPhone leaves no doubt about his involvement in the theft of PGCU funds. His digital communications establish him as the orchestrator of the scheme, with Rosie Lloyd and Oliver playing critical supporting roles. The combination of financial motives, detailed planning, and efforts to obscure evidence highlights a deliberate and coordinated criminal act. This evidence not only implicates Peter but also provides critical links to his co-conspirators, offering a comprehensive narrative of the case.

Bonus Conclusion





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

The conclusion that Oliver is "Mr. X" stems from multiple pieces of evidence found on Peter Barnes's iPhone. A voicemail from Oliver to Peter explicitly confirms his involvement in the theft, stating that he would take "20% off the top" of the stolen funds, further aligning with the role of "Mr. X" as referenced in Peter's emails. Additionally, Oliver's phone number (+16158070242) appears in both the voicemail metadata and the SMS database, directly linking him to Peter. This connection, coupled with Peter's trust in "X" as the initiator of the scheme, confirms that Oliver and "Mr. X" are the same person.

Appendix A: Correspondence Evidence

Timestamp	Header	Key Information			Evidence Location
		Description	Source	Destination	
2023-10-12 00:39:24 AEDT	Email	Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non work things.	peterbarnes12792@icloud.com	rosielloyd071292@icloud.com	PeteriPhoneImage/Mail/MessageData/9/full.emlx
2023-10-12 22:36:08 AEDT	Email	hey peter, likewise was so great to get a chance to hangout, 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, really frustrating :(rosielloyd071292@icloud.com	peterbarnes12792@icloud.com	PeteriPhoneImage/Mail/MessageData/11/full.emlx
2023-10-12 22:59:41 AEDT	Email	I hear you, I'm really frustrated as well. Lets get together after work tonight, wanted to run something by you.	peterbarnes12792@icloud.com	rosielloyd071292@icloud.com	PeteriPhoneImage/Mail/MessageData/12/full.emlx
2023-10-18 15:39:05 AEDT	iMessage	Dinner tonight?	P:+16154278267	P:+16154278267	RosieiPoneImage/SMS/sms.db
2023-10-18 15:40:48 AEDT	iMessage	Yup, see you then	P:+16154278267	P:+16154278267	RosieiPoneImage/SMS/sms.db
2023-10-18 15:40:48 AEDT	iMessage	Yup, see you then	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-18 15:59:47 AEDT	SMS	Check your email	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-18 16:00:36 AEDT	SMS	Ok, will do	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-19 01:31:07 AEDT	Email	so, is Rosie in?	hockeyfan4747@proton.me	peterbarnes12792@icloud.com	PeteriPhoneImage/Mail/MessageData/13/full.emlx



2023-10-20 02:02:43 AEDT	Email	Great getting together again, what did you think of the 'idea' I ran by you?	peterbarne s12792@icloud.com	rosielloyd071292@icloud.com	PeteriPhonelImage/Mail/MessageData/14/full.emlx
2023-10-20 02:07:55 AEDT	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?	rosielloyd 071292@icloud.com	peterbarnes12792@icloud.com	PeteriPhonelImage/Mail/MessageData/15/full.emlx
2023-10-20 02:11:14 AEDT	Email	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?	peterbarne s12792@icloud.com	rosielloyd071292@icloud.com	PeteriPhonelImage/Mail/MessageData/16/full.emlx
2023-10-20 02:19:59 AEDT	Email	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 Laanzo, I think her last name is Agneza?	rosielloyd 071292@icloud.com	peterbarnes12792@icloud.com	PeteriPhonelImage/Mail/MessageData/17/full.emlx
2023-10-20 02:22:57 AEDT	Email	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	peterbarne s12792@icloud.com	rosielloyd071292@icloud.com	PeteriPhonelImage/Mail/MessageData/18/full.emlx

		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.			
2023-10-20 02:38:10 AEDT	Email	Yes, we are good, should get this going this Friday.	peterbarnes12792@icloud.com	hockey747@proton.me	PeteriPhoneImage/Mail/MessageData/20/full.emlx
2023-10-20 02:43:23 AEDT	Email	excellent	hockey747@proton.me	peterbarnes12792@icloud.com	PeteriPhoneImage/Mail/MessageData/21/full.emlx
2023-10-20 06:53:39 AEDT	SMS	 IMG_0006.jpg picture of envelope with money	P:+16154278267	P:+16155719608	RosieiPhoneImage/SMS/Attachments/a8/08/B35F722B-8B47-4AF6-BA7D-6A5DC5753F20/IMG_0006.HEIC/IMG_0006.jpg
2023-10-20 06:53:39 AEDT	SMS	 IMG_0006.jpg picture of envelope with money	P:+16154278267	P:+16155719608	RosieiPhoneImage/SMS/Attachments/a8/08/B35F722B-8B47-4AF6-BA7D-6A5DC5753F20/B35F722B-8B47-4AF6-BA7D-6A5DC5753F20.pvt/IMG_0006.HEIC/IMG_0006.jpg
2023-10-20 06:53:39 AEDT	SMS	 IMG_0006.jpg picture of envelope with money	P:+16155719608	P:+16154278267	PeteriPhoneImage/SMS/Attachments/33/03/00E33F22-7F93-41B1-80DB-D9CFAD02E410/IMG_0006.HEIC/IMG_0006.jpg
2023-10-20 06:53:39 AEDT	SMS	 IMG_0006.jpg	P:+16155719608	P:+16154278267	PeteriPhoneImage/SMS/Attachments/33/03/00E33F22-7F93-41B1-80DB-D9CFAD02E410/00E33F22-7F93-41B1-80DB-D9CFAD02E

		picture of envelope with money			410.pvt/IMG_0006.HEIC/IMG_0006.jpg
2023-10-20 08:53:20 AEDT	webhistory	Forensic Accounting Advice - How to Minimize the Risk of Fraud in Your Business			PeteriPhoneImage/Safari History/History.db
2023-10-20 08:53:20 AEDT	webhistory	forensic account how to not get detected			PeteriPhoneImage/Safari History/History.db
2023-10-20 09:05:00 AEDT	webhistory	money laundering 101 - Google Search			PeteriPhoneImage/Safari History/History.db
2023-10-20 09:05:00 AEDT	webhistory	Money Laundering 101: Understanding The Basics IPS			PeteriPhoneImage/Safari History/History.db
2023-10-21 00:56:57 AEDT	iMessage	I did it today, can't beleive it. Going to the mall later, wanna join me ? Also, I sent you a picture.	P:+16154278267	P:+16154278267	RosieiPoneImage/SMS/sms.db
2023-10-21 00:57:23 AEDT	iMessage	I did it today, can't believe it. Going to the mall later, wanna join me me ? Also, I sent you a picture.	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-21 00:58:50 AEDT	iMessage	Let's get off texts please, just email me to that email address.	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-21 00:58:50 AEDT	iMessage	Let's get off texts please, just email me to that email address.	P:+16154278267	P:+16154278267	RosieiPoneImage/SMS/sms.db
2023-10-24 03:33:49 AEDT	webhistory	paying cash for a car: consider the pros and cons - kelly blue book			RosieiPhoneImage/Safari History.db
2023-10-24 03:33:49 AEDT	webhistory	purchasing luxury cars with cash is that sage - Google Search			RosieiPhoneImage/Safari History.db

2023-10-24 03:35:29 AEDT	webhistory	best places to store large amounts of cash			RosieiPhoneImage/Safary History.db
2023-10-24 03:35:29 AEDT	webhistory	The 5 Best Places to Hide Emergency Cash at Home			RosieiPhoneImage/Safary History.db
2023-10-24 03:39:59 AEDT	webhistory	how to hide case in your home - Google Search			RosieiPhoneImage/Safary History.db
2023-10-24 03:39:59 AEDT	webhistory	50 Secret Hiding Places for Valuables in Your Home Family Handyman			RosieiPhoneImage/Safary History.db
2023-10-25 18:37:50 AEDT	SMS	Just left you a VM, listen to it and get back to me!	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db
2023-10-25 18:38:04 AEDT	SMS	Ok	P:+16155719608	P:+16155719608	PeteriPhoneImage/SMS/sms.db > table messages > rowid 31
2023-10-25 18:37:50 AEDT	Voicemail	1.amr file from Oliver to Peter detailing that Oliver gets a 20% cut of the 125k withdrawal, oliver will clear the audit records to protect peter. Instructing peter to put the money in an envelope and leave it at Olivers back door.	P:+16155719608		PeteriPhoneImage\Voicemail\A-D3E419E4-6BF5-5B09-AC57-67804CB8C6B4\1.amr

Appendix B: GPS Location Information

Timestamp	Header Information	Key Information	Evidence Location
October 20	<div><div><div>Camera Make and Model</div><div>Apple - iPhone SE (2nd generation)</div></div><div><div>Camera Location Details</div><div>Photo GPS Location: 32.21745, -86.077338810003</div><div></div><div><div>Image Preview</div><div></div><div>IMG_0006.jpg</div></div></div></div> <div><div>All Photo EXIF Data</div><div><div>Save & Share</div><div>Make</div><div>Apple</div><div>Model</div><div>iPhone15,2 (2nd generation)</div><div>Orientation</div><div>bottom-right</div><div>Width</div><div>72</div><div>Height</div><div>72</div><div>Resolution</div><div>1080</div><div>Software</div><div>16.5</div><div>Date/Time</div><div>2023:10:20 18:53:39</div><div>Host Computer</div><div>iPhone SE (2nd generation)</div><div>Lat</div><div>32.21745</div><div>GPS Info</div><div>GPS Info</div><div>ExposureTime</div><div>1/18</div><div>ExposureProgram</div><div>Normal program</div></div></div> <div><div>Photo of the cash was taken near Nashville, in Texas which is the location of the branch. Oliver asked for an envelope with cash to be delivered.</div></div> <div><div>PeteriPhone1 mage/SMS/A ttachments/3 3/03/ 00E33F22-7F 93-41B1-80D B-D9CFAD02 E410/IMG_0 006.HEIC/IM G_0006.jpg</div></div>		