| Cybersecurity |
| --- |
| 21.3 The Final Report |

Case Report

Pure Gold Credit Union

### 

# Table of Contents

[Case Report](#_8mjg1w2w81ai)

[Pure Gold CU](#_lrib8gqk2z7b)

[Peter's iPhone](#_219o4hryceis)

[Table of Contents](#_786gzvga2e8h)

[Executive Summary](#_ccs3x82xm1tu)

[Equipment and Tools](#_hw4rzs3hh4tn)

[Details of Peter’s iPhone](#_ebsdggfieq5h)

[Evidence to Establish Personas](#_qixiazcd0tiw)

[Plot Timeline](#_nz1crxu2ypd4)

[Conclusion](#_m5r3zcqmj9ou)

Appendix A: [Correspondence Evidence](#_w4pkinqwxqi8)

Appendix B: [GPS Location Information](#_f8fx30pgaw29)

# 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.

The forensic investigation revealed that Peter Barnes and Rosie Lloyd conspired to steal funds from PGCU. Their email correspondence highlights their dissatisfaction with their pay and discussions about a fraudulent scheme. Peter mentioned that the idea was initially brought to him by someone referred to as "X," who was later identified as Oliver after leaving a voicemail on Peter’s phone, demanding his share of the stolen funds. Rosie expressed interest in the plan, and they discussed potential collaborators. Peter advised against sharing too many details over email to avoid leaving evidence.

### Equipment and Tools

Autopsy

Sqlitebrowser

Kali Linux

onlineexifviewer.com

# 

# 

# Details of Peter’s iPhone

### **Details of Peter’s iPhone**

| **Name** | **Findings** | **Location/File in iPhone image file** |
| --- | --- | --- |
| Model | iPhone 12.8 | 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 | 1-615-571-9608 | com/apple.commcenter.plist |
| Serial Number | FFNHHK2RPLJM | activation\_record.plist |
| ICCID | 89148000009489719791 | activation \_record.plist |
| IMEI | 352853889135063 | activation \_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 |  |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 |  |

# Details of Rosie’s iPhone

| **Name** | **Findings** | **Location/File in iPhone image file** |
| --- | --- | --- |
| Model | iPhone 12.8 | activation\_record.plist |
| Host Name | Rosie’s iPhone | data\_ark.plist |
| OS Version | V16.5 | data\_ark.plist |
| User Email | rosielloyd071292@icloud.com | Accounts3.sqlite |
| Phone Number | 1-615-427-8267 | com/apple.commcenter.plist |
| Serial Number | FFPHG1LYPLJM | activation\_record.plist |
| ICCID | 89148000009489732844 | activation \_record.plist |
| IMEI | 359844406101632 | activation \_record.plist |
| MD5 Hash |  |  |
| SHA256 Hash |  |  |

# 

# 

# Evidence to Establish Personas

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

Peter Barnes:

Phone Number: 1 (615) 571-9608

Email: peterbarnes12792@icloud.com

Relationship: Lead Teller (Accused)

Rosie Lloyd:

Phone Number: 1 (615) 427–8267

Email: rosielloyd071292@icloud.com

Relationship: Financial Advisor (Accused)

Oliver Bell(“MR. X”):

Phone Number 1 (615) 807-0242

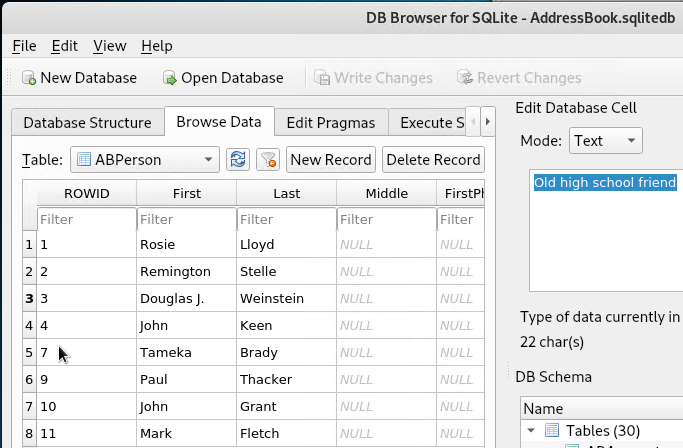
Email: hockeyfan4747@proton.met

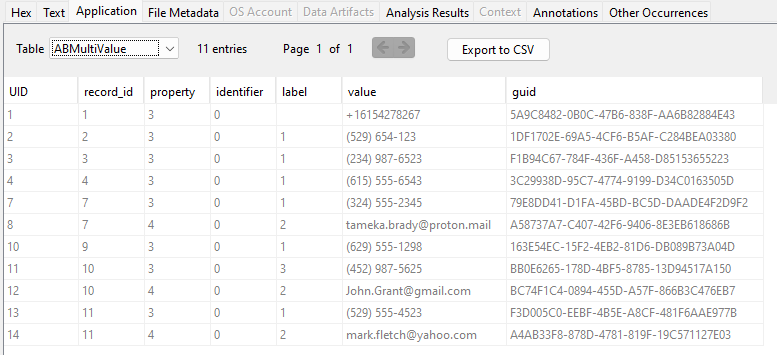
Relationship: District Manager (ring leader)

**List any other contacts here**

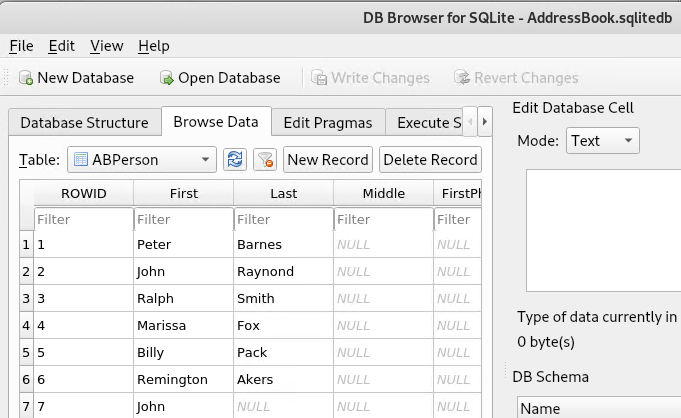
The name of **Michaela Rokas**(Bank teller) was also mentioned in **email #15**, but I was not able to find evidence that directly linked her to the case as an accomplice.

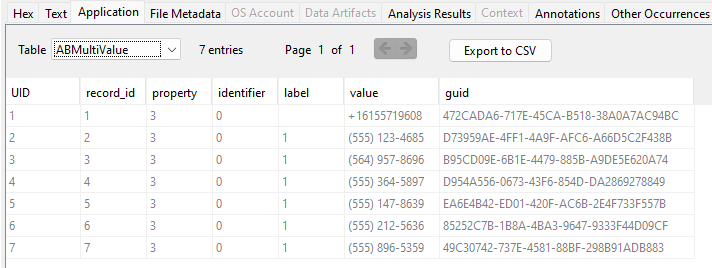
Peter’s Address Book and Contacts





Rosie’s Address Book





After reviewing the emails, text messages, and voicemails, it is evident that Rosie and Peter share no common contacts in their address books, aside from each other. Although Oliver does not appear in either Rosie's or Peter's address book, there is a direct correspondence between Peter and Oliver, suggesting a personal connection. Rosie, however, seems unaware of Oliver’s identity, as no evidence links her to him directly, further indicating that Oliver’s involvement in the scheme was primarily through Peter.

# Evidence relating to the theft of PGCU funds

In the investigation of the theft of funds, I analyzed various artifacts retrieved from the two iPhone bit-by-bit images from Peter Barnes and Rosie Lloyd. Our findings indicate several significant elements that support the conclusion of illicit activity.

* SMS Records: The examination of SMS records uncovered messages between Peter and Rosie that showcased a picture and video of an envelope with a large sum of money.
* Browser history: In the browser history of Peter’s iPhone showcasing that he looked at how to do money laundering, and how to avoid forensics detection.
* Voice Mail: This voicemail appears to be from the same unidentified individual referenced in the email records as “Mr. X”, later known as Oliver Bell further implying a connection to the theft and how he used his leverage to keep the information from Evelyn.
* Email Correspondence: A review of emails associated with the iPhones indicated conversations between Peter and a mysterious email in which they talked about recruiting Rosie into their scheme. As well as emails between Peter and Rosie in which she accepts joining them.

The evidence collected from the iPhone images collectively supports the conclusion that these 3 individuals did plot and worked together to steal over 125K from PGCU.

# Plot Timeline

| **Master Timeline of NGDC** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Key Information** | **Evidence Location** |
| R10\_SMS | October 11, 2023, 20:46:38 UTC | **To:** Rosie  **From:** Peter | Dinner tonight? | sms.db |
| R11\_SMS | October 11, 2023, 20:47:30 UTC | **To:** Peter  **From:** Rosie | Yup, see you then | sms.db |
| P10\_EMAIL | Thu,  12 Oct 2023 00:47:25 GMT | **To:** rosielloyd071292@icloud.com  **From:** Peter Barnes peterbarnes12792@icloud.com  **Subject:** Dinner | Hey Rosie, great hanging out with you this weekend! Always good to hang out and talk about non-work things. Peter Barnes | Email |
| P16\_SMS | Thu,  October 12, 2023, 02:48:40 GMT | **To:** Peter  **From:** Rosie | Yup, see you then | sms.db |
| P17\_SMS | October 12, 2023, 02:56:25 UTC | **To:** Peter  **From:** Oliver | Check your email | sms.db |
| P18\_SMS | October 12, 2023, 02:56:36 UTC | **To:** Oliver  **From:** Rosie | Ok, will do  <not delivered> | sms.db |
| P21\_SMS | October 12, 2023, 06:32:30 UTC | **To:** Peter  **From:** Rosie |  | sms.db |
| P22\_SMS | October 12, 2023, 06:32:48 UTC | **To:** Peter  **From:** Rosie | I did it today, can’t believe it. Going to the mall later, wanna join me me ? Also, I sent you a picture. | sms.db |
| P23\_SMS | October 12, 2023, 06:34:20 UTC | **To:** Rosie  **From:** Peter | Let’s get off texts please, just email me to that email address. | sms.db |
| P30\_SMS | October 12, 2023, 07:36:10 UTC | **To:** Peter  **From:** Oliver | Just left you a VM, listen to it and get back to me! | sms.db |
| P31\_SMS | October 12, 2023, 07:36:50 UTC | **To:** Oliver  **From:** Peter | Ok  <not delivered> | sms.db |
| P11Email | Thu  12 Oct 2023 22:36:08 GMT | **To**: Peter Barnes peterbarnes12792@icloud.com  **From:** Rosie Lloyd rosielloyd071292@icloud.com  **Subject line**: Re: Dinner | 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 Lloyd | Email |
| P12\_EMAIL | Thu,  12 Oct 2023 22:59:41 GMT | To: Rosie Lloyd rosielloyd071292@icloud.com  From: Peter Barnes peterbarnes12792@icloud.com  Subject: Re: Dinner | I hear you, I’m really frustrated as well. Let's get together after work tonight; I wanted to run something by you.  Peter Barnes | Email |
| P13\_EMAIL | Thu,  19 Oct 2023 01:31:07 GMT | To: "peterbarnes12792@icloud.com" peterbarnes12792@icloud.com  From: hockeyfan4747 hockeyfan4747@proton.me  Subject: Question | So, is Rosie in? | Email |
| P14\_EMAIL | Fri,  20 Oct 2023 02:02:43 GMT | To: Rosie Lloyd rosielloyd071292@icloud.com  From: Peter Barnes peterbarnes12792@icloud.com  Subject: Idea | Great getting together again last night, what did you think of the ‘idea’ I ran by you?  Peter Barnes | Email |
| P15\_EMAIL | Fri,  20 Oct 2023 02:07:55 GMT | To: Peter Barnes peterbarnes12792@icloud.com  From: Rosie Lloyd rosielloyd071292@icloud.com  Subject: Re: Idea | 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? | Email |
| P16\_EMAIL | Fri,  20 Oct 2023 02:11:14 GMT | To: Rosie Lloyd rosielloyd071292@icloud.com  From: Peter Barnes peterbarnes12792@icloud.com  Subject: Re: Idea | 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 execs 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? | Email |
| P17\_EMAIL | Fri,  20 Oct 2023 02:19:59 GMT | To: Peter Barnes peterbarnes12792@icloud.com  From: Rosie Lloyd rosielloyd071292@icloud.com  Subject: Re: Idea | 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? | Email |
| P18\_EMAIL | Fri,  20 Oct 2023 02:22:57 GMT | **To:** Rosie Lloyd (rosielloyd071292@icloud.com)  **From:** Peter Barnes (peterbarnes12792@icloud.com)  **Subject:** Re: Idea | 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 | Email |
| P19\_EMAIL | Fri,  20 Oct 2023 02:33:47 GMT | **To:** Peter Barnes (peterbarnes12792@icloud.com)  **From:** Rosie Lloyd (rosielloyd071292@icloud.com)  **Subject:** Re: Idea | No message content provided. | Email |
| P20\_EMAIL | Fri,  20 Oct 2023 02:38:10 GMT | **To:** hockeyfan4747 (hockeyfan4747@proton.me)  **From:** Peter Barnes (peterbarnes12792@icloud.com)  **Subject:** Re: Question | Yes, we are good, should get this going this Friday. | Email |
| P21\_EMAIL | Fri,  20 Oct 2023 02:43:23 GMT | **To:** Peter Barnes peterbarnes12792@icloud.com  **From**: hockeyfan4747 hockeyfan4747@proton.me  **Subject**: Re: Question | Excellent! | Email |
| P22\_EMAIL | Fri,  20 Oct 2023 19:06:38 GMT | **To**: Peter Barnes  peterbarnes12792@icloud.com  **From**: "Straight Talk Special" straighttalk@email2.straighttalk.com  **Subject**: It's time! Pay less for your service | It’s time! Pay less for your service.  Sent with [Proton Mail](https://proton.me/) secure email. | Email |

# Conclusion

Evidence found on Peter’s iPhone indicated the following:

* The evidence gathered from Peter's iPhone reveals a concerning pattern of behavior that strongly implicates him in the theft of funds from Digitech Inc. The text messages exchanged between Peter and Rosie indicate a secretive communication style, particularly when Peter requests to switch from texting to email, hinting at a desire for discretion. Additionally, Peter’s enthusiasm about an unspecified action he took that day, along with his invitation to Rosie to view a photo of a large sum of cash in an envelope, raises significant alarms. This image, combined with his preference for discussing financial matters through private channels, strongly suggests Peter’s involvement in illicit activities. Collectively, these elements build a compelling case that Peter not only had a motive but also actively participated in the theft from PGCU.

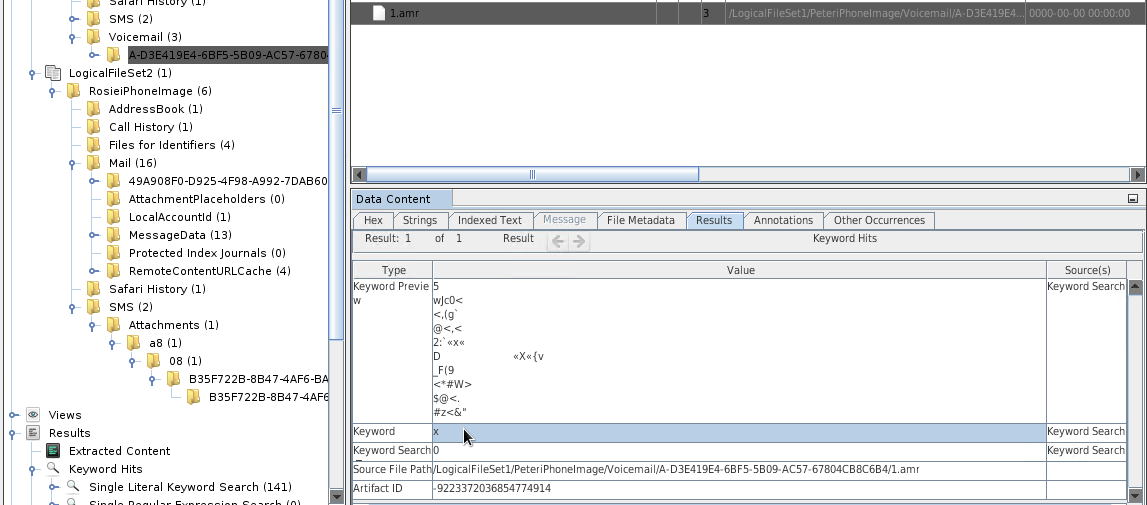
# 

# **Bonus Conclusion**

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

* Yes, Mr. X was identified as Oliver Bel PGCU District Manager. This conclusion was reached through the analysis of voicemail left on Peter's phone, in which Oliver referenced getting his share of the deal and cleaning the audit records, so Evelyn would not find anything, showcasing how he was using his position so he could tamper this kind of evidence. Peter's email indicated that he trusted X and was discussing a fraudulent scheme, linking Oliver directly to the plot.

The voicemail [left by Oliver](https://drive.google.com/file/d/1cpWEsm-PzAX910XK43em-JuqCIsVX9XJ/view?usp=drive_link)

**** If you further analyze this Image of the autopsy in which the number who left the compromising voicemail had the keyword value of **“X”.**

# Appendix A: Correspondence Evidence

I located 2 attachments which include a .MOV file which you can access below

[SMS Attachment Video file](https://drive.google.com/file/d/1IimEPwNRvcCSjxVl3j69NUxpjDKCr1Co/view?usp=drive_link)   
  
And this image showcases an envelope with money



# Appendix B: GPS Location Information

The location where the picture was taken is **Brentwood, Tennessee**, it happened at 19:53 on the date of 10/20/2023.

# 

