| 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.

Using the iphone images from Peter Barnes’ and Rosie Lloyd’s phones, it was discovered that there was correspondence between Peter Barnes, Rosie Lloyd, and Oliver Bell regarding a conspiracy to steal $125,000 from their employer Pure Gold Credit Union. The investigation revealed that Peter Barnes, Rosie Lloyd, and Oliver Bell conversed through text messaging, emails, and voicemail in regards to the theft.

### Equipment and Tools

Autopsy: Digital Forensic Tool used to analyze the contents of Peter Barnes’ and Rosie Lloyd’s phones. This included call history, emails, address book, SMS, and internet history

SQLite Browser: Digital Forensic Tool used to further analyze SMS and emails

Website <https://onlineexifviewer.com/> : used to acquire GPS location information of a photo attachment.

Website <https://heic2jpg.com/> : used to convert file IMG\_0006.HEIC to a viewable JPG format.

An AMR player downloaded from <https://www.amrplayer.com/> : used to listen to voicemail file 1.amr.

# Details of Peter’s iPhone

| **Name** | **Findings** | **Location/File in iPhone image file** |
| --- | --- | --- |
| Model | iPhone12 | activation\_record.plist |
| Host Name | nPeter | data\_ark.plist |
| OS Version | V16.5.1 | data\_ark.plist |
| User Email | peterbarnes12792@icloud.com | accounts3.sqlite |
| Phone Number | 16155719608 | CellularUsage.db |
| Serial Number | FFNHHK2RPLJM | activation\_record.plist |
| ICCID | 89148000009489719791 | activation\_record.plist |
| IMEI | 35285389135063 | activation\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | provided |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | provided |

# 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 | T16.5 | data\_ark.plist |
| User Email | rosielloyd071292@icloud.com | Accounts3.sqlite |
| Phone Number | +16154278267 | CellularUsage.db |
| Serial Number | FFPHGILYPLJM | activation\_record.plist |
| ICCID | 89148000009489732844 | activation\_record.plist |
| IMEI | 359844406101632 | activation\_record.plist |
| MD5 Hash | 34c4888f095dc3241330462923f6fea5 | provided |
| SHA256 Hash | 71aed05a86a753dec4ef4033ed7f52d6577ccb534ca0d1e83ffd27683e621607 | provided |

# 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, Lead Teller at PGCU Dallas Branch

Rosie Lloyd:

Phone Number: +16154278267

Email: rosielloyd071292@icloud.com

Relationship: Conspirator, Financial Advisor at PGCU Dallas Branch

Oliver Bell:

Phone Number: +16158070242

Email: [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me)

Relationship: Conspirator, District Manager at PGCU, Midwest Region

Summary Conclusion:

Through the course of the investigation it was determined that Oliver Bell initiated the idea to steal from their employer and brought the idea to Peter Barnes. Peter Barnes then involved Rosie Lloyd to aid in execution of the theft. It was revealed that $125,000 was stolen from PGCU and from a voicemail left on Peter Barnes’ phone, Oliver Bell would continue to cover for Peter Barnes and Rosie Lloyd if he gets 20% of the stolen money.

# 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 investigation began with Peter Barnes’ iPhone Image. From the iPhone Image, Peter Barnes’ emails, SMS messages, internet history, and voicemail were accessed.

Several emails were recovered from Peter Barnes’ iPhone. Multiple emails were revealed to be correspondence between Peter Barnes and Rosie Lloyd. The emails first established a relationship between Mr. Barnes and Ms. Lloyd outside of work, where they had dinner, and discussed their displeasure in the work/financial situation **(PGCU-1 - PGCU-2)**. The email correspondence then began to discuss an idea proposal Mr. Barnes presented to Ms. Lloyd **(PGCU-3, PGCU-5 - PGCU-7)**. This email discussion introduced an unknown individual known as X, and was revealed to have come up with the original idea. The emails between Mr. Barnes and Ms. Lloyd continued into more detail about what would be needed to make the plan work and how to cover their tracks to avoid detection **(PGCU-8 - PGCU-10)**.

A second email thread was discovered between an unknown person with the email, [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me) and Peter Barnes. The emails from hockeyfan4747 were discovered to be encoded by base64. When investigating the emails on the Digital Forensic tool Autopsy, the emails could be read in text format. The email thread from hockeyfan4747 to Mr. Barnes inquired about Rosie Lloyd taking part in the plan, and then a reply from Mr. Barnes confirmed her involvement and specified that the plan should be able to go Friday. Hockeyfan4747 acknowledged Rosie Lloyd’s involvement and the plan to go ahead **(PGCU-4, PGCU-11 - PGCU-12).**

The SMS messages were then investigated and revealed more correspondence between Peter Barnes and Rosie Lloyd. The first two messages recovered were dinner invitations from Ms. Lloyd to Mr. Barnes and his acceptance to the invitation **(PGCU-13 - PGCU-14)**. The following message received from Ms. Lloyd indicated that she had completed the plan and sent Mr. Barnes a photograph (**PGCU-15**). Mr. Barnes response was Ms. Lloyd was to stay of text messages and to email instead (**PGCU-16).** The final two messages recovered from the iphone were messages from the unknown number +1685070242. The messages stated that they had left a voicemail for Mr. Barnes (**PGCU-17)** and that he needed to check his email (**PGCU-18)**.

Inside the SMS folder of Mr. Barnes iPhone two files were discovered in the attachments file. One file was an image file and the other was a movie file, **PGCU-34**  and **PGCU-33** respectively. The movie file and image file were sent from Rosie Lloyd. The movie file contained a short video of US currency in a white envelope. The image file consisted of a GPS photo location which placed Ms. Lloyd in Nashville, TN in the parking lot of a Best Buy electronics store.

The internet search history was examined on Mr. Barnes iPhone. The investigation revealed Mr. Barnes had searched for information regarding forensic accounting (**PGCU-19 - PGCU-23**) and money laundering (**PGCU-24 - PGCU-25).**

From the information gathered from the SMS messages, Mr. Barnes’ voicemail was then examined. A single voicemail was located on the iPhone, file 1.amr (**PGCU-32)**The file was extracted from the phone, using an AMR player downloaded from <https://www.amrplayer.com/>, the file was then listened to. The file revealed that Oliver Bell was an accomplice to stealing money from their employer and he would be getting a 20% cut of the theft. Mr. Bell also stated in the voicemail that he would continue to cover up evidence and that his portion of the theft should be placed into an envelope and left at his back door. The file also implicated Mr. Barnes and Ms. Lloyd in the theft of more than $125,000. The written transcript in its entirety can be found below:

*“Hey Peter, it’s me, your buddy Oliver. From my math, you and Rosie have Cleared over 125K. Remember though, I get 20% and I’ll keep clearing the audit records so Evelyn can never catch you. Give me my cash though, put it in an envelope, leave it at my back door. Pleasure doing business with you.”*

Rosie Lloyd’s iPhone Image was also examined. Emails, SMS messages and internet history were examined.

Searching through Ms. Lloyd’s emails it was found to corroborate the findings from Mr. Barnes’ phone (**PGCU-1 - PGCU-3, PGCU-5 - PGCU-10**). The emails were consistent in information and timestamps.

The SMS messages located on Ms. Lloyd’s phone were also consistent with that of Mr. Barnes’ phone (**PGCU-13 - PGCU-16).**

The search history on Ms. Lloyd’s phone revealed that she had searched for purchasing luxury cars with cash (**PGCU-26**), the pros and cons of buying a car in cash (**PGCU-27**), and how to hide large amounts of money (**PGCU-28 - PGCU-31**).

# Plot Timeline

10/12/2023

Peter Barnes and Rosie Lloyd began an email conversation establishing a personal relationship outside of work and venting their frustrations about work. The conversation ends with Mr. Barnes asking to run an idea by Ms. Lloyd.

10/18/2023

Via text message Rosie Lloyd invites Peter Barnes to dinner and he accepts

Text message from Oliver Bell to Peter Barnes to check his email.

10/19/2023

Peter Barnes searches information forensic accounting and money laundering

10/20/2023

Peter Barnes was sent an encrypted email at 01:31 GMT from hockeyfan4747 asking if Rosie Lloyd is in.

At 02:02 GMT Peter Barnes began an email thread with Rosie Lloyd, where he asks her what she thinks about his idea. Ms. Lloyd replies 02:07 GMT that she is intrigued and does Peter Barnes trust X. At 02:11 GMT Peter responds that he does trust X and that the idea was originally X’s, Peter also indicates that the idea cannot work without Ms. Lloyd’s aid. Ms. Lloyd responds she understands and needs forged withdrawal receipts to make it work (02:20 GMT) Further correspondence ensues regarding covering tracks (02:22 GMT)

Peter Barnes replies to hockeyfan4747 at 02:38 GMT stating that Rosie is in and will go ahead with the plan Friday.

Second encrypted email is sent from hockeyfan4747 confirming Peter Barnes previous email.

10/21/2023

Text message from Rosie Lloyd to Peter Barnes stating she has done it and that she sent him a photo (12:56 GMT) Reply text message from Peter Barnes insists they stay off texting and email only (12:59 GMT)

Movie file and image file sent to Peter Barnes from Rosie Lloyd.

10/23/2023

Rosie Lloyd searches purchasing luxury cars with cash and how to hide large amounts of cash.

10/25/2023

Text message from Oliver Bell to Peter Barnes that he left him a voicemail.

# Conclusion

Evidence found on Peter’’s iPhone indicated the following:

* Through emails it was determined that X gave Peter Barnes the idea to steal from their employer, PGCU.
* Peter Barnes researched how forensic accounting works and money laundering in preparation (Internet Search History)
* Peter Barnes and Rosie Lloyd have a relationship outside of work (emails and SMS)
* Peter Barnes used his relationship with Rosie Lloyd to gain her aid in stealing from PGCU (emails)
* Rosie Lloyd was provided forged withdrawal receipts in order to accomplish theft (emails)
* Text message confirmation was given to Peter Barnes when Rosie Lloyd completed the theft.
* Voice message from Oliver Bell, detailed his involvement in the theft and his knowledge of Rosie Lloyd’s involvement. Revealed the theft of more than $125,000 from PGCU.
* Comparing the timestamps from the text messages from the number +16158070242 and the corresponding emails and voicemails the texts alluded to, it was determined that Oliver Bell was the owner of this phone number and the email hockeyfan4747@proton.me.

# **Bonus Conclusion**

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

* It was determined that X was Mr. Oliver Bell, the District Manager at PGCU, Midwest Region.
* This was discovered by a comparison of voicemails, emails, and text messages.
* A voicemail was left on Peter Barnes phone, the transcript of the voicemail revealed it was from Oliver Bell. The voicemail also revealed Oliver Bell’s involvement in the PGCU theft.
* A text from +16158070242 was located and indicated that this number had left a voicemail. The only voicemail on Peter Barnes' phone was from Oliver Bell. From this it was determined the phone number belonged to Oliver Bell.
* A second text message from the same number mentioned an email. Comparing the timestamps revealed that Oliver Bell sent Peter Barnes encoded messages as [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me).

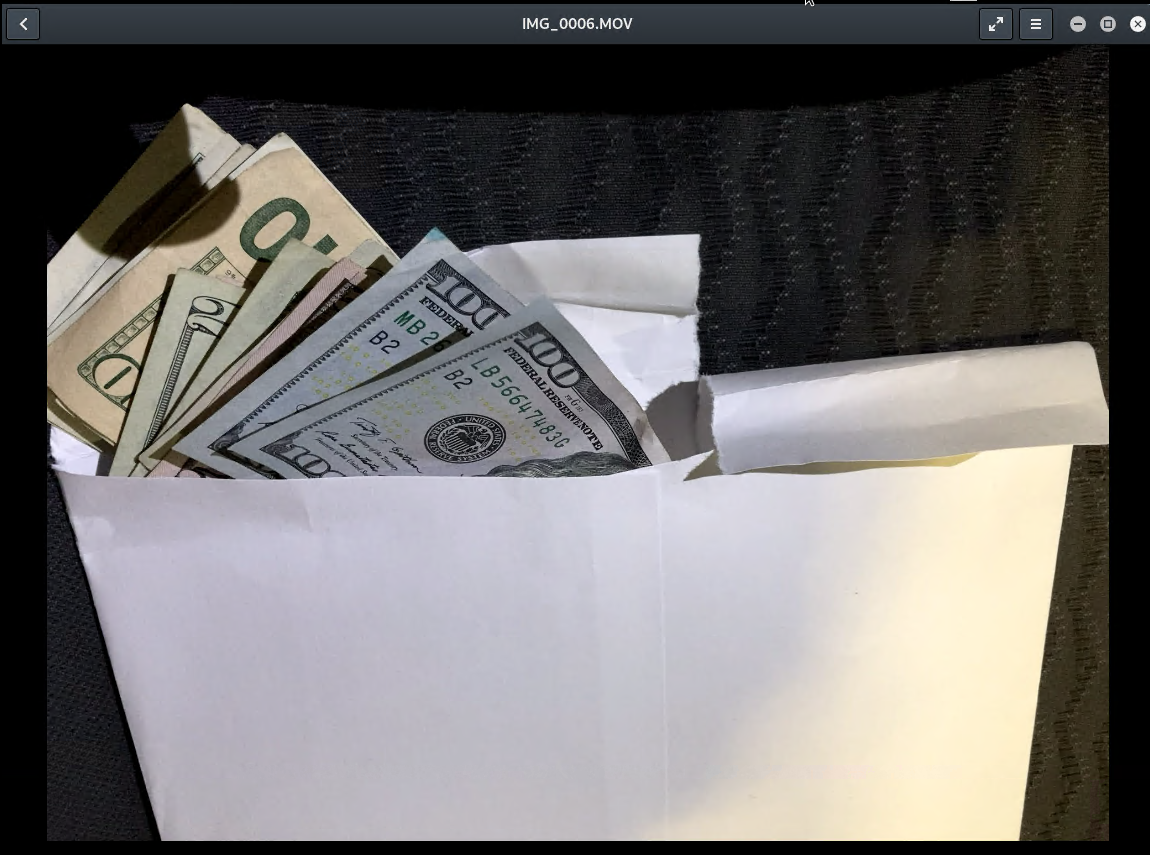
# Appendix A: Correspondence Evidence

List any sms attachments and pictures found here

### 

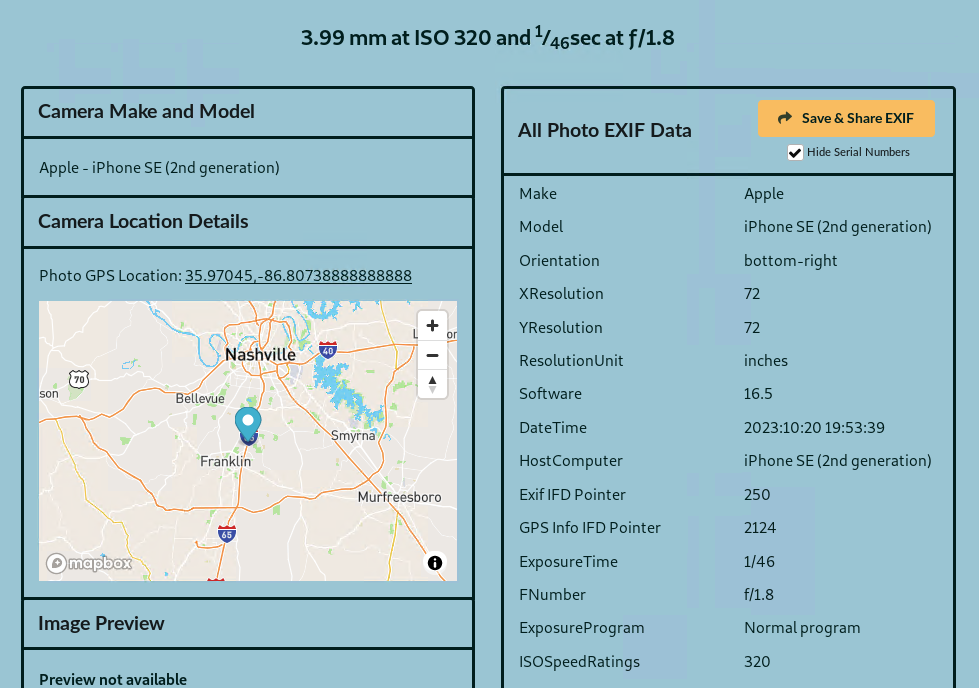
| **Master Timeline of PGCU** | | | | |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp (GMT)** | **Header Information** | **Key Information** | **Evidence Location** |
| PGCU-1 | Thur  10/12/2023  00:47:25 | Rosie Lloyd  Peter Barnes  Subject Dinner | Enjoyed dinner and glad they talked about non work | PeteriPhoneImage/mail/MessageData/10/full.emlx  RosieiPhoneImge/mail/MessageData/4/full.emlx |
| PGCU-2 | Thur 10/12/2023  22:36:11 | Rosie Lloyd  Peter Barnes  Subject: Re: Dinner | Enjoyed dinner with Peter, agrees they are not paid enough | PeteriPhoneImage/mail/MessageData/11/full.emlx  RosieiPhoneImge/mail/MessageData/7/full.emlx |
| PGCU-3 | Thur  10/12/2023  22:59:41 | Rosie Lloyd, Peter Barnes, Subject Re: Dinner | Peter Barnes wants to get together and run an idea past Rosie Lloyd | PeteriPhoneImage/mail/MessageData/12/full.emlx  RosieiPhoneImge/mail/MessageData/6/full.emlx |
| PGCU-4 | Fri 10/20/2023  01:31:07 | [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me) to Peter Barnes  Subject: Question | Encoded message (base64) from hockeyfan4747. Reads: So, is Rosie in? | PeteriPhoneImage/mail/MessageData/13/full.emlx |
| PGCU-5 | Fri  10/20/2023  02:02:43 | Rosie Lloyd,  Peter Barnes  Subject: Idea | Peter Barnes asks about his idea proposal. | PeteriPhoneImage/mail/MessageData/14/full.emlx  RosieiPhoneImge/mail/MessageData/8/full.emlx |
| PGCU-6 | Fri  10/20/2023  02:07:55 | Rosie Lloyd,  Peter Barnes  Subject: Re: Idea | Rosie is intrigued by the idea, asks about trusting X and Micheal Rokas | PeteriPhoneImage/mail/MessageData/15/full.emlx  RosieiPhoneImge/mail/MessageData/9/full.emlx |
| PGCU-7 | Fri 10/20/2023  02:11:14 | Rosie Lloyd  Peter Barnes  Subject Re: Idea | Peter says he trusts x, and it was x’s idea. Needs Rosie to make idea work. Feeling pay and work is unjustified. | PeteriPhoneImage/mail/MessageData/16/full.emlx  RosieiPhoneImge/mail/MessageData/10/full.emlx |
| PGCU-8 | Fri  10/20/2023  02:20:00 | Rosie Lloyd,  Peter Barnes  Subject: Re: Idea | Rosie understands the plan, needs forged withdrawal receipts to make it work. Asks about Catarina Mona and Lanzo Agneza | PeteriPhoneImage/mail/MessageData/17/full.emlx  RosieiPhoneImge/mail/MessageData/11/full.emlx |
| PGCU-9 | Fri 10/20/2023  02:22:57 | Rosie Lloyd  Peter Barnes  Subject: Re: Idea | Peter tells rosie how to cover her tracks and watch what she puts in emails so they don’t get caught | PeteriPhoneImage/mail/MessageData/18/full.emlx  RosieiPhoneImge/mail/MessageData/12/full.emlx |
| PGCU-10 | Fri  10/20/2023  02:33:47 | Rosie Lloyd  Peter Barnes  Subject: Re: Idea | Rosie tells Peter to relax and she will cover her tracks | PeteriPhoneImage/mail/MessageData/19/full.emlx  RosieiPhoneImge/mail/MessageData/13/full.emlx |
| PGCU-11 | Fri 10/20/2023  02:38:10 | [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me)  Peter Barnes  Subject: Re: Question | Reply about Rosie and something is good to go on friday with hockeyfan4747 | PeteriPhoneImage/mail/MessageData/20/full.emlx |
| PGCU-12 | Fri 10/20/2023  02:43:23 | [hockeyfan4747@proton.me](mailto:hockeyfan4747@proton.me) to Peter Barnes  Subject: Re: Question | Encoded message (base64) from hockeyfan4747. “Excellent!” | PeteriPhoneImage/mail/MessageData/21/full.emlx |
| PGCU-13 | Wed 10/18/2023 03:39:05 | Rosie Lloyd (+16154278267)  Peter Barnes (+16155719608) | SMS message from Rosie Lloyd to Peter Barnes inviting him to dinner. | RosieiPhoneImage/SMS/sms.db |
| PGCU-14 | Wed, 10/18/2023 03:40:48 | Rosie Lloyd (+16154278267)  Peter Barnes (+16155719608) | SMS message from Peter Barnes to Rosie Lloyd agreeing to dinner. | RosieiPhoneImage/SMS/sms.db  PeteriPhoneImage/SMS/sms.db |
| PGCU-15 | Sat, 10/21/2023 12:56:57 | Rosie Lloyd (+16154278267)  Peter Barnes (+16155719608) | SMS message from Rosie Lloyd to Peter Barnes, claims she did it and headed to the mall and that she sent him a photo | RosieiPhoneImage/SMS/sms.db  PeteriPhoneImage/SMS/sms.db |
| PGCU-16 | Sat  10/21/2023 12:59:48 | Rosie Lloyd (+16154278267)  Peter Barnes (+16155719608) | SMS message from Peter Barnes to Rosie Lloyd. Tells her to avoid texting. | RosieiPhoneImage/SMS/sms.db  PeteriPhoneImage/SMS/sms.db |
| PGCU-17 | Wed  10/25/2023 06:37:50 | Oliver Bell (+16158070242)  Peter Barnes (+16155719608) | SMS message from Oliver Bell to Peter Barnes relaying that he left him a voicemail | PeteriPhoneImage/SMS/sms.db |
| PGCU-18 | Wed  10/18/202303:59:47 | Oliver Bell (+16158070242)  Peter Barnes (+16155719608) | SMS message from Oliver Bell to Peter Barnes advising him to check his email | PeteriPhoneImage/SMS/sms.db |
| PGCU-19 | Thur  10/19/2023  09:46:30 | Peter Barnes  Google | Browsing History from Peter Barnes: Google Search: forensic accounting | PeteriPhoneImage/Safari History/History.db |
| PGCU-20 | Thur  10/19/2023  09:50:00 | Peter Barnes  Website: Wikipedia | Wikipedia webpage for forensic accounting | PeteriPhoneImage/Safari History/History.db |
| PGCU-21 | Thur  10/19/2023  09:53:20 | Peter Barnes  Google | Google Search: forensic accounting how to not get detected | PeteriPhoneImage/Safari History/History.db |
| PGCU-22 | Thur  10/19/2023  09:48:50 | Peter Barnes  Google | Google Search: forensic accounting how to not get detected | PeteriPhoneImage/Safari History/History.db |
| PGCU-23 | Thur  10/19/2023  09:53:20 | Peter Barnes  Website: Forensic Accounting Advice | Website: Forensic Accounting Advice: How to Minimize the Risk of Fraud in Your Business | PeteriPhoneImage/Safari History/History.db |
| PGCU-24 | Thur  10/19/2023  10:05:00 | Peter Barnes  Google | Google Search: Money laundering 101 | PeteriPhoneImage/Safari History/History.db |
| PGCU-25 | Thur  10/19/2023  10:05:00 | Peter Barnes  Website: Money Laundering 101 | Website: Understanding the basics | PeteriPhoneImage/Safari History/History.db |
| PGCU-26 | Mon  10/23/2023  04:33:49 | Rosie Lloyd  Google | Google Search: Purchasing luxury cars with cash | RosieiPhoneImage/Safari History/History.db |
| PGCU-27 | Mon  10/23/2023  04:33:49 | Rosie Lloyd  Website: Kelly Blue Book | Paying Cash for a Car: Pros and Cons | RosieiPhoneImage/Safari History/History.db |
| PGCU-28 | Mon  10/23/2023  04:35:29 | Rosie Lloyd  Google | Google Search: best places to store large amounts of cash | RosieiPhoneImage/Safari History/History.db |
| PGCU-29 | Mon  10/23/2023  04:35:29 | Rosie Lloyd  Website | 5 Best Places to Hide Emergency Cash at Home | RosieiPhoneImage/Safari History/History.db |
| PGCU-30 | Mon  10/23/2023  04:39:59 | Rosie Lloyd  Google | Google Search: how to hide case in home | RosieiPhoneImage/Safari History/History.db |
| PGCU-31 | Mon  10/23/2023  04:39:59 | Rosie Lloyd  Website: Family Handyman | 50 Secret Hiding Places for Valuables in your Home | RosieiPhoneImage/Safari History/History.db |
| PGCU-32 | Unknown | Peter Barnes (+16155719608)  Oliver Bell (+16158070242) | Voicemail from Oliver Bell. Voicemail details Oliver Bell's involvement, also implicates Peter Barnes and Rosie Lloyd in the theft of $125,000. Oliver Bell directs Peter Barnes on how to deliver his portion of the theft. | PeteriPhoneImage/Voicemail/1.amr |
| PGCU-33 | Sat, 10/21/2023 12:56:57 | Rosie Lloyd  Peter Barnes | Movie file sent to Peter Barnes from Rosie Lloyd | PeteriPhoneImage/SMS/Attachments/33/03/00E33F22-7F93-41B1-80DB-D9CFAD02E410.pvt/IMG\_0006.MOV |
| PGCU-34 | Sat, 10/21/2023 12:56:57 | Rosie Lloyd  Peter Barnes | Image file sent to Peter Barnes from Rosie Lloyd | PeteriPhoneImage/SMS/Attachments/33/03/00E33F22-7F93-41B1-80DB-D9CFAD02E410.pvt/IMG\_0006.HEIC |

### 



PGCU-33 : Still from movie file sent to Peter Barnes from Rosie Lloyd. Movie file showing US currency inside of a white envelope.

# Appendix B: GPS Location Information



PGCU-34 : Image file sent to Peter Barens from Rosie Lloyd. GPS coordinates place Rosie Lloyd at Best Buy in Brentwood,, TN. The Photo GPS location corresponds with the movie file Rosie Lloyd sent to Peter Barnes showing an envelope with US currency inside.

# 