|  |
| --- |
| 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.

Evelyn Lane, Bank Manager at Pure Gold Credit Union (PGCU) – Dallas Branch, discovered a significant discrepancy during the branch’s bi-annual audit. Nearly $100,000 in cash transactions had gone unaccounted for over the past six months.

An initial investigation revealed that several employees referenced a mysterious individual referred to as "Mr. X," who was reportedly disgruntled over their treatment at PGCU. Upon escalating the matter to senior management, all company-issued mobile devices were confiscated from employees at the Dallas branch as part of a broader forensic review.

Peter Barnes was identified as the initial suspect and was subsequently placed on suspension pending the outcome of the investigation. In addition to his cell phone, all relevant digital evidence associated with his accounts and access was secured for examination.

### Equipment and Tools

* Kali Linux
* Autopsy
* Sqlite DB Browser
* Windows Media

# Details of Peter’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location/File  in iPhone image file** |
| Model | iPhone12.8 | LogicalFileSet(1)/peter/File for Identifiers/activation\_record.plist |
| Host Name | Peter’s iPhone | LogicalFileSet(1)/peter/File for Identifiers/data\_ark.plist |
| OS Version | V16.5.1 | LogicalFileSet(1)/peter/File for Identifiers/data\_ark.plist |
| User Email | [peterbarnes12792@icloud.com](mailto:peterbarnes12792@icloud.com) | LogicalFileSet(1)/peter/File for Identifiers/Accounts3.sqlite |
| Phone Number | +16155719608 | LogicalFileSet(1)/peter/File for Identifiers/CellularUsage.db |
| Serial Number | FFNHHK2RPLJM | LogicalFileSet(1)/peter/File for Identifiers/activation\_record.plist |
| ICCID | 89148000009489719791 | LogicalFileSet(1)/peter/File for Identifiers/activation\_record.plist |
| IMEI | 352853889135063 | LogicalFileSet(1)/peter/File for Identifiers/activation\_record.plist |
| MD5 Hash | cbcc58b538466287895220d1a763d5ed | /home/kali/Desktop/imagefiles/peter.orig.md5log.txt |
| SHA256 Hash | 0c559080e112633baaf1b60a15b2873534f2822b54ac1ba707421688323a6b37 | /home/kali/Desktop/imagefiles/peter.orig.sha256log.txt |

# Details of Rosie’s iPhone

|  |  |  |
| --- | --- | --- |
| **Name** | **Findings** | **Location/File  in iPhone image file** |
| Model | iPhone12,8 | LogicalFileSet(1)/rosie/File for Identifiers/activation\_record.plist |
| Host Name | Rosie’s iPhone | LogicalFileSet(1)/rosie/File for Identifiers/data\_ark.plist |
| OS Version | 16.5 | LogicalFileSet(1)/rosie/File for Identifiers/data\_ark.plist |
| User Email | rosielloyd071292@icloud.com | LogicalFileSet(1)/rosie/File for Identifiers/Accounts3.sqlite |
| Phone Number | +16154278267 | LogicalFileSet(1)/rosie/File for Identifiers/CellularUsage.db |
| Serial Number | FFPHG1LYPLJMRosie’s iPhone | LogicalFileSet(1)/rosie/File for Identifiers/activation\_record.plist |
| ICCID | 89148000009489732844 | LogicalFileSet(1)/rosie/File for Identifiers/activation\_record.plist |
| IMEI | 359844406101632 | LogicalFileSet(1)/rosie/File for Identifiers/activation\_record.plist |
| MD5 Hash | e666cd1232ead8f76c0a42910f54b7d5 | /home/kali/Desktop/imagefiles/rosie.orig.sha256log.txt |
| SHA256 Hash | 0aa14fa06a416fd59c1e6586c888dd3511b1a98c7a01915233181866bedd7671 | /home/kali/Desktop/imagefiles/rosie.orig.sha256log.txt |

# 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](mailto:peterbarnes12792@icloud.com)

Relationship: Accused

Rosie:

Phone Number: +16154278267

Email: rosielloyd071292@icloud.com

Relationship: Co-conspirator, Peter’s coworker.

List any other contacts here

**Oliver Bell:**

Alias: Mr. X ?

Phone Number: 6158070242

Email: hockeyfan4747@proton.me

Relationship: PGCU’s District Manager, is suspected of being a co-conspirator or

mastermind.

**Catarina Mona**:

Relationship: Peter's co-worker, a Bank Teller.

**Lanzo Agneza**:

Relationship: Peter's co-worker, a Bank Teller.

**Michaela Rokas**:

Relationship: Peter's co-worker, a Bank Teller.

The primary suspects in the investigation are **Peter Barnes** and **Rosie Lloyd**. The most significant cash discrepancies occurred during Peter Barnes' shift as lead bank teller, and Rosie Lloyd was frequently seen in close communication with him. This prompted the collection of digital evidence from both individuals.

Data from Peter’s phone implicated a third party, referred to as **"Mr. X,"** as the possible mastermind behind the theft. A matching phone number and email address were found in Peter’s communications, and analysis suggests both were used by the same individual. A final SMS and voicemail linked **Mr. X** to a person identified as **Oliver Bell**.

While **Catarina Mona**, **Lanzo Agneza**, and **Michaela Rokas** were mentioned in various emails, no direct evidence of their involvement was found on Peter or Rosie’s devices. Further investigation is needed to determine their roles, if any.

# Evidence relating to theft of PGCU funds

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

1. Evidence that was found in Peter's phone confirms that he corresponded with Rosie "hockeyfan4747".
2. Evidence found in Peter's phone confirms the sms correspondence between him and Rosie, as well between him and unknown/unsaved number 16158070242.
3. Peter’s phone had some incriminating images, video and phone mail evidence linking him to the crime and possible exposing the identity of Mr X
4. Further evidence was found on Peter's phone, including internet search history containing queries related to *"money laundering"* and *"forensic accounting,"* suggesting a possible link to the crime.

**Legal Summary of Evidence – PGCU Internal Theft Case**

**Case Overview:**  
A forensic investigation was launched by PGCU's Dallas Branch following the discovery of significant financial discrepancies during a bi-annual audit. The total unaccounted cash was estimated at approximately **$100,000**. This summary outlines key findings from digital evidence artifacts recovered from the mobile devices of employees, with particular focus on **Peter Barnes** and **Rosie Lloyd**.

**I. Email Evidence**

**Artifacts #7–12**

* **Rosie Lloyd** requested **Peter Barnes** to obtain copies of forged withdrawal receipts to begin executing the fraudulent scheme.
* Rosie asked Peter whether he trusted **Mr. X**, **Michaela Rokas**, **Catarina Mona**, and **Lanzo Agneza**.
* Peter confirmed that **Mr. X** had proposed the plan and, driven by financial hardship and discontent with executive compensation, he was ready to act—with Rosie’s assistance.
* Peter advised Rosie to keep sensitive details out of emails and to delete existing messages to cover their tracks.

**Artifacts #6, 13, 14**

* Peter received a message from **hockeyfan4747@proton.me** inquiring if Rosie was aligned with the plan.
* In his reply to the October 18, 2023 message titled *“Question”*, Peter confirmed the operation would begin that Friday.

**II. SMS/Text Message Evidence**

**Artifacts #4–5**

* Rosie messaged Peter stating she *“did it today,”* was going to the mall, and had sent a photo.
* Peter responded by instructing her to stop using SMS and to communicate via email instead.

**Artifacts #6–7**

* Peter received a message from an **unsaved number** (same as the one from October 18) informing him of a voicemail being left, linking back to earlier communications.

**III. Web Browsing Activity**

**Artifacts #1–6**

* Peter’s browser history included searches related to **“money laundering”** and **“forensic accounting,”** strongly suggesting forethought and knowledge of criminal financial practices.

**IV. Media Evidence (Images, Video, Audio)**

**Artifacts #1–3**

* Recovered data from Peter’s phone included:
  + An image sent by Rosie depicting an envelope filled with cash.
  + A **voicemail from Oliver Bell**, in which he demanded **20% of the $125,000** and claimed he would continue falsifying audit records to avoid detection by **Branch Manager Evelyn Lane**.
  + Additional media links Peter, Rosie, and **Mr. X** directly to the planning and execution of the theft.

**V. GPS Location Evidence**

**Artifacts #1–2**

* Embedded GPS metadata from a **.HEIC file** confirmed the physical location where Rosie’s photograph (of the money envelope) was taken, corroborating her involvement in the fraudulent activity.

**Conclusion**

The body of evidence, including emails, messages, browsing history, media files, and location data, implicates **Peter Barnes**, **Rosie Lloyd**, and a third party known as **Mr. X** in the planning and execution of a substantial internal theft at PGCU. While the names **Michaela Rokas**, **Catarina Mona**, and **Lanzo Agneza** were mentioned, no direct evidence currently links them to criminal involvement. Further investigation is required to confirm or rule out their participation.

# Plot Timeline

| **Date/Time** | **Communication** | **Description** |
| --- | --- | --- |
| **Wednesday Oct 11, 2023** | **email** | Hey Rosie, great hanging out w=  ith you this weekend! Always good to hang out and talk about non work thin=  gs |
| **Thursday Oct 12, 2023** | **email** | I hear=0A you, I=E2=80=99m really frustrated as well. Lets get together a=  fter work tonight,=0A wanted to run something by you.Peter BarnesOn Oct 1=  2, 2023, at 5:36 PM, Rosie Lloyd <rosielloyd071292@icloud.com> wrote:Hey=0A=  Peter, Likewise, was so great to get a chance to hang out, outside of=0A=  work.=C2=A0 Sounds like we both feel that we=0A aren't being paid enoug=  h, and on top of that all the Gold Credit Union=0A executives are pulling=  up in sports cars.=C2=A0 Its really frustrating :( .RosieWE |
| **Wednesday Oct 18, 2023** | **SMS** | Rosie messaged Peter on his mobile phone agreeing to see  each other later. |
| **Wednesday Oct 18, 2023** | **SMS** | Peter received a sms message on his phone from an  unsaved/unknown number asking him to check his email. |
| **Wednesday Oct 18, 2023** | **Email** | Yes, we are good, should get this going this FridayPeter BarnesOn Oct 18, =  2023, at 8:31 PM, hockeyfan4747 <hockeyfan4747@proton.me> wrote:So, is Ros=  ie in?=C2=A0Sent with Proton Mail secure email. |
| **Thursday OCT 19, 2023** | **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 evidence. You are=  being a little reckless and going to get us caught. They are ok, I get al=  ong with them for the most part.Peter BarnesOn Oct 19, 2023, at 9:20 PM, R=  osie Lloyd <rosielloyd071292@icloud.com> wrote:Yup, you explained it well =  last night.=C2=A0 Just get me the copies of the forged withdrawal receipts=  so I can get this going. Also, what about Catarina Mona and Lanzo, I thin=  k her last name is Agneza ?=C2=A0Rosie LloydOn Oct 19, 2023, at 9:11 PM, P=  eter Barnes <peterbarnes12792@icloud.com> wrote:I trust X, it was actually=  X that brought this idea to me a while back.=C2=A0 I thought they were ki=  dding, but X kept asking.=C2=A0 Now after seeing the exec=E2=80=99s gettin=  g rich while I have trouble paying my bills, I am ready to put this into a=  ction.=C2=A0 But I need your help to make this work. You know what to do n=  ext?Peter BarnesOn Oct 19, 2023, at 9:07 PM, Rosie Lloyd <rosielloyd071292=  @icloud.com> wrote:Honestly, I am intrigued.=C2=A0 Was up all night thinki=  ng about it, and how we can pull it off.=C2=A0 Are you sure =E2=80=9CX=E2=80=  =9D can help us out?=C2=A0 Do you trust X ?=C2=A0 How about Michaela Rokas=  ?Rosie LloydOn Oct 19, 2023, at 9:02 PM, Peter Barnes <peterbarnes12792@i=  cloud.com> wrote:Great getting together again last night, what did you thi=  nk of the =E2=80=98idea=E2=80=99 I ran by you?Peter Barnes  --Apple-Webmail-42--8c916441-07b1-4508-98b8-c26c01f865df |
| **Thursday OCT 19, 2023** | **Email** | To: "peterbarnes12792@icloud.com" <peterbarnes12792@icloud.com>  From: hockeyfan4747 <hockeyfan4747@proton.me>  Subject: Question  Yes, we are good, should get this going this FridayPeter BarnesOn |
| **Friday Oct 20, 2023** | **SMS** | Peter received an SMS message from Rosie saying  “she did it today”, was going to the mall, and had sent  him a picture.  Peter asked her to stop sending him messages on the  phone and to email him instead. |
| **Wednesday Oct 25, 2023** | **SMS** | Peter received a sms message on his phone from an  unsaved/unknown number (same number that messaged him  on Oct 18, 2023) saying he left Peter a voice message. |
|  |  |  |

# Conclusion

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

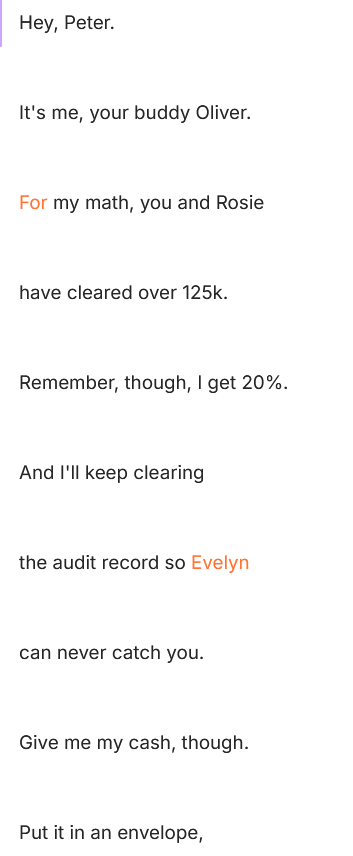
* Email correspondence between Peter and Rosie reveals that both individuals felt underpaid and were struggling financially.
* SMS messages and images retrieved from a mobile device confirm that Peter and Rosie were responsible for the theft. A photo sent by Rosie, accompanied by GPS metadata, substantiates their involvement.
* Further investigation by Digitech Inc. uncovered email and SMS communications referencing a third party identified only as "X." This alias appeared in multiple exchanges between Peter and Rosie. Peter later disclosed that "X" was the architect behind the theft scheme.
* Digitech Inc. also found an email from an account using the alias **hockeyfan4747** (hockeyfan4747@proton.me) requesting an update on the operation. This email followed a text message instructing Peter to check his inbox, suggesting that "hockeyfan4747" communicated through both SMS and email. This individual is suspected to be Mr. X, but further investigation is required to confirm their identity.
* The phone number that sent the SMS also left a voicemail for Peter. The caller identified himself as *Oliver*. Voice analysis later confirmed the speaker as Oliver Bell, District Manager at Pure Gold Credit Union's Midwest Region. A transcript of the voicemail is provided below.

# **Bonus Conclusion**

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

* Mr. X made deliberate efforts to conceal his identity. He used a generic, anonymous email address (*hockeyfan4747@proton.me*) and communicated only twice through an unregistered phone number, minimizing traceable digital footprints. Despite his caution, the key piece of evidence linking him to a real identity is a voicemail he left for Peter, in which he identified himself as "Oliver" while inquiring about receiving his share of the stolen money. Voice analysis will confirmed that the speaker was Oliver Bell, the District Manager at Pure Gold Credit Union's Midwest Region, strongly suggesting that Oliver Bell is Mr. X, the orchestrator of the scheme.

The transcript from the voice mail is found here:



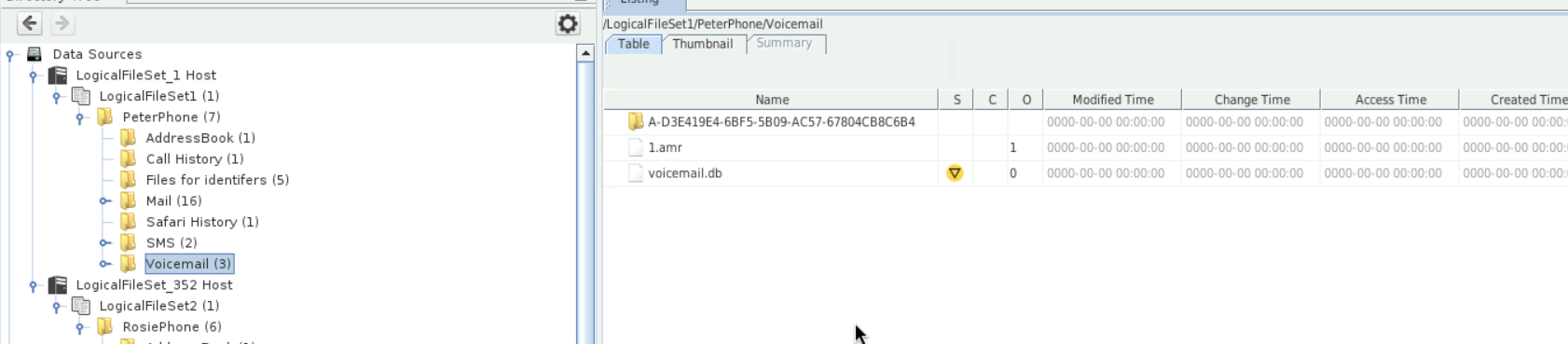
# Appendix A: Correspondence Evidence

## Email Artifact Table

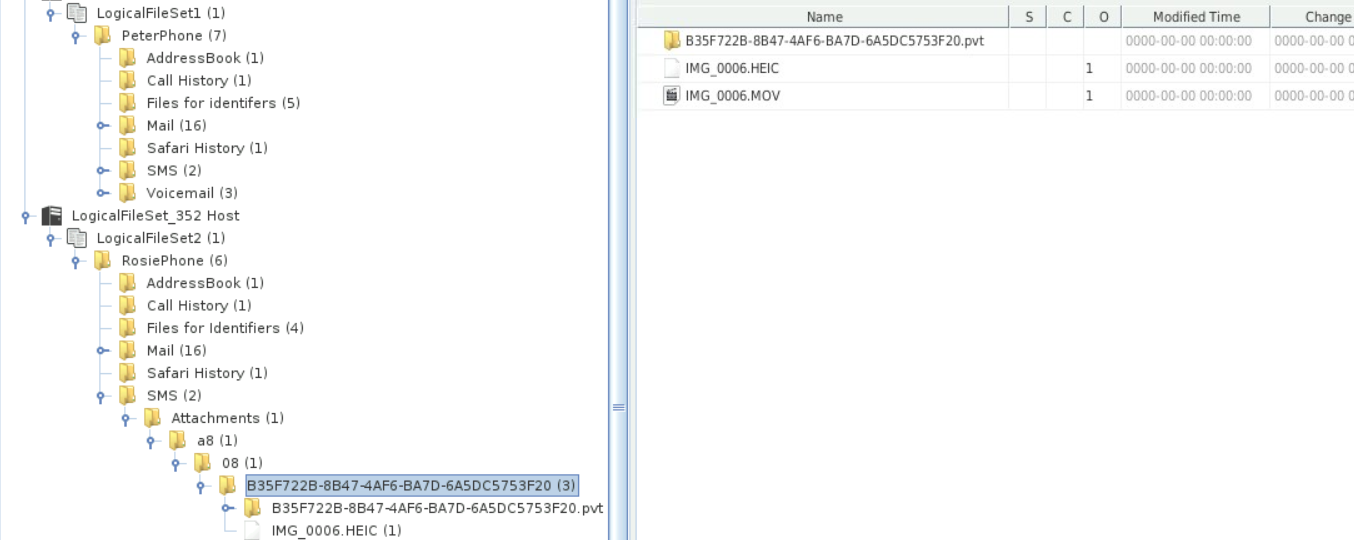
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Artifact #** | **Timestamp** | **Header Information** | **Key Information** | **Evidence Location** |
| 1 | Wed, Oct 11, 2023, at 7:39:24 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: rosieloyd071292@icloud.com Subject: Dinner | Peter emailed Rosie about spending time together and avoiding work-related talk. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/9/ |
| 2 | Wed, Oct 11, 2023, at 7:39:25 PM CDT | From: Mail Delivery System <postmaster@icloud.com> To: peterbarnes12792@icloud.com Subject: Undelivered Mail Returned to Sender | Peter’s email to Rosie bounced back due to an incorrect address. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/8/ |
| 3 | Wed, Oct 11, 2023, at 7:47:24 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: rosielloyd071292@icloud.com Subject: Dinner | Peter resent the message to the correct email address, referencing their weekend. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/10/ |
| 4 | Thu, Oct 12, 2023, at 5:36:08 PM CDT | From: Rosie Lloyd <rosielloyd071292@icloud.com> To: Peter Barnes <peterbarnes12792@icloud.com> Subject: Re: Dinner | Rosie replied they both felt underpaid and frustrated by executive luxury. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/11/ |
| 5 | Thu, Oct 12, 2023, at 5:59:41 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: Rosie Lloyd <rosielloyd071292@icloud.com> Subject: Re: Dinner | Peter suggested meeting after work to discuss an idea. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/12/ |
| 6 | Wed, Oct 18, 2023, 20:31:07 CDT | From: hockeyfan4747 <hockeyfan4747@proton.me> To: peterbarnes12792@icloud.com Subject: Question | An anonymous sender asked Peter if Rosie was onboard with the plan. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/13/ |
| 7 | Thu, Oct 19, 2023, at 9:02:43 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: Rosie Lloyd <rosielloyd071292@icloud.com> Subject: Idea | Peter followed up on their prior meeting and asked Rosie’s thoughts about the plan. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/14/ |
| 8 | Thu, Oct 19, 2023, at 9:07:55 PM CDT | From: Rosie Lloyd <rosielloyd071292@icloud.com> To: Peter Barnes <peterbarnes12792@icloud.com> Subject: Re: Idea | Rosie showed interest and asked if Peter trusted 'X' and mentioned others who could help. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/15/ |
| 9 | Thu, Oct 19, 2023, at 9:11:14 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: Rosie Lloyd <rosielloyd071292@icloud.com> Subject: Re: Idea | Peter confirmed X’s involvement and discussed motivation behind the plan. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/16/ |
| 10 | Thu, Oct 19, 2023, at 9:19:59 PM CDT | From: Rosie Lloyd <rosielloyd071292@icloud.com> To: Peter Barnes <peterbarnes12792@icloud.com> Subject: Re: Idea | Rosie asked for forged receipts and mentioned Catarina Mona and Lanzo Agneza. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/17/ |
| 11 | Thu, Oct 19, 2023, at 9:22:57 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: Rosie Lloyd <rosielloyd071292@icloud.com> Subject: Re: Idea | Peter urged Rosie to delete the emails and avoid discussing the plan through email. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/18/ |
| 12 | Thu, Oct 19, 2023, at 9:33:47 PM CDT | From: Rosie Lloyd <rosielloyd071292@icloud.com> To: Peter Barnes <peterbarnes12792@icloud.com> Subject: Re: Idea | Rosie agreed to delete the emails and reassured Peter. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/19/ |
| 13 | Thu, Oct 19, 2023, at 9:38:10 PM CDT | From: Peter Barnes <peterbarnes12792@icloud.com> To: hockeyfan4747 <hockeyfan4747@proton.me> Subject: Re: Question | Peter confirmed that everything was ready and they would proceed on Friday. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/20/ |
| 14 | Thu, Oct 19, 2023, at 9:43:23 PM CDT | From: hockeyfan4747 <hockeyfan4747@proton.me> To: Peter Barnes <peterbarnes12792@icloud.com> Subject: Re: Question | The anonymous sender confirmed receipt of Peter’s response and expressed approval. | LogicalFileSet1/PeteriPhoneImage/Mail/MessageData/21/ |

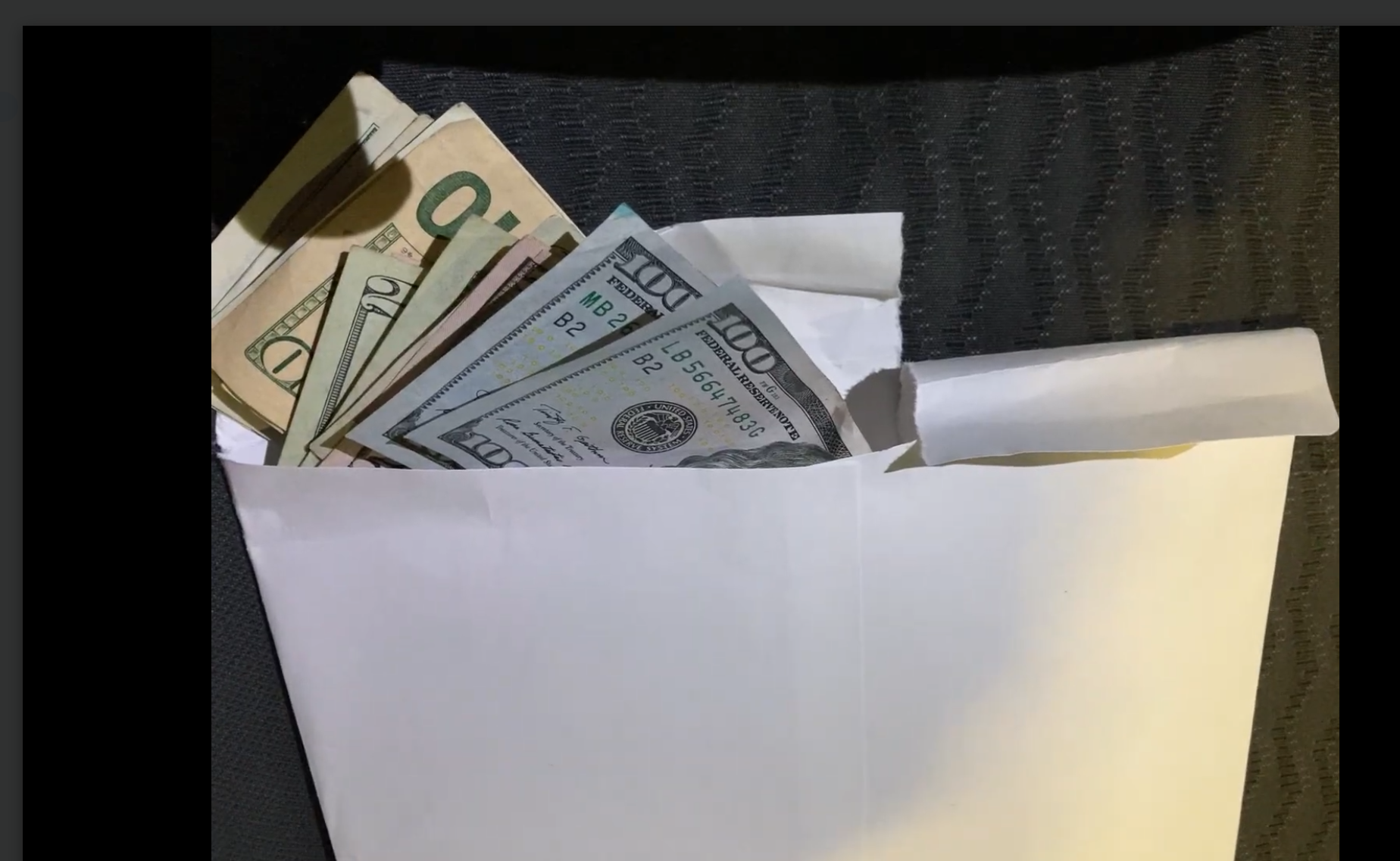
List any sms attachments and pictures found here

Audio File transcript provided above



Movie and HEIC to get location





# Appendix B: GPS Location Information

[