

CYBERSECURITY AND FRAUD IMPACTS ON UNCLAIMED PROPERTY

Wednesday —October 13th, 2021



NATIONAL ASSOCIATION OF
UNCLAIMED PROPERTY ADMINISTRATORS



NATIONAL ASSOCIATION OF
STATE TREASURERS

Features of Zoom Webinar

All audience members are muted.

Use “Q & A” to ask questions of the panelists and organizers.

Presenting

Jonathan Fairtlough, Managing Director, Cyber Risk, Kroll
Government Solutions

Ken Wagers, Vice President, Client Information Service, Kelmar
Associates, LLC

Alan McBride, Investigator, Louisiana Department of the
Treasury





Deep and Dark Web Findings

Unclaimed Property Fraud Overview

Kroll Services



01

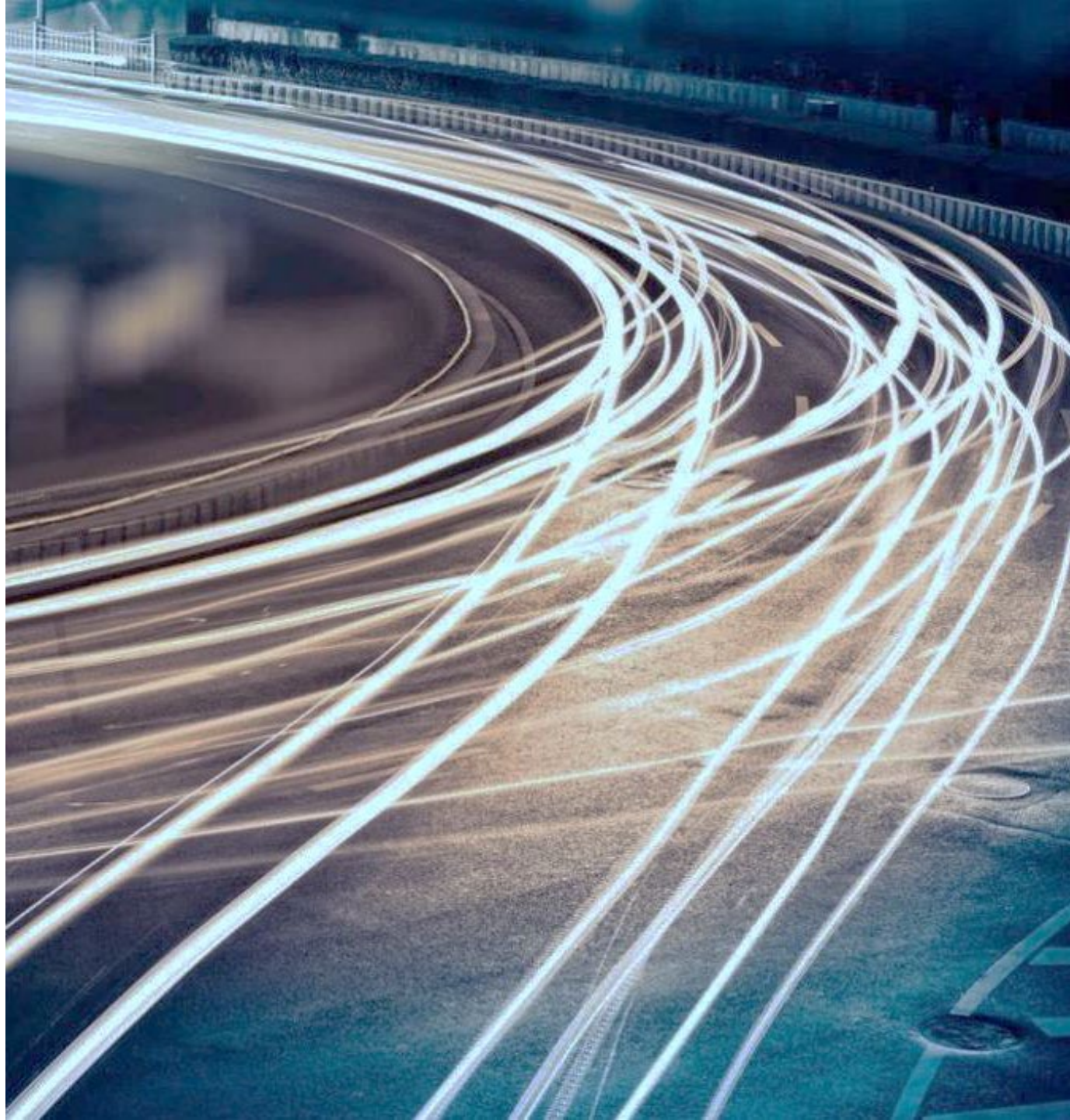
Key Takeaways

Key Takeaways

Kroll identified a variety of results referencing unclaimed property fraud on deep and dark web marketplace and in cybercrime/hacking forums.

Malicious actors upload images of States' unclaimed property on forums, including the names and mailing addresses of the legitimate property owners. They are then able to obtain fake identification mimicking the PII of the legitimate owners, allowing them to fraudulently claim the property.

Among other illicit products, dark web forums and paste sites often sell fake ID's, including driver's licenses and passports. Malicious actors are able to purchase photo identification matching the name and physical address of individuals with unclaimed property in any given State. These IDs are then able to be used to fraudulently claim said property.



02

DDW FINDINGS

References to Unclaimed Property Fraud in Telegram Chatroom

Kroll identified a July 12, 2021 Telegram chatroom message that includes an image of a US State Department of Treasury Unclaimed Property form. The form is for a \$384.00 check reportedly belonging to a US university. The "Claimant Information" portion of the form has been left blank.

The user appears to be looking for someone with driver's license editing capabilities, most likely to fraudulently fill out the form matching the legitimate owner's, whose name and mailing address is included on the form.

Chatroom Details:

Chat Type: Telegram

Channel: MAD-HACKERS

Channel Type: Supergroup

Contributors: 17,383

Messages: 704,874

Created on: April 02, 2019

Jul 12, 2021 09:37:29 Horror Games

Come for this update if you edit driver's license

📎 | 69 KB .jpg (image/jpeg) | SHA1: e25b8cc1a0e00f43c02b61d9adb4c452f0dcf6ff | Filename: e25b8cc1a0e00f43c02b61d9adb4c452f0dcf6ff.jpg

← 162599101824...

State Treasurer
Department of the Treasury
unclaimed Property Division

Claim ID: 8424807
Date: 8/11/2021

Dear Claimant:

The State of _____ Unclaimed Property Division is holding funds or securities for the individual(s) listed below in Section B. If you believe that you are the owner of the item(s) listed, complete Section A of this claim form. If we require additional documentation from you, it will be indicated in Section C and should be returned with the completed claim form.

There is no charge for this service. We appreciate the opportunity to be of assistance.

ALL AREAS MUST BE COMPLETED BELOW:

A. Claimant Information

Name(s) to appear on check: _____ Daytime Phone: () - _____

Current Mailing Address (this is where check will be mailed):
City: _____ State: _____ Zip: _____

Email Address: _____ Date of Birth: / /

Tax identification number for reporting purposes, SSN for an individual or FEIN for a business: _____

B. Property Information

Owner	Company/Security Name	Type of Property	Property ID	Value
STATE UNIV RIVER ROAD RM 1043 BATON ROUGE, LA 70803	UNIVERSITY OF C	Type: CHECK, VENDOR CHECKS Report Year: 2020	12317336	Cash \$384.00
PKYEE			INTEREST FORGONE BY CLAIMANT, TEL, NO INT RATE	Shares 0.0000

Total Shares Claimed: 0.0000 Total Cash: \$384.00

Images courtesy of Flashpoint

References to Unclaimed Property Fraud in Telegram Chatroom

Kroll identified an April 28, 2021 Telegram chatroom message that includes an image of a US State Department of Treasury Unclaimed Property Administration form.

The form is for a \$90,000 cashiers check and includes the email address, DOB, and phone number of the legitimate owner. The portion of the form requiring proof of ID has been left blank, allowing malicious actors to seek fraudulent identifications in the owner's name.

Chatroom Details:

Chat Type: Telegram

Channel: Juicy Kingdom

Channel Type: Supergroup

Contributors: 1,991

Messages: 46,329

Created on: December 15, 2020

State of [redacted] Department of the Treasury Unclaimed Property Administration

01/10/2021

A. Claimant Information

Name (s) if different than above: [redacted] Home Phone: [redacted]

Current Mailing Address if different than above: [redacted]

Email Address: [redacted].COM Date of Birth: 07/24/[redacted]

B. Property Information

Owner	Company/Security Name	Property Type	Last Activity Date	Property ID	Value
[redacted]	PNCBANK NATIONAL ASSOCIATION	CASHIER'S CHECKS	10/04/2016	325 [redacted]	\$90,000.00
Total Cash:					\$90,000.00

C. Security Information

Not Applicable

D. Documentation Required

- ☐ **Official Identification** Please provide a copy of your driver's license or other official government identification such as your passport, military ID or state-issued identification card.
- ☐ **Proof of SSN** Please provide verification of your social security number such as a copy of your Social Security card, correspondence from the Social Security administration, tax document or paycheck stub.
- ☐ **Proof of Reported Address** If the reported address(es) listed in the 'Property Information' section is no longer current, proof of prior address is required. Acceptable documents include utility bill, bank statement, tax documentation, official school document, etc.
- ☐ **Notarized Signature** Please obtain valid notarization(s) for **ALL** signatures.
- ☐ **Signature** Please return a completed and executed claim form.

Page 1 / 2

Image courtesy of Flashpoint

References to Unclaimed Property Fraud in Telegram Chatroom

Kroll identified a December 5, 2020 Telegram chatroom message that includes an image of an unknown website selling access to a variety of compromised databases, including ones for unclaimed property.

The user who posted the image was referencing the Driver's License database also available of the site. The chatroom discussions cover a range of hacking topics, including different types of fraud.

Chatroom Details:

Chat Type: Telegram

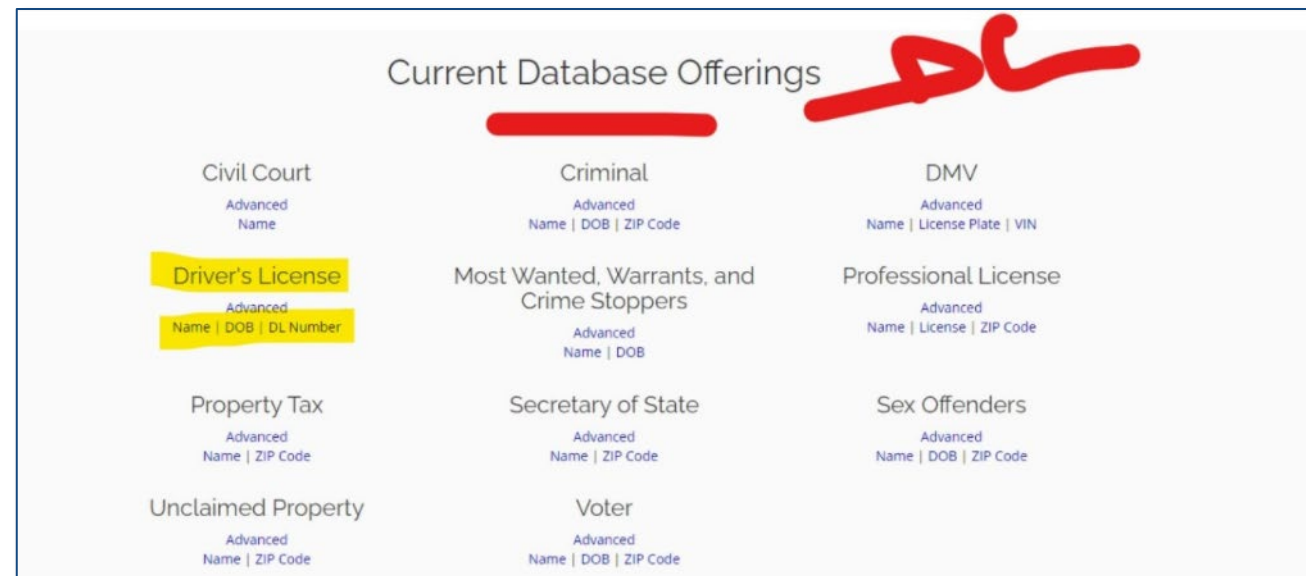
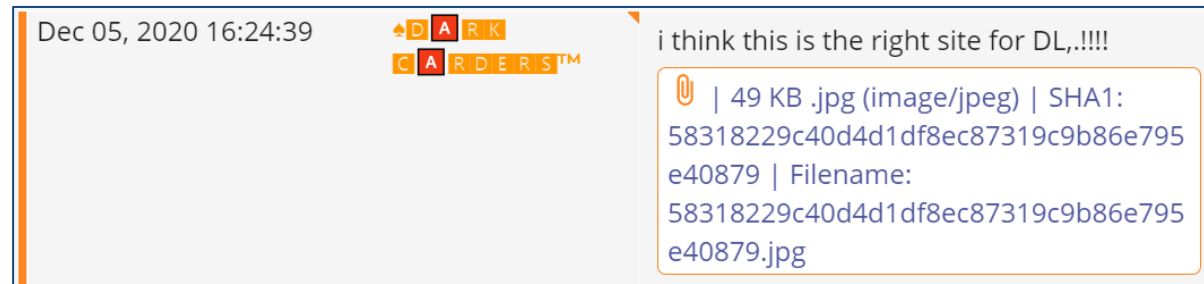
Channel: DARK CARDERS

Channel Type: Supergroup

Contributors: 66

Messages: 12,318

Created on: August 11, 2020



Images courtesy of Flashpoint

References to Unclaimed Property Fraud on DDW Marketplace

Kroll identified an April 23, 2021 World Market listing for a database including Unclaimed Property data from 15 different States. The listing also includes data bases for civil case searches, criminal searches, driver's license numbers, property tax rolls, sex offender registries, and others.

Details:

Marketplace: World Market

Date: April 23, 2021

Product Class: Digital Goods

Quantity Left: 999

Price: USD30

Payment: Escrow

World Market ⓘ
world6zlyzbs6yol36h6wjdzddsnos3b4rakizkm3q75dwkiujyauaid.onion

🛒 [Clone] Ultimate Person Lookup Service HUGE DATABASES

DATE: Apr 23, 2021 23:15 ⓘ

ITEM DESCRIPTION:

PRICE(S):
USD30

Unclaimed Property lookup, AL, CO, CT, FL, GA, HI, IA, MA, NM, NY, ND, OK, TX, WV, WI.


Images courtesy of Flashpoint

References to Unclaimed Property Fraud on Nulled Forum

Kroll identified a May 14, 2020 forum post in which a user “XXXXXXXXXX” offers to sell a script allowing buyers to make monthly revenue via unclaimed property fraud.

The post was uploaded to **Nulled Forum**. Nulled is a forum primarily dedicated to hacking and sharing compromised/leaked data.

Nulled

 **KILLER CLOSER ACADEMY - BUILD \$3,000 PER MONTH INCOM...**

Created On May 14, 2020 By [1m6r0kk3n](#)

Killer Closer Academy (Build a \$3,000 Per Month Income in 30-60 Days)

The Killer Closer Academy is a step by step blueprint for total beginners and veterans that shows how to build a \$1k-\$3k per month business in 30-60 days by using a simple & proven sales script to help recover unclaimed property for people across the united states. You will see exactly how to start and grow this business with zero investment, experience and get sales as soon as tomorrow!

Killer Closer Script (Step by Step How to Convert Strangers Into Closed Deals)

The Killer Closer Script is the virtually the same script that hundreds of successful Surplus Warriors have used to close millions in deals over the last year and a half. In fact this script is so powerful that people have offered to pay us \$1,000+ for it alone! But today you can get access to it for a super discounted price!

Images courtesy of Flashpoint

Fraudulent Identities Available for Sale on DDW Markets

In most instances, malicious actors must purchase or create fraudulent identifications in order to claim property from a State's database. To do so, malicious actors can utilize DDW markets.

Example:

July 19, 2021 Paste Site post on **Deep Paste**, advertising the sale of fake IDs, including Driver's Licenses and Passports.

Deep Paste

📄 Get Passports/Driver'S License

Date: Jul 19, 2021 15:59 UTC ?

Author: Anon

Source: <http://4m6omb3gmrnmwzxi.onion/show.php?md5=ad27851a1deb1f7ab8a80d48656da3ea>

Native ID: [ad27851a1deb1f7ab8a80d48656da3ea](#)

GET PASSPORTS/DRIVER'S LICENSE

Fake ID's for 19.95 Over 50's state drivers license cards and State ID cards available. Includes state driver's license hologram and magnetic strip or bar code on back. 2 business day shipping order (2.95 shipping and handling). The BEST authentic fake ID's on the web. Same quality, high resolution that Department of Motor Vehicles use. Send current .JPG or .GIF of current license with picture and changes in NAME, DOB, LICENSE #, RESTRICTIONS, etc. we produce the best fake ID online we sell UK/EU fake ID, Canadian fake ID,

Images courtesy of Flashpoint



For more information, please contact:

Kroll Cyber Response at:

CL.CyberResponse@kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.

© 2021 Duff & Phelps, LLC. All rights reserved. Kroll is a trade name for Duff & Phelps, LLC and its affiliates.

DRAFT
TLP:AMBER

Questions?

Fraudulent Activity

Using External Data Sources to identify
bad actors and fraudulent activity



Data Sources

- IP Addresses
- National Change of Address (NCOA) data
- Threat profiling services
- Embedded data, such as EXIF metadata on images



IP Addresses

- Who owns the IP address?
- Where is the IP address geographically located?
- Known TOR (The Onion Router) IP Address?
- Blacklist information

```
ip: "24.8.101.73",
is_eu: false,
city: "Boulder",
region: "Colorado",
region_code: "CO",
country_name: "United States",
country_code: "US",
continent_name: "North America",
continent_code: "NA",
latitude: 40.0373,
longitude: -105.279,
postal: "80304",
calling_code: "1",
asn: {
  asn: "AS7922",
  name: "Comcast Cable Communications, LLC",
  domain: "comcast.com",
  route: "24.0.0.0/12",
  type: "isp"
}
languages: {
  name: "English",
  native: "English"
}
currency: {
  name: "US Dollar",
  code: "USD",
  symbol: "$",
  native: "$",
  plural: "US dollars"
}
time_zone: {
  name: "America/Denver",
  abbr: "MDT",
  offset: "-0600",
  is_dst: true,
  current_time: "2021-09-13T14:47:14.358798-06:00"
}
threat: {
  is_tor: false,
  is_proxy: false,
  is_anonymous: false,
  is_known_attacker: false,
  is_known_abuser: false,
  is_threat: false,
  is_bogon: false
}
```



NCOA data

- Determine deliverable address
- Identify address risk codes
- Find recent moves / address changes

Code	Short Description	Long Description
AS01	Valid Address	The address is valid and deliverable according to official postal agencies.
AS03	Non USPS Address Match	US Only. This US address is not serviced by the USPS but does exist and may receive mail through third party carriers like UPS.
AS10	CMRA Address	US Only. The address is a Commercial Mail Receiving Agency (CMRA) like a Mailboxes Etc. These addresses include a Private Mail Box (PMB or #) number.
AS12	Moved to New Address	The record moved to a new address.
AS16	Vacant Address	US Only. The address has been unoccupied for more than 90 days.



Threat Profiling

- Aggregated data from other internet transactions and activity
- Track behavior over time and across
- Leverage other internet history

REASONS & SCORES

Name Per Phone Global GE 2 (0)
OS Anomaly (0)
VPN_Detection (-15)
TMX Summary Reason: GEO_Spoofing (-5)
Time Zone/True Geo Mismatch (-15)
User Agent Mismatch: Windows - Linux (-3)
3 or more identities per Phone - global (-5)



Threat Profiling

Description	Count
ThreatMetrix High Risk Level	31,054
True IP Geo not in US	25,750
More than one name per SSN	18,562
Business claim with generic email domain	11,699
True IP in Global Reject List	9,800
10 or more identities per Smart ID - global	5,233
True/Input/Proxy IP Org Type Server Farm	3,605
Email Seen Less Than 1 Week GBL	3,442
US address, Foreign Claim Creation	3,103
True IP in Global Blacklist	2,076
Suspect Email Domain	1,457
Likely Finder Claim	1,113
Phone in Global Blacklist	730
High Risk Country	73
IP Address listed as potentially fraudulent	66
High Risk Country DNS IP	45
Name tagged confirmed fraud	37
Name listed as potentially fraudulent	36
TOR_Detection	24



Threat Profiling

- Selected results

	Count	Percentage
Profiled Claims	1,140,219	100.00%
Foreign Claim, US Address	3,195	0.28%
High Risk Country	74	0.01%
TOR IP Address	28	0.00%
Medium Risk Country	2,144	0.19%
Fraud Or Blocklist	4,336	0.38%
High Score	29,981	2.63%



Embedded Data

- Exchangeable image file format (EXIF)
- Often contains image device, system location, software

#1 - claim_██████████_20210913160226129_0.jpeg - 61 data rows [Show Full EXIF Data](#)

File Info		Date & Time		Location	
kaps_filename:	claim_██████████_20210913160226129_0.jpeg	Sub-Sec Time Digitized:	754	Long:	-70.85003611111111
Lens Model:	iPad Air 2 back camera 3.3mm f/2.4	Date/Time Original:	2021:09:13 15:49:15	Lat:	42.09386944444444
Make:	Apple	kaps_created:	2021-09-13 16:02:29		
Software:	14.7.1	Sub-Sec Time Original:	754		
Model:	iPad Air 2	Date/Time Digitized:	2021:09:13 15:49:15		
		Date/Time:	2021:09:13 15:49:15		
		Run Time:	[104 values]		

#1 - claim_██████████_20210914011409780_3.jpg - 57 data rows

File Info	
kaps_filename:	claim_██████████_20210914011409780_3.jpg
Make:	Apple
Software:	Adobe Photoshop 21.0 (Macintosh)
Model:	iPhone 8 Plus

#1 - claim_██████████_20210907182132279_0.jpg - 59 data rows

File Info	
kaps_filename:	claim_██████████_20210907182132279_0.jpg
Lens Model:	iPhone 8 Plus back dual camera 3.99mm f/1.8
Make:	Apple
Software:	GIMP 2.10.24
Model:	iPhone 8 Plus



Questions?

UNCLAIMED PROPERTY LAW

Why have a specific law...???

**To manage the unique needs & requirements of protecting the
Unclaimed Properties We're responsible for.**



What needs protection

The ultimately INFINITE number of Claims & Systems utilized to protect them.

The ability to ensure properties are legally maintained & properly preserved until the Owner or Heir may make a legal claim.



HOW DO WE PROTECT UNCLAIMED PROPERTY

Utilization of technology to ensure integrity of the Claim.

Human brain power & technology yet imagined to understand & identify efforts of Those who would exploit technology in an effort to circumvent safeguards protecting Property/Owners/Heirs.

Enacting Legislation to support Treasuries in the protection, detection, & prevention of loss.



Questions?

Webinar Ideas?
Contact Jeff Chetkauskas
jeff.chetkauskas@maine.gov

Thank You



NATIONAL ASSOCIATION OF
STATE TREASURERS