



DARKTOWER

Crypto Scams and Protecting our Clients

BEC was the #1 fraud – from 2015 to 2021

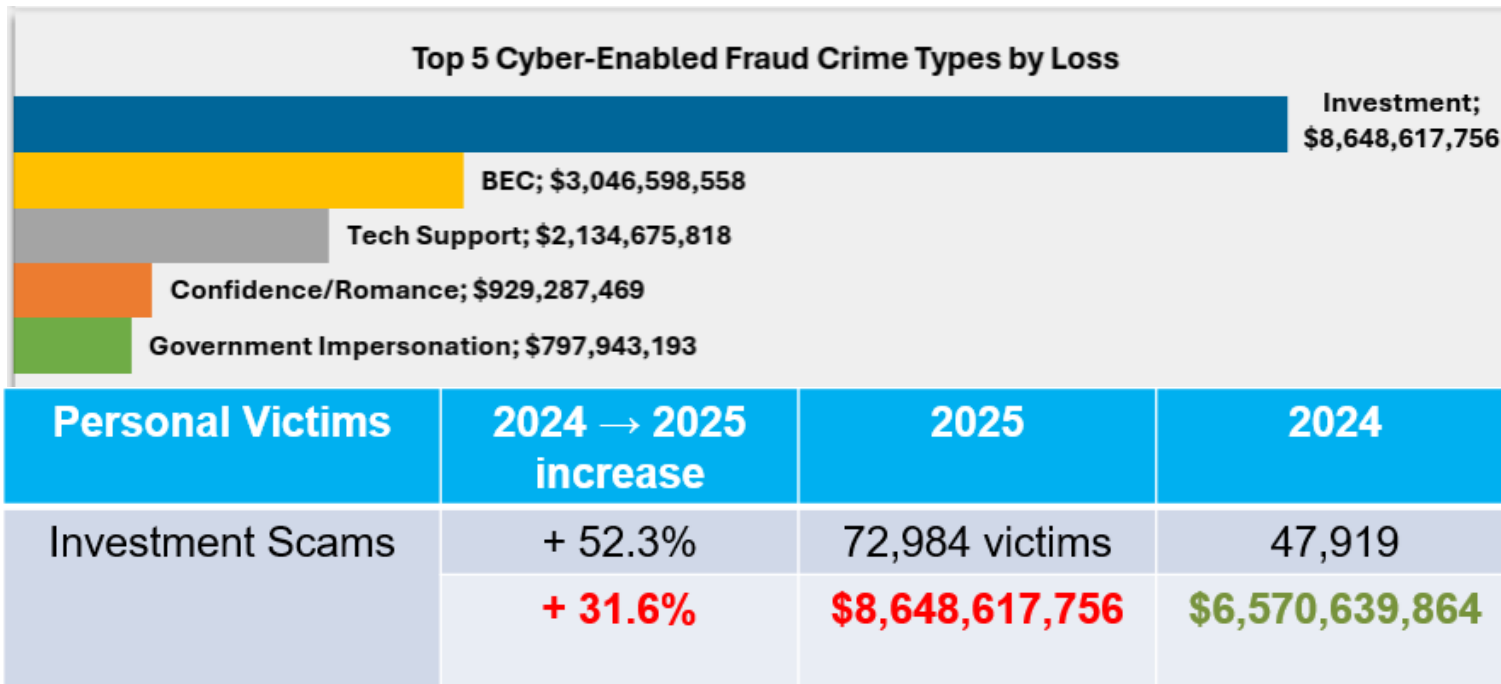
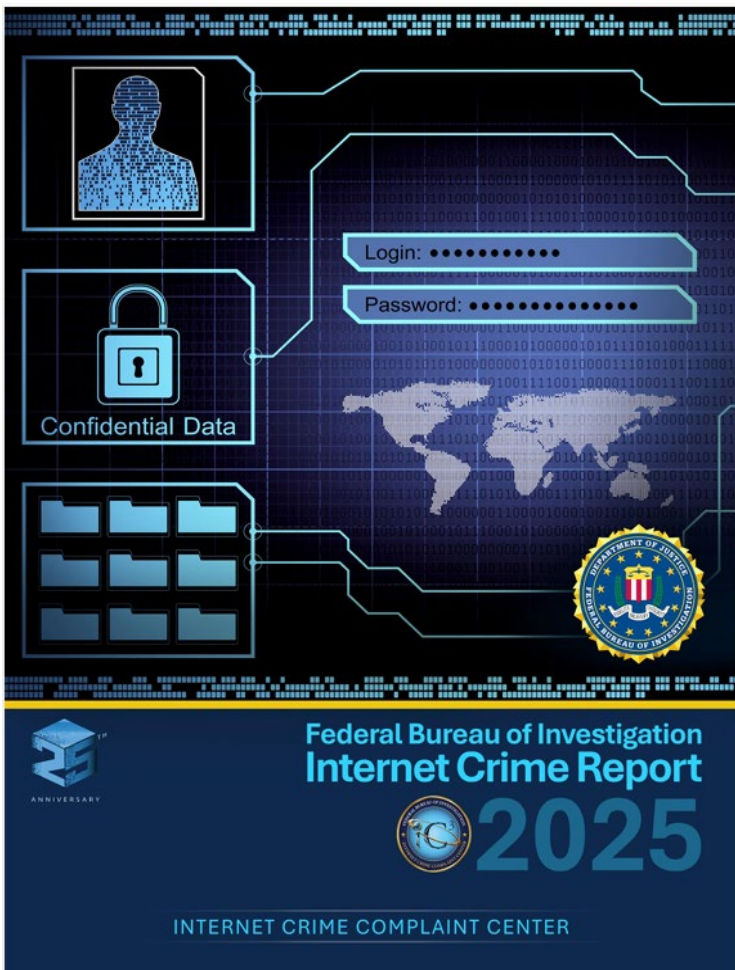
From IC3.gov annual reports

- ... 2015 – #17 by number of complaints - #1 by losses: \$246,226,016
- ... 2016 - #15 by number of complaints - #1 by losses: \$360,513,961
- ... 2017 - #10 by number of complains - #1 by losses: \$676,151,185
- ... 2018 - #6 by number of complaints - #1 by losses: \$1,297,803,489
- ... 2019 - #6 by number of complaints - #1 by losses: \$1,776,549,688
- ... 2020 – #10 by number of complaints - #1 by losses: \$1,866,642,107
- ... 2021 – #9 by number of complaints - #1 by losses: \$2,395,953,296
- ... 2022 – #9 by number of complaints - **#2 by losses: \$2,742,354,049**
- ... 2023 - #7 by number of complaints - **#2 by losses: \$2,946,830,270**
- ... 2024 - #7 by number of complaints - **#2 by losses: \$2,770,151,146**
- ... 2025 - #9 by number of complaints - **#2 by losses: \$3,046,598,558**



FBI IC3.gov Annual Report

It's all about Crypto Investment Scams



Age	60+	50-59	40-49
Investment Scams	16,926	12,773	13,737
	\$3,519,296,354	\$1,748,651,287	\$1,152,243,858



Almost Half of all Dollars **STOLEN** were from our Elders

49.1% of money stolen in **Investment Scams** came from those over age 60! **\$3.5 BILLION!**

59.4% of money stolen in **Tech Support Scams** came from those over age 60!

59.6% of money stolen in **Gov Impersonation** came from those over age 60!

48.5% of money stolen via **Extortion** came from those over age 60!

Romance Scams particularly target older adults. **46.9% of victims** were over age 60, while **67.9% of money stolen** came from those over age 60!

Age		% over 60	60+	Under 60
Investment Scams		27.6%	16,926	44,509
		49.1%	\$3,519,296,354	\$3,645,961,393
	Tech Support Scams	52.9%	21,333	19,008
		59.4%	\$1,040,730,043	\$712,129,613
	Government Impersonation	29.1%	8,628	21,039
		59.6%	\$413,206,251	\$280,484,184
Confidence/Romance		46.9%	10,188	11,535
		67.9%	\$584,032,745	\$276,646,227
Employment		13.3%	2,853	18,610
		25.0%	\$78,712,899	\$235,862,234
Extortion		10.8%	9,111	75,032
		48.5%	\$54,309,050	\$57,771,775

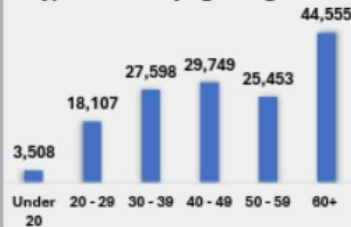
For the first time, Crypto was the #1 Payment Vehicle for Cybercrime - \$11.3 Billion!

Complaints Involving Cryptocurrency - 2025

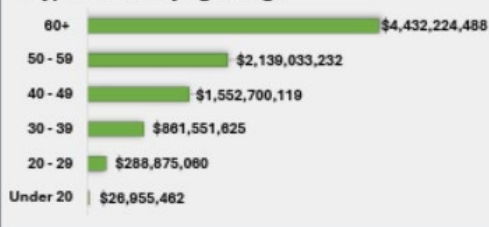
Highlights

181,565 Complaints
 ↑ 21% FROM 2024
 \$11.366 Billion in Losses
 ↑ 22% FROM 2024
 18,589 Complainants Lost >\$100K
 \$62,604 Average Loss

Crypto Counts by Age Range



Crypto Losses by Age Range



IC3 Complaints with Cryptocurrency Nexus



Crypto is 54.4% of the total money reported stolen to IC3.gov in 2025!

Investment Scams COULD NOT EXIST without Crypto as a payment rail.

Crypto ATMs are one of the primary cash out models used by the Call Center Scams.

Recovery Scams are follow-ups primarily to Investment Scams.

Cryptocurrency Investment

61,559 Complaints; \$7.228 billion

 48% Increase in Complaints from 2024
 25% Increase in Losses from 2024

 New Scam Center Strike Force Battles Southeast Asian Crypto Investment Fraud Targeting Americans | United States Department of Justice

Crypto Investment Fraud Reported by Age Group

Age Group	Count	Losses
Under 20	629	\$12,582,997
20 - 29	4,627	\$117,353,587
30 - 39	8,576	\$412,626,617
40 - 49	10,750	\$924,623,370
50 - 59	9,856	\$1,383,263,248
60+	13,685	\$2,763,921,910

Cryptocurrency ATMs/Kiosks

13,460 Complaints; \$389 million in Losses

 23% Increase in Complaints from 2024
 58% Increase in Losses from 2024

 The FBI Warns of Fraudulent Schemes Leveraging Cryptocurrency ATMs and QR Codes to Facilitate Payment

Crypto ATM/Kiosk Use Reported by Age Group

Age Group	Count	Losses
Under 20	58	\$124,013
20 - 29	825	\$6,474,240
30 - 39	1,275	\$10,936,943
40 - 49	1,472	\$20,826,227
50 - 59	1,524	\$44,584,724
60+	6,188	\$257,466,130

Recovery Scams

10,516 Complaints; \$1.4 billion in Losses

 Increase in complaints reporting impersonation of government officials and recovery firms.

 Fictitious Law Firms Targeting Cryptocurrency Scam Victims Combine Multiple Exploitation Tactics While Offering to Recover Funds

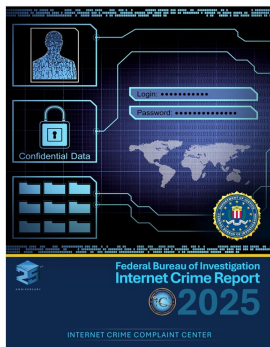
 FBI Warns of Scammers Impersonating the IC3

Recovery Scams Reported by Age Group

Age Group	Count	Losses*
Under 20	106	\$3,825,212
20 - 29	841	\$22,498,411
30 - 39	1,511	\$76,183,433
40 - 49	1,977	\$194,670,794
50 - 59	1,706	\$298,233,813
60+	2,529	\$540,505,980

*Losses may also include losses experienced from previous scams which prompted the contact with the recovery company.

Investment Scams were 7.2% of complaints and 41.4% of money stolen. \$8.6 BILLION DOLLARS



2025 Crime Types

By Complaint Count

Crime Type	Complaints	Crime Type	Complaints
Phishing/Spoofing	191,561	Credit Card/Check Fraud	18,774
Extortion	89,129	Real Estate	12,368
Investment	72,984	Advanced Fee	7,762
Personal Data Breach	67,456	Lottery/Sweepstakes/Inheritance	5,623
Non-Payment/Non-Delivery	56,478	Threats of Violence	4,826
Tech/Customer Support	47,794	Data Breach	3,963
Government Impersonation	32,424	Ransomware	3,611
Identity Theft	31,675	IPR/Copyright and Counterfeit	2,386
Business Email Compromise	24,768	Overpayment	2,194
Employment	24,688	SIM Swap	971
Confidence/Romance	23,159	Malware	893
Harassment/Stalking	21,557	Botnet	715
Other	20,031	Charity	662

2025 Crime Types, *continued*

By Complaint Loss

Crime Type	Loss	Crime Type	Loss
Investment	\$8,648,617,756	Lottery/Sweepstakes/Inheritance	\$194,147,851
Business Email Compromise	\$3,046,598,558	Identity Theft	\$185,832,657
Tech/Customer Support	\$2,134,675,818	Advanced Fee	\$155,910,852
Personal Data Breach	\$1,314,923,988	Extortion	\$122,499,133
Confidence/Romance	\$929,287,469	Ransomware	\$32,320,105
Government Impersonation	\$797,943,193	Harassment/Stalking	\$27,707,167
Other	\$512,146,819	IPR/Copyright and Counterfeit	\$26,667,006
Non-Payment/Non-Delivery	\$503,373,587	Overpayment	\$22,898,075
Data Breach	\$435,240,992	Malware	\$19,370,572
Employment	\$362,934,762	SIM Swap	\$17,366,758
Credit Card/Check Fraud	\$282,670,235	Botnet	\$13,859,049
Real Estate	\$275,110,419	Threats of Violence	\$9,509,532
Phishing/Spoofing	\$215,843,126	Charity	\$7,907,609

2025 FTC Consumer Sentinel agrees:

Investment Scams are 4.75% of complaints
and 49.8% of dollars stolen. \$7.9 BILLION DOLLARS

Top 10 Fraud Categories

Rank	Category	# of Reports	% Reporting \$ Loss	Total \$ Loss	Median \$ Loss
1	Imposter Scams	1,005,012	20%	\$3,511.5M	\$700
2	Online Shopping and Negative Reviews	419,098	78%	\$446.4M	\$117
3	Internet Services	193,911	19%	\$209.3M	\$300
4	Business and Job Opportunities	157,841	32%	\$906.8M	\$2,008
5	Investment Related	143,918	78%	\$7,932.9M	\$10,400
6	Telephone and Mobile Services	96,844	44%	\$65.5M	\$280
7	Health Care	82,868	55%	\$77.7M	\$275
8	Prizes, Sweepstakes and Lotteries	70,901	25%	\$303.6M	\$780
9	Travel, Vacations and Timeshare Plans	64,342	63%	\$297.0M	\$700
10	Advance Payments for Credit Services	51,327	37%	\$100.8M	\$768

Source: <https://public.tableau.com/app/profile/federal.trade.commission/viz/FraudReports/FraudFacts>



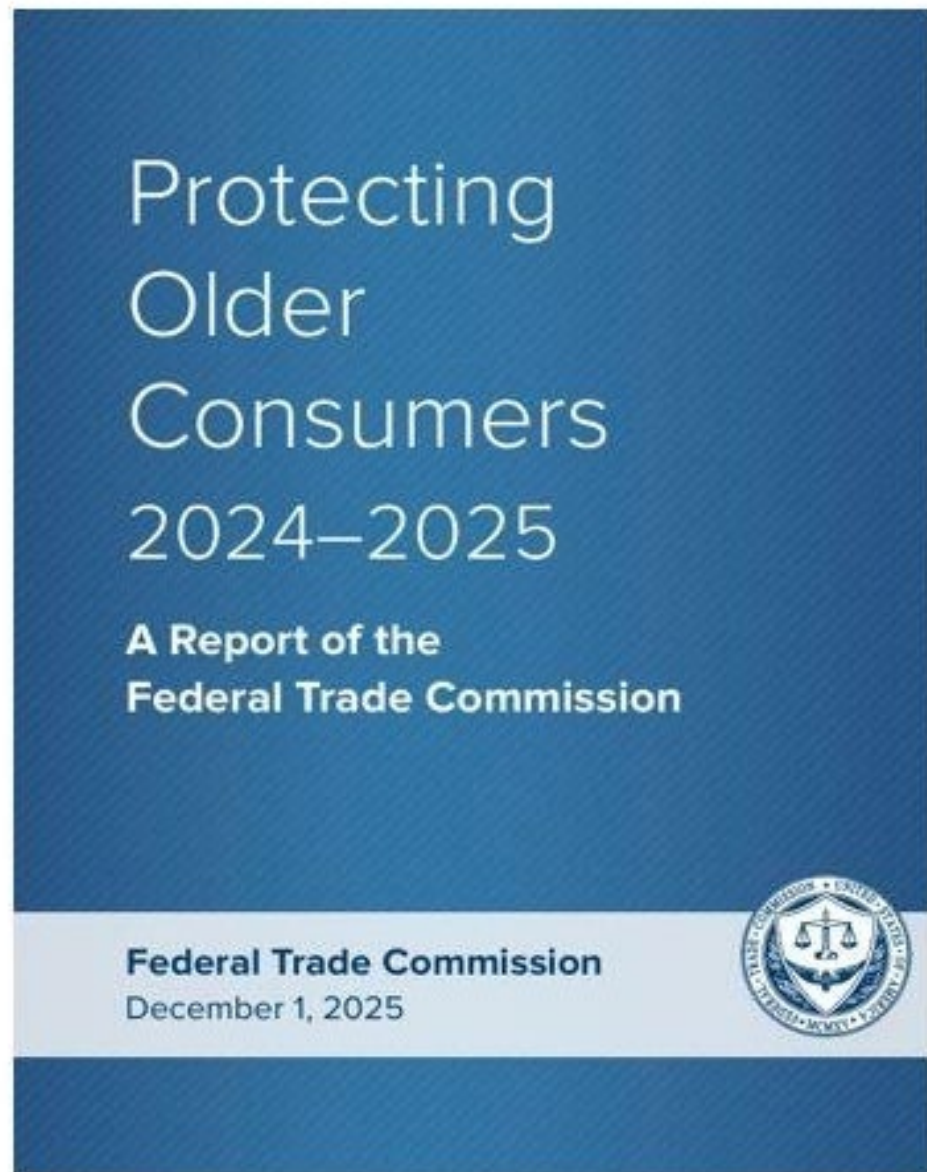
Belief:

Only 2% of losses under \$1K
and **6.7%** of losses over \$1K
are reported to Consumer Sentinel
(pg. 28)

\$195.9 Billion

\$81.5 Billion

likely stolen from our elders





What is a Crypto Investment Scam?

“Making a false or fraudulent statement to entice an investor”

MANIPULATIVE AND DECEPTIVE DEVICES AND CONTRIVANCES (§§ 240.9j-1 - 240.10c-1a)

§ 240.9j-1 Prohibition against fraud, manipulation, or deception in connection with security-based swaps.

§§ 240.10a-1--240.10a-2 [Reserved]

§ 240.10b-1 Prohibition of use of manipulative or deceptive devices or contrivances with respect to certain securities exempted from registration.

§ 240.10b-2 [Reserved]

§ 240.10b-3 Employment of manipulative and deceptive devices by brokers or dealers.

§ 240.10b-4 [Reserved]

§ 240.10b-5 Employment of manipulative and deceptive devices

§ 240.10b5-1 Trading “on the basis of” material nonpublic information in insider trading cases.

§ 240.10b5-2 Duties of trust or confidence in misappropriation insider trading cases.

§§ 240.10b-6--240.10b-8 [Reserved]

§ 240.10b-9 Prohibited representations in connection with certain offerings.

§ 240.10b-10 Confirmation of transactions.

§ 240.10b-13 [Reserved]

§ 240.10b-16 Disclosure of credit terms in margin transactions.

§ 240.10b-17 Untimely announcements of record dates.

§ 240.10b-18 Purchases of certain equity securities by the issuer and others.

§ 240.10b-21 Deception in connection with a seller's ability or intent to deliver securities on the date delivery is due.

A “False or Fraudulent Claim” enticing an Investment

evergreenmining.org



EVERGREEN
MINING INVESTMENT

HOME ABOUT ANTI-MONEY LAUNDERING FAQS CONTACT

Select Language

Register Login

REAL ESTATE PLAN

12% Daily

For 8 Days

OIL AND GAS PLAN

3% Daily

For 26 Days

VIP PLAN

2% Daily

For 30 Days

Min : \$10,000
Max : \$100,000
% Referral Commission

DEPOSIT

blackmor-trader.top

TRADING PLATFORM FOR Crypto Investors

LOGIN REGISTRATION

Investment PLANS

British company blackmor-trader.top provides profitable cryptocurrency trading. Customers can choose different investment plans for rewarding asset management. Our platform allows performing a high-quality analysis of the currency market and makes investments well-payable for any selected plan.

	SILVER	GOLD	VIP
	4.50% For 24 Hours	60% Daily 2 Days	140% After 3 Days
INVEST NOW	INVEST NOW	INVEST NOW	INVEST NOW
Deposit min-\$25	\$25-\$25000	\$50-\$25000	\$100-\$25,000
Payouts Min \$5	Returned 108%	Returned 120%	Returned 140%

Investment Plans

38 % Duration : 24hrs Minimum : \$600 - Maximum : \$1499 Reinvestment : Yes Invest Now	75 % Duration : 2.5 Days Minimum : \$1500 - Maximum : \$2999 Reinvestment : Yes Invest Now	100 % Duration : 3.5 Days Minimum : \$3000 - Maximum : Unlimited Reinvestment : Yes Invest Now
--	--	--

Amazing ROI on
Plan.

Guarenteed Profits On All Plans

Trusted Accross 120+ Countries

join

Plan work: All Days of week

Invest

Invest

Invest



We've recruited students from 13 Universities to help us

Participating Universities

2026 Current Stats

- **195** Students registered
 - **98** submitting data, rest completing training
- **18,088** crypto investment scam sites submitted
- **33,024** wallet addresses reported

Stats as of 28SEP2026

So far, we have **98** students participating across **20** university teams. These students have reported **18088** crypto investment scam sites containing **33024** unique fraudulent wallets.

Live stats taken from leaderboard



CHAMPLAIN
COLLEGE



THE UNIVERSITY OF
ALABAMA AT BIRMINGHAM



ST. CLOUD STATE
UNIVERSITY



URLScan.io – we’ve shared 40,000+ Crypto Investment Scam websites

Click “Search” and look for “**task.tags:cryptoscam**”



Search for domains, IPs, filenames, hashes, ASNs

task.tags:cryptoscam

Search

Pro Search

X

Help

Search results (100 / 10000+, sorted by date, took 342ms)

Showing All Hits

Details: Hidden

URL		Age		Size		IPs		
 bulktrade.ai/	Public	5 hours		1 MB	64	1	1	
 onehour.homes/	Public	6 hours		51 KB	13	1	1	
 morecash.homes/	Public	6 hours		43 KB	11	1	1	
 winvest.com/	Public	7 hours		7 MB	115	3	2	
 bulktrade.ai/	Public	7 hours		1 MB	65	1	1	
 bulktrade.ai/	Public	7 hours		1 MB	65	1	1	
 batonexus.com/	Public	20 hours		4 MB	157	11	4	
 animalcsi.com/	Public	20 hours		3 MB	86	3	3	
 animalcsi.com/	Public	20 hours		2 MB	86	3	2	
 558t.com/index/index/home	Malicious Public	22 hours		701 KB	38	6	2	
 meizi.store/index/index/home	Malicious Public	22 hours		701 KB	38	5	2	
 11ve.com/index/index/home	Malicious Public	22 hours		701 KB	38	6	2	

Some of the 340 sites that look exactly like this ...





IQExpress.pro gave me 9 Different Cryptocurrency choices!



EliteFinex and WealthGainCenter were non-functional, although they let me register and sent an email, they wouldn't let me deposit.

HOME ABOUT FAQ GET STARTED AFFILIATES SUPPORT PAYMENTS ACCOUNT LOGOUT

MAKE A **DEPOSIT**

ACCOUNT DEPOSIT EARNINGS HISTORY WITHDRAW REFERRALS SETTINGS

10%
DAILY FOREVER
MINIMUM DEPOSIT: \$20
MAXIMUM DEPOSIT: \$1,000
INSTANT WITHDRAWALS
SELECT

12%
DAILY FOREVER
MINIMUM DEPOSIT: \$1,001
MAXIMUM DEPOSIT: \$5,000
INSTANT WITHDRAWALS
SELECT

15%
DAILY FOREVER
MINIMUM DEPOSIT: \$5,001
MAXIMUM DEPOSIT: \$10,000
INSTANT WITHDRAWALS
SELECT

20%
DAILY FOREVER
MINIMUM DEPOSIT: \$10,001
MAXIMUM DEPOSIT: \$100,000
INSTANT WITHDRAWALS
SELECT

Amount to Spend (\$):

☐ Bitcoin

☐ USDT TRC20

☐ Bitcoin

☐ Litecoin

☐ Ethereum

☐ Dogecoin

☐ Tron

☐ BNB

☐ XRP

SPEND

The deposit addresses had been used 171 times, receiving \$36,534

crypto	address	amount	deposits	first_used	last_used
USDT	TEsJc7Tg7fnmH3T3MRtY1ei57hWLwbDSyF	\$ 13,646.24	63	21-Dec-21	4-Jun-24
BTC	bc1qwhwf4f4pqz56u8vc4f9mu354hy0vzwq5l89m6w	\$ 17,120.00	80	17-Nov-21	1-Aug-24
BTC	1FcGmJFiNUGjHmNu7qbwwRsF66KWE1Jaeu	\$ 2,165.36	6	20-Jun-24	1-Aug-24
LiteCoin	LSx8YGjUbL7SQP3i4GMipcka8qx5yHhFp5	\$ 78.75	1	17-Nov-21	
Ethereum	0x85D2824A86FC23479eF420ABec0c30BaD4dEA2c6	\$ 1,379.99	13	25-Jan-22	9-Aug-24
DogeCoin	DREeBN2G2fCH8UePmDahTvLyDCArD2PqS9	\$ 1,894.00	7	18-Nov-21	29-Aug-23
BNB	bnb1hr85z0u68fparcr5wj6mzms3th726schhydml	\$ 250.09	1		
XRP	rLceJbd5kYXcvCt63CY8ZAX3QxbXuLZhXd	private			
		\$ 36,534.43	171.00	17-Nov-21	9-Aug-24

The earliest deposit was November 17, 2021

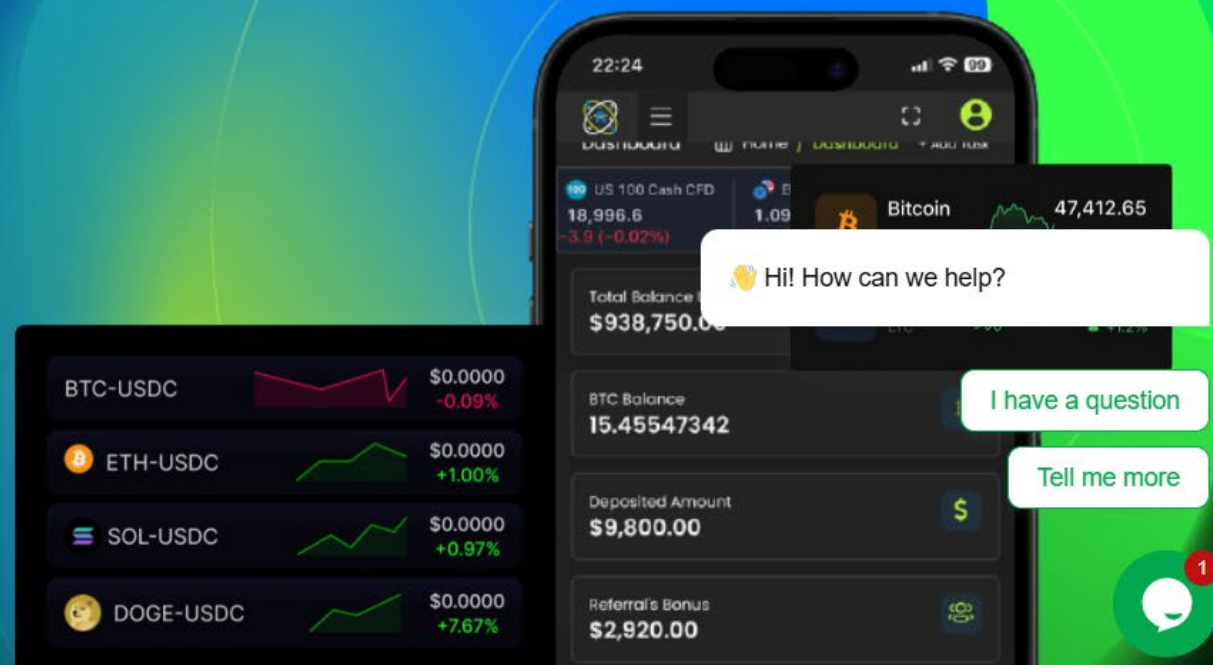
The most recent was August 9, 2024

But the addresses were originally used at “EasyBit247.ltd”

[HOME](#)[ABOUT US](#)[TRADING ASSETS](#)[FAQ](#)[CUSTOMER REVIEWS](#)[DOCUMENTS](#) [CONTACT](#)[Login](#) [TRADING PLATFORMS](#)

TRADE WITH SAPPHIRE UNION MARKET

Covesting allows you to automatically copy top performing traders and achieve the returns

[Start Trading](#) 

The more you invest, the higher the return

from 9% ... to 23% WEEKLY

Silver	Gold
AMOUNT: \$9000 0.14465573 BTC ✓ Weekly Interest: 09% ✓ Investment Sum: \$9000 ✓ Trading/Withdrawal Commission: 10% ✓ Referral Bonus: 5%	AMOUNT: \$19000 0.30538431 BTC ✓ Weekly Interest: 15% ✓ Investment Sum: \$19000 ✓ Trading/Withdrawal Commission: 10% ✓ Referral Bonus: 5%
Diamond	Elite
AMOUNT: \$50000 0.80364292 BTC ✓ Weekly Interest: 18% ✓ Investment Sum: \$50000 ✓ Trading/Withdrawal Commission: 10% ✓ Referral Bonus: 5%	AMOUNT: \$100000 1.60728585 BTC ✓ Weekly Interest: 23% ✓ Investment Sum: \$100000 ✓ Trading/Withdrawal Commission: 10% ✓ Referral Bonus: 5%

Choose your Crypto type

Our team harvests these addresses and reports them

1	ETHEREUM	ETH	0xAb540Ed2C02eb646C55E24bEF0fF88854EA30cB7	COPY	 click to view
2	BITCOIN	BTC	bclq9yv6lvq3v0qmmvdyxysvrgmmkvs9qtcca6njen	COPY	 click to view
3	USDT	TRX network	TWxDQehZEURXEKATyNqXUdBkGhfSnWwDNZ	COPY	 click to view
4	USDC	USDC	0x3b0B1b47101ABb8eFd0ec1f983e57Ef4d9638e75	COPY	 click to view

\$19,610 total volume

\$4,706

\$2,988

\$78,432

“My” Path to Disruption

1

Identify & Document

Find Scam Websites,
collected domain, registrar,
IP, netblock, ASN.

Harvest crypto deposit
addresses from each site.

2

Analyze & Connect

Use passive DNS, URLScan,
and blockchain analysis to
link sites, wallets, and
infrastructure across
networks.

3

Report & Disrupt

Submit findings to partners
who terminate hosting, label
wallets, block addresses, and
make criminal referrals

Reporting & Partnerships

Industry Partners



Coinbase

Crypto Exchange Partner

Flagged wallet addresses are reported to Coinbase's platform within five minutes of student submission. Any user attempting to send funds to a flagged address is immediately blocked and alerted that they may be involved in a scam



PayPal

Financial Crime Intelligence (FCII)

Scam site and wallet intelligence shared with PayPal's FCII team to support SAR filings and disrupt fiat on/off ramps tied to crypto scams.



Crypto Analysis Partner



Chainalysis

Crypto Analysis Partner

Law Enforcement



U.S. Secret Service

Global Investigative Operations Center (GIOC)

Weekly site reports for investigation and "letterhead" domain takedowns.



FBI

Data shared to IC3.gov and MCCU1 via Birmingham FBI

Weekly site reports distributed to 4 field offices, used in support of their investigations and active cases.



Milestone #1: 40,000 websites labeled

(40,158 to be exact). In partnership with urlscan.io, we tag our reported websites as [hashtag#CryptoScam](#), allowing them to be publicly searched on URLScan using the term "Task.tags:cryptoscam"

The project which is now Scambusters was originally a classroom project in my UAB Course, "Investigating Online Crime" and was later continued in the UAB Computer Forensics Research Lab through sponsorship from [Intelligence for Good](#). That website history breaks down like this:

7,725 domains in 2023

7,655 domains in 2024

9,746 domains in 2025

15,031 domains so far in 2026!

Of those 40,000+ domains, 10,248 are currently live and believed to be still hosting Crypto Investment Scam content:

10,248 are live

3,280 are parked

2,318 are seized, disabled, expired or otherwise non-functional

24,047 are DEAD. NX_Domain or failure to resolve

Milestone #2: 25,000 crypto addresses identified

13,372 of the USDT, ETH, and BTC addresses were found to have on-chain transaction history.

806 received deposits in the past 7 days (with total transaction history of **\$43,190,678**).

339 of these are mapped to a known currently live website.

2439 received deposits in the past 30 days (with total transaction history of **\$96,306,382**)

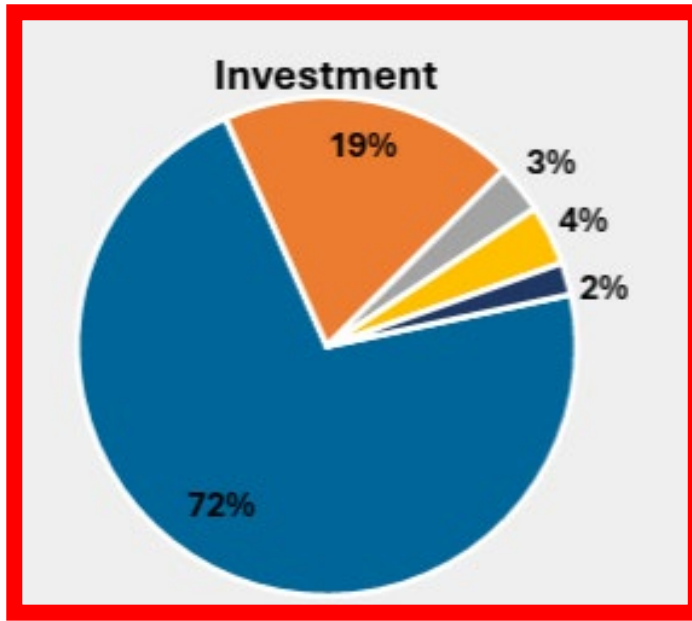
982 of these are mapped to a known currently live website.



DARKTOWER

But what is
YOUR
path to disruption?

Investment Fraud **DEPENDS ON CRYPTO** But it isn't **ALL Crypto!**



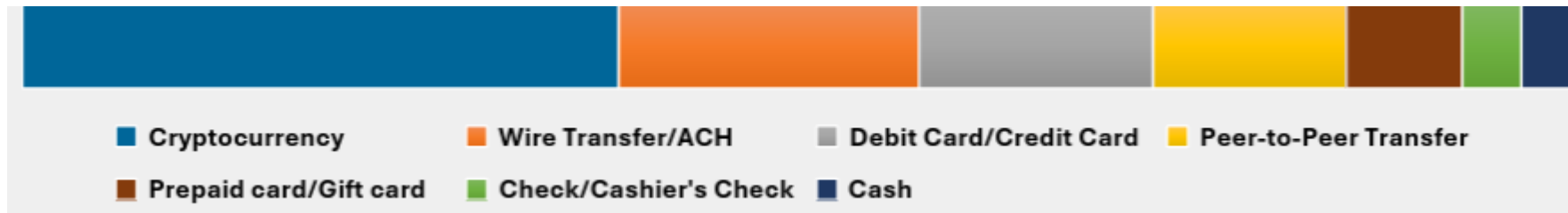
19% of the Investment Scam losses reported to the FBI were via **Wire Transfer**.

That's \$1.6 Billion!

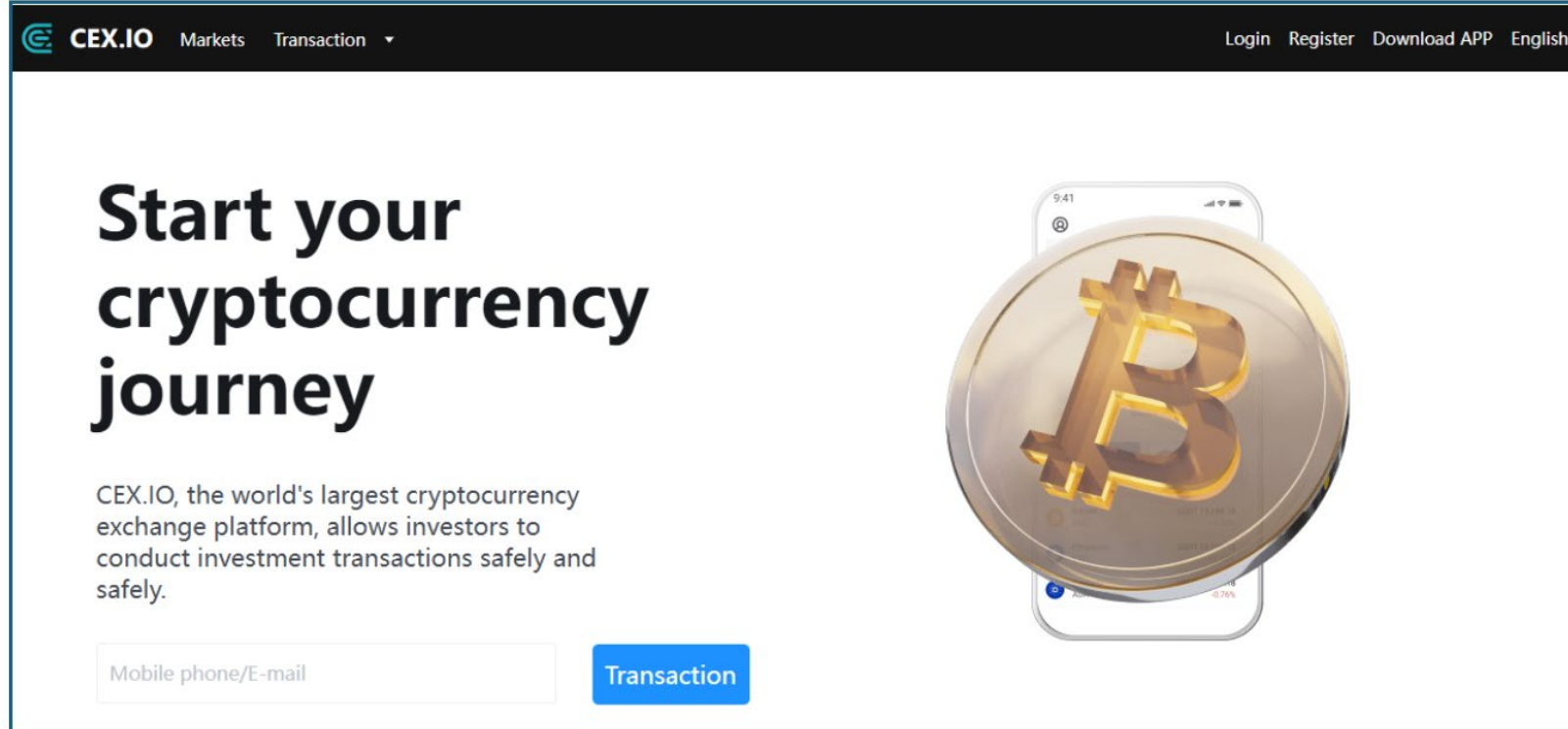
\$258 Million via Credit/Debit Card

\$344 Million in [CashApp/Zelle/Venmo/etc.]

\$172 Million in Cash



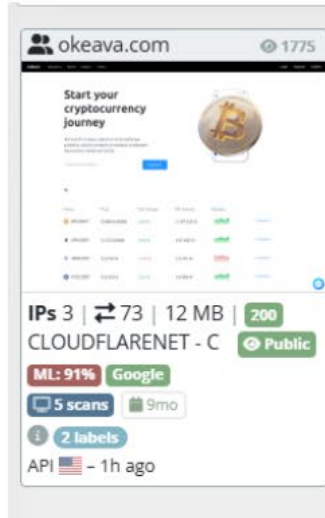
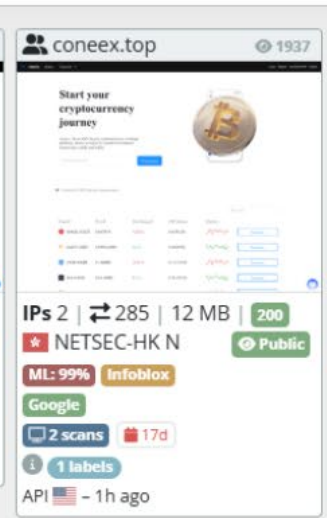
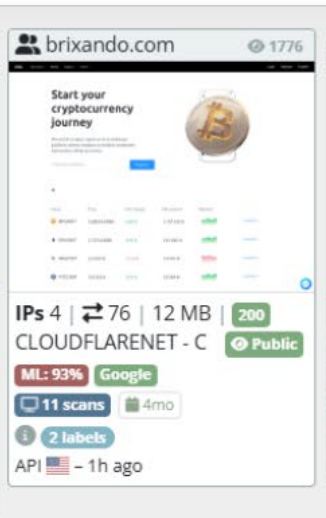
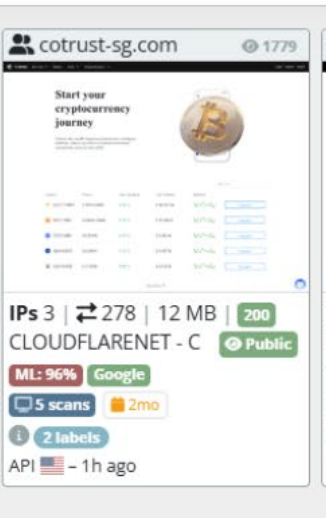
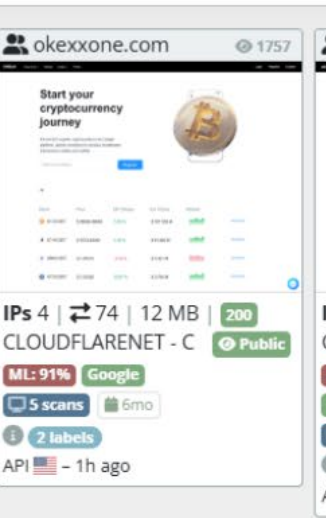
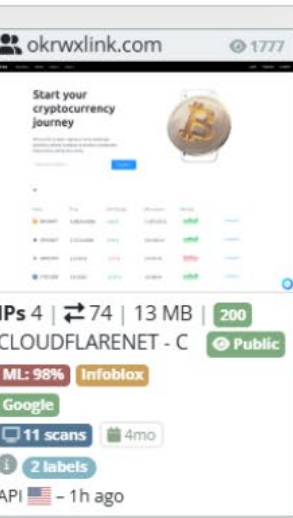
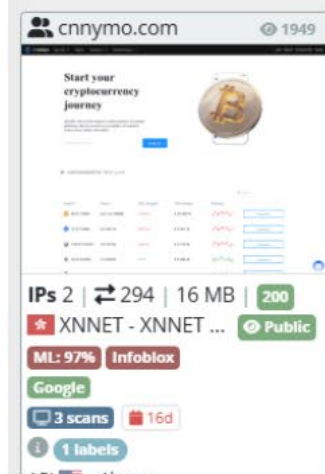
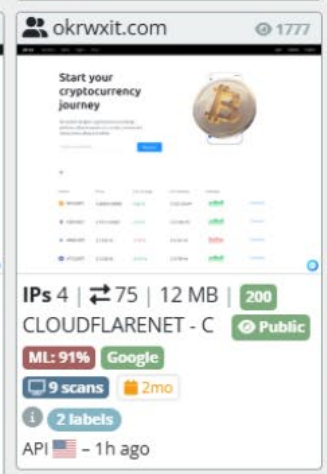
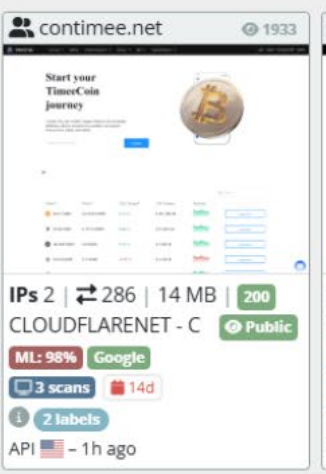
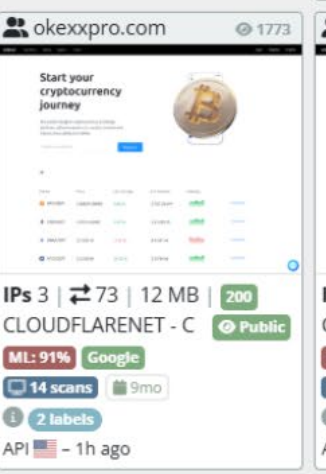
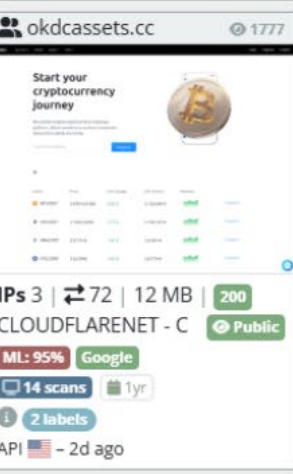
The Story of Mr. D of Madison, Alabama



Crypto	Address	# of deposits	First Date	Last Date	Amount
BTC	3JiEGxPAYkiL78eWLUayjPFqEmGsLJybsH	1	18FEB2026	18FEB2026	\$4930
USDT	0x2E0efD2D6608F0d07Fc5fE2A1a5e10EEe22d924	12	08DEC2025	19FEB2026	\$134,360
USDC	0x2E0efD2D6608F0d07Fc5fE2A1a5e10EEe22d924	6	06FEB2026	19FEB2026	\$86,954
ETH	0x2E0efD2D6608F0d07Fc5fE2A1a5e10EEe22d924	18	09DEC2025	20FEB2026	\$48,044
	TOTAL				\$274,288

At least 436 domains have all claimed to be “CEX.IO”

My team gathered crypto addresses from 64 of them.

 okeava.com 1775 Start your cryptocurrency journey IPs 3 73 12 MB 200 CLOUDFLARENET - C Public ML: 91% Google 5 scans 9mo 2 labels API - 1h ago	 coneex.top 1937 Start your cryptocurrency journey IPs 2 285 12 MB 200 NETSEC-HK N Public ML: 99% Infoblox Google 2 scans 17d 1 labels API - 1h ago	 brixando.com 1776 Start your cryptocurrency journey IPs 4 76 12 MB 200 CLOUDFLARENET - C Public ML: 93% Google 11 scans 4mo 2 labels API - 1h ago	 cotrust-sg.com 1779 Start your cryptocurrency journey IPs 3 278 12 MB 200 CLOUDFLARENET - C Public ML: 96% Google 5 scans 2mo 2 labels API - 1h ago	 okexxone.com 1757 Start your cryptocurrency journey IPs 4 74 12 MB 200 CLOUDFLARENET - C Public ML: 91% Google 5 scans 6mo 2 labels API - 1h ago	 okrwlink.com 1777 Start your cryptocurrency journey IPs 4 74 13 MB 200 CLOUDFLARENET - C Public ML: 98% Infoblox Google 11 scans 4mo 2 labels API - 1h ago
 cnnymo.com 1949 Start your cryptocurrency journey IPs 2 294 16 MB 200 XNNET - XNNET ... Public ML: 97% Infoblox Google 3 scans 16d 1 labels API - 1h ago	 okrwxit.com 1777 Start your cryptocurrency journey IPs 4 75 12 MB 200 CLOUDFLARENET - C Public ML: 91% Google 9 scans 2mo 2 labels API - 1h ago	 phantomvip.com 1959 Start your cryptocurrency journey IPs 3 283 12 MB 200 CLOUDFLARENET - C Public ML: 95% Google 4 scans 1yr 2 labels API - 1h ago	 contimee.net 1933 Start your TimeCoin journey IPs 2 286 14 MB 200 CLOUDFLARENET - C Public ML: 98% Google 3 scans 14d 2 labels API - 1h ago	 okexxpro.com 1773 Start your cryptocurrency journey IPs 3 73 12 MB 200 CLOUDFLARENET - C Public ML: 91% Google 14 scans 9mo 2 labels API - 1h ago	 okdcassets.cc 1777 Start your cryptocurrency journey IPs 3 72 12 MB 200 CLOUDFLARENET - C Public ML: 95% Google 14 scans 1yr 2 labels API - 2d ago

The Story of Mr. D of Madison, Alabama

REDSTONE
FEDERAL CREDIT UNION
220 Wynn Drive Huntsville AL 35893 (800) 234-1234

Foreign Exchange Wire Receipt

Your wire request for \$29,000.00 is debited from account ending in 0100. In addition, a \$40.00 transfer fee is debited from account ending in 0100.

Originator Settlement Information		Beneficiary Settlement Information	
Wire Number:	113555	Available Date:	03/02/2026
Today's Date / Time:	02/20/2026 12:26 PM timezoneVariation: TimezoneExtended	Transfer Amount:	29,000.00 USD
Contract Number:	39242719		
Exchange Rate:	\$1.00 USD = 1.00 USD	Other Fees:	- 0.00 USD
Transfer Amount:	\$29,000.00 USD	Other Taxes:	- 0.00 USD
Transfer Fee:	\$40.00 USD		
Total from Originator:		Total to Beneficiary:	29,000.00 USD
\$29,040.00 USD		Beneficiary may receive less due to fees charged by the beneficiary's bank and foreign taxes.	
Originating Financial Institution Redstone FCU 220 Wynn Drive Originator [REDACTED] [REDACTED] MADISON AL 35758 United States		Beneficiary FI The Bk Rakyat Indonesia (Persero) T BRINIDJAXXX Jl. Jenderal Sudirman, Kav 44-46 Jakarta Indonesia	
Additional Information PAYMENT FOR ANTIQUE FURNITURE		Beneficiary RONI FANZORI BBAN 473402000001502 JL LENGKOK LENDAND NO 11 BANDUNG, 83653 Indonesia	

On February 21, 2026 “Mr. D” was told he was no longer allowed to send crypto to “CEX.IO” – the investment website he believed he was using.

He was instructed to wire \$29,000 to the criminals, to an Indonesian bank account, and to indicate that it was “Payment for Antique Furniture.”

Mr. D lives modestly. He has never sent money to Indonesia.

Suggested questions:

“Oh! How interesting! What type of furniture are you buying? How did you learn about the buyer? I’d love to see that furniture, could we look at the website together?”



Mr. D cashes out his TSP.gov retirement liquidates a \$365,000 401(k), paying a \$73,000 tax penalty

Your **Withdrawal Request** has been processed and will be effective at 12:00 pm eastern time on **February 25, 2026**.

You'll receive a confirmation email.

Note: For your privacy, some details won't be in the email. Print this page for your records.

Your Total Payment

<u>Gross Cash Payment</u>	\$365,000.00
Federal Withholding	-\$73,000.00
<u>Net Cash Payment</u>	\$292,000.00

Note: These amounts may change due to market fluctuations.

Destination for Cash Paid to You

Net Cash	\$292,000.00
----------	--------------

We contacted TSP.gov.

We were told that any person can withdraw their own funds for any purpose if they are willing to pay the tax penalty.

The **Alabama Securities Commission** sent agent's to Mr. D's door. He refused to answer.

He later received a certified letter from ASC informing him he was involved in a scam.

He sent the letter to the scammers saying:

"HELP ME PROVE THEM WRONG!"

On February 26th Mr. D attempts to wire \$100,000 to “Gree Constracting Services Inc” in Houston, TX.

Wire Transfer Services
Outgoing Wire Transfer Request

Today's Date: 02/26/2026
Banker Name: [REDACTED]
Banker Phone: 256/429-1300
Branch Number: 07281
Banker AUI: 0065661
Wells Fargo Reference Number: FW0065661057629158
Officer/Portfolio Number: C2594
Banker MAC: W0162-010

Outgoing wires can only be sent for Wells Fargo customers. Provide the Customer Copy to the customer ensuring you give them the Wire Transfer Agreement on pages 3 and 4. Note: Wells Fargo Wire Transfer Services will route wires based on correspondent banking relationships. See the Wire Transfer Information for explanations of the Mexican CLABE number, SWIFT BIC, the International Routing Code ("IRC"), Indian Financial System Code (IFSC) and the International Bank Account Number ("IBAN").

Originator's Information

Authorized Party Name: [REDACTED]
Street Address: [REDACTED]
Address Line 2: [REDACTED]
Address Line 3: [REDACTED]
City: MADISON
State: AL
ZIP/Postal Code: 357586828
Country: [REDACTED]
Home Phone: [REDACTED]
Business Phone: [REDACTED]

Wire Amount and Source of Funds

Create AUI: 0065661
Amount (US Dollars): \$100,000.00
Debit Wells Fargo Account: 5725553969
Bank/COD: 220

Beneficiary/Recipient Information

Beneficiary/Recipient Name: GREE CONSTRACTING SERVICES INC
Beneficiary Account Number/IBAN (Foreign)/CLABE (Mexico): 1075629798
Purpose of Payment: [REDACTED]
Name/Address Line 1: 7510 HORNWOOD DR APT 505
Name/Address Line 2: HOUSTON TX 770364322
Name/Address Line 3: [REDACTED]

Texas Secretary of State
Jane Nelson

UCC Business Organizations Trademarks Account Help/Fees Briefcase Logout

Filing Number: 806312265
Original Date of Filing: November 19, 2025
Formation Date: N/A
Tax ID: 32103086255
Duration: Perpetual

Entity Type: Domestic For-Profit Corporation
Entity Status: In existence
FEIN:

Name: Gree Constracting Services Inc
Address: 7510 HORNWOOD DR APT 505
HOUSTON, TX 77036-4322 USA

REGISTERED AGENT	FILING HISTORY	NAMES
Name	Address	
JILIN ZHU	7510 Hornwood Dr Apt 505 Houston, TX 77036 USA	

Gree Constracting (not a typo!) was created 19NOV2025. It's a mule account for a Chinese Money Laundering Organization's Professional Money Launderer.

Questions to ask:

How did you choose Gree Constracting of Houston to do home improvements in Madison, Alabama?

On March 2nd, Mr. D tries to wire \$75,000 to GHGC Construction of Brooklyn, New York

Wire Transfer Services
Outgoing Wire Transfer Request

Today's Date: 03/02/2026 Wells Fargo Reference Number: FW0065694061577668

Banker Name: [REDACTED]

Banker Phone: 256-5 [REDACTED] Branch Alt: 0065694

Outgoing wires can only be sent for Wells Fargo customers. Provide the Customer Copy to the customer ensuring you give them the Wire Transfer Agreement on pages 3 and 4. Note: Wells Fargo Wire Transfer Services will route wires based on correspondent banking relationships. See the Wire Transfer Information for explanations of the Mexican CLABE number, the SWIFT BIC, the International Routing Code ("IRC"), Indian Financial System Code (IFSC) and the International Bank Account Number ("IBAN").

Customer's Information

Authorized Party Name: [REDACTED] Street Address: [REDACTED] D

Address Line 2: [REDACTED]

Address Line 3: [REDACTED]

City: MADISON State: AL

ZIP/Postal Code: 35758-6828 Country: US

Home Phone: [REDACTED] Business Phone: [REDACTED]

Wire Amount and Source of Funds

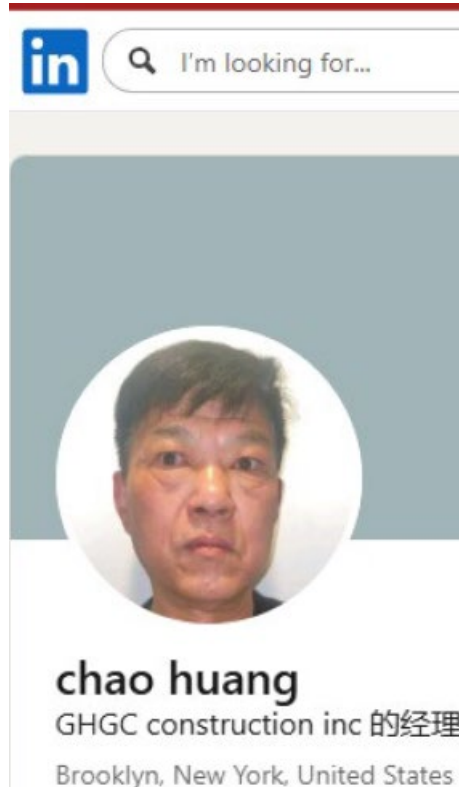
Amount (US Dollars): \$75,000.00 Debit Wells Fargo Account: 5725553969 Bank/COID: 220

Recipient Information (This is the ultimate recipient of the wire transfer funds)

Recipient Name: ghgc construction inc Name/Address Line 1: 1238 65th st

Recipient Account Number (Routing Number) (Mexico): 1470021105651 Name/Address Line 2: [REDACTED]

Purpose of Funds: [REDACTED] Name/Address Line 3: brooklyn, NY, 11219



GHGC Construction is another mule account for the same CMLO PML.

Chao Huang formed the corporation on 22DEC2025.

Mr. Huang of Brooklyn, New York would be receiving his wire at a Truist Bank branch in Richmond, Virginia.

Questions: Gee, Mr. D?

We notice you didn't send the \$100k to the contractor in Houston one week ago.

Help us understand the pivot to using a three-month old construction company in Brooklyn instead?

The scammers establish a “same name” account for Mr. D. He successfully wires \$200K to them.

To ensure the safety of your funds and comply with regulatory and anti-money laundering (AML) requirements, when you deposit fiat currency into the platform, we will generate a dedicated receiving account for you that matches your real name information

This account is used solely for your personal deposits and fund verification and will not be used by others, nor will it affect your normal transactions on the platform

Using an account with the same name as yours effectively avoids risks such as fund mismatch and third-party payments, ensuring clear source and account ownership of funds, thereby maximizing the security of your funds. Please feel free to use it

Bank: Slovak Savings Bank

Account Name: [REDACTED]

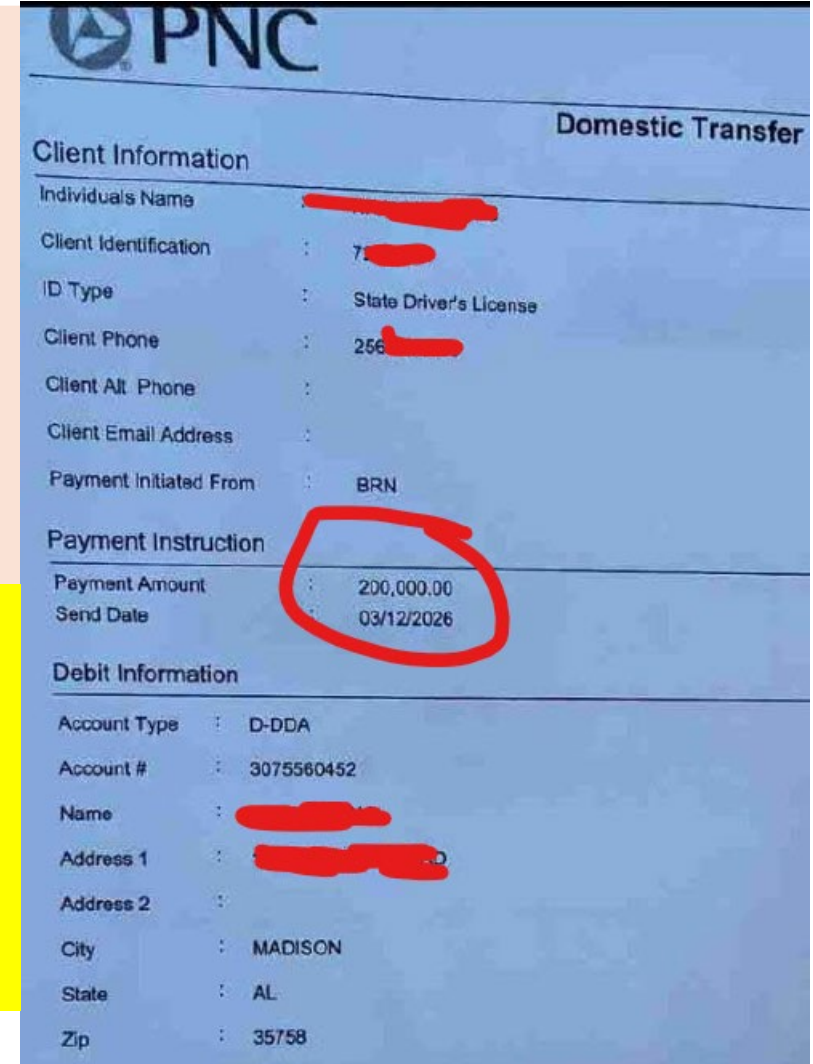
Account Number: 971718060829

ABA: 043087080

SWIFT/BIC: SSBAUS32

Questions?

“Mr. Dang, can you tell us how you chose to open an account in Pittsburgh with Slovak Savings Bank, having never lived in Pittsburgh and having no family or business contacts in Pittsburgh?”



The image shows a screenshot of a PNC Domestic Transfer form. The form is titled "PNC Domestic Transfer". It contains several sections: "Client Information", "Payment Instruction", and "Debit Information". In the "Client Information" section, the "Individuals Name" is redacted, "Client Identification" is 7 [REDACTED], "ID Type" is "State Driver's License", "Client Phone" is 256 [REDACTED], "Client Alt Phone" is blank, "Client Email Address" is blank, and "Payment Initiated From" is "BRN". In the "Payment Instruction" section, the "Payment Amount" is 200,000.00 and the "Send Date" is 03/12/2026, both of which are circled in red. In the "Debit Information" section, the "Account Type" is "D-DDA", "Account #" is 3075560452, "Name" is redacted, "Address 1" is redacted, "Address 2" is blank, "City" is "MADISON", "State" is "AL", and "Zip" is 35758.

Client Information	
Individuals Name	[REDACTED]
Client Identification	7 [REDACTED]
ID Type	State Driver's License
Client Phone	256 [REDACTED]
Client Alt Phone	
Client Email Address	
Payment Initiated From	BRN

Payment Instruction	
Payment Amount	200,000.00
Send Date	03/12/2026

Debit Information	
Account Type	D-DDA
Account #	3075560452
Name	[REDACTED]
Address 1	[REDACTED]
Address 2	
City	MADISON
State	AL
Zip	35758

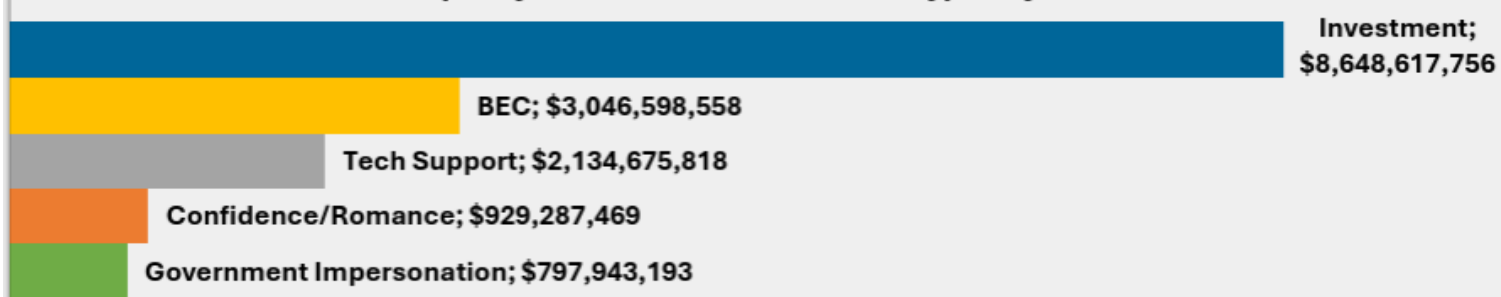


DARKTOWER

Crypto Scams and a Global Cybercrime Infrastructure

The FBI's Top Five Categories intersect heavily

Top 5 Cyber-Enabled Fraud Crime Types by Loss



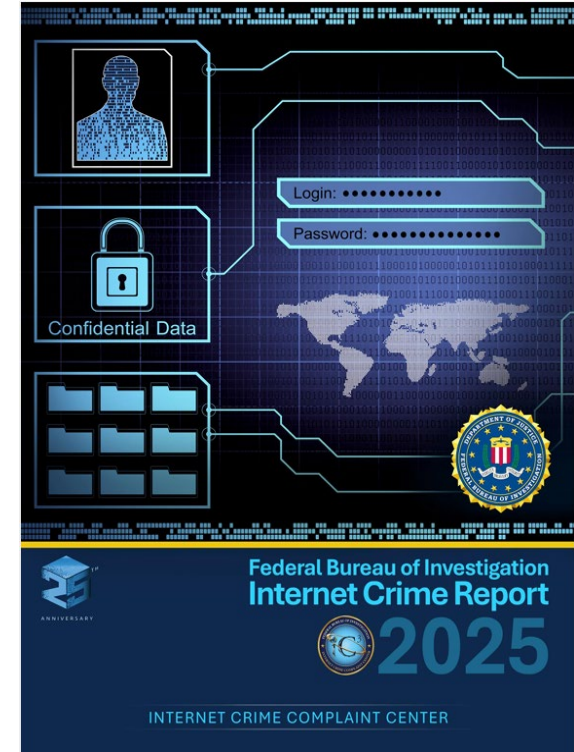
Crypto Investment Scams: dominated by Chinese organized crime but imitated by West African organized crime

BEC: dominated by West African organized crime

Tech Support: Scams run from India – but “cash/gold pickup” often using Chinese CMLO

Romance Scams: the key factor in most Crypto Investment Scams but also used by West African organized crime

Gov Impersonation: started by Indian call centers, growing in Chinese scam compounds



Romance Scammers:

- West African “Yahoo Boys”
 - Typically young and male
 - Between 2-3 million scammers
 - Often impoverished
 - Looking for “Fast Money”
 - Unsophisticated and undisciplined
 - Tend to imitate Soldiers, Doctors, Celebrities, Oil Platform Workers
 - Usually met on Dating Platforms or Facebook
- Chinese-run “Scam Compounds”
 - Often Human Trafficking victims
 - 300,000 – 500,000 scammers
 - Casts much wider net via unsolicited SMS
 - Tend to imitate wealthy but unknown persons
 - Forced to follow tightly regimented “playbooks”
 - May be beaten, tortured, or killed for failing to deliver on established quotas
 - Often uses LinkedIn as a targeted approach

Chinese Guarantee Syndicates: Crime-as-a-Service



By the summer of 2025, we were actively tracking nine
“Guarantee Syndicates.”

Between them they had more than 8,000 vendors!



Hai Hua (newest)!



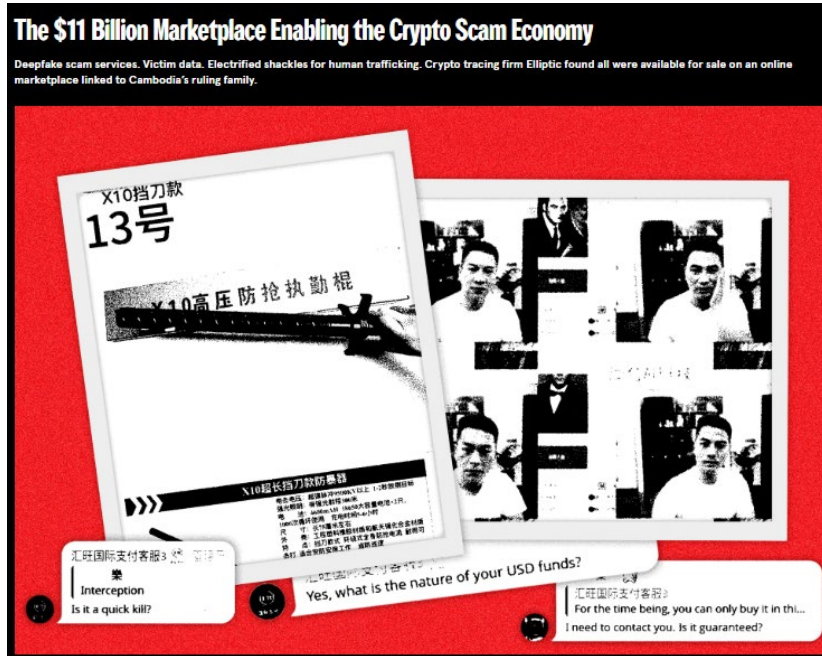
Each worked the same way.

- Vendors deposit a “Guarantee”
- They are listed in a topical “Crime-as-a-Service” menu
- The syndicate serves as “Escrow” for all transactions



Da Li

The previous “Biggest” : Haowang Guarantee (Huione Pay)



MATT BURGESS LILY HAY NEWMAN SECURITY JAN 14, 2025 4:00 AM

The ‘Largest Illicit Online Marketplace’ Ever Is Growing at an Alarming Rate, Report Says

Huione Guarantee, a gray market researchers believe is central to the online scam ecosystem, now includes a messaging app, stablecoin, and crypto exchange- while facilitating \$24 billion in transactions.



Huione Pay’s Haowang Guarantee was first exposed by Elliptic in partnership with WIRED magazine

July 2024

– “an \$11 Billion criminal marketplace”

January 2025

- “The Largest Illicit Online Marketplace Ever” (\$24 Billion!)



FinCEN on Huione Group

“Serves as a critical node for laundering proceeds of cyber heists carried out by the DPRK”

FinCEN Finds Cambodia-Based Huione Group to be of Primary Money Laundering Concern, Proposes a Rule to Combat Cyber Scams and Heists

Immediate Release: May 01, 2025

WASHINGTON — Today, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) issued a [finding and notice of proposed rulemaking](#) (NPRM) pursuant to Section 311 of the USA PATRIOT Act that identifies Cambodia-based Huione Group as a financial institution of primary money laundering concern and proposes to sever its access to the U.S. financial system.

Huione Group serves as a critical node for laundering proceeds of cyber heists carried out by the Democratic People's Republic of Korea (DPRK), and for transnational criminal organizations (TCOs) in Southeast Asia perpetrating convertible virtual currency (CVC) investment scams, commonly known as “pig butchering” scams, as well as other types of CVC-related scams. Given the money laundering risk posed by Huione Group, FinCEN is proposing to prohibit U.S. financial institutions from opening or maintaining correspondent or payable-through accounts for or on behalf of Huione Group.

FinCEN's investigation identified that, in aggregate, Huione Group laundered **at least \$4 billion** worth of illicit proceeds between August 2021 and January 2025.

Including AT LEAST:

\$37 Million from DPRK / Lazarus Group

\$36 Million from Pig Butchering

\$300 Million from “other scams”

Xin Bi (“New Coin”) Guarantee Syndicate

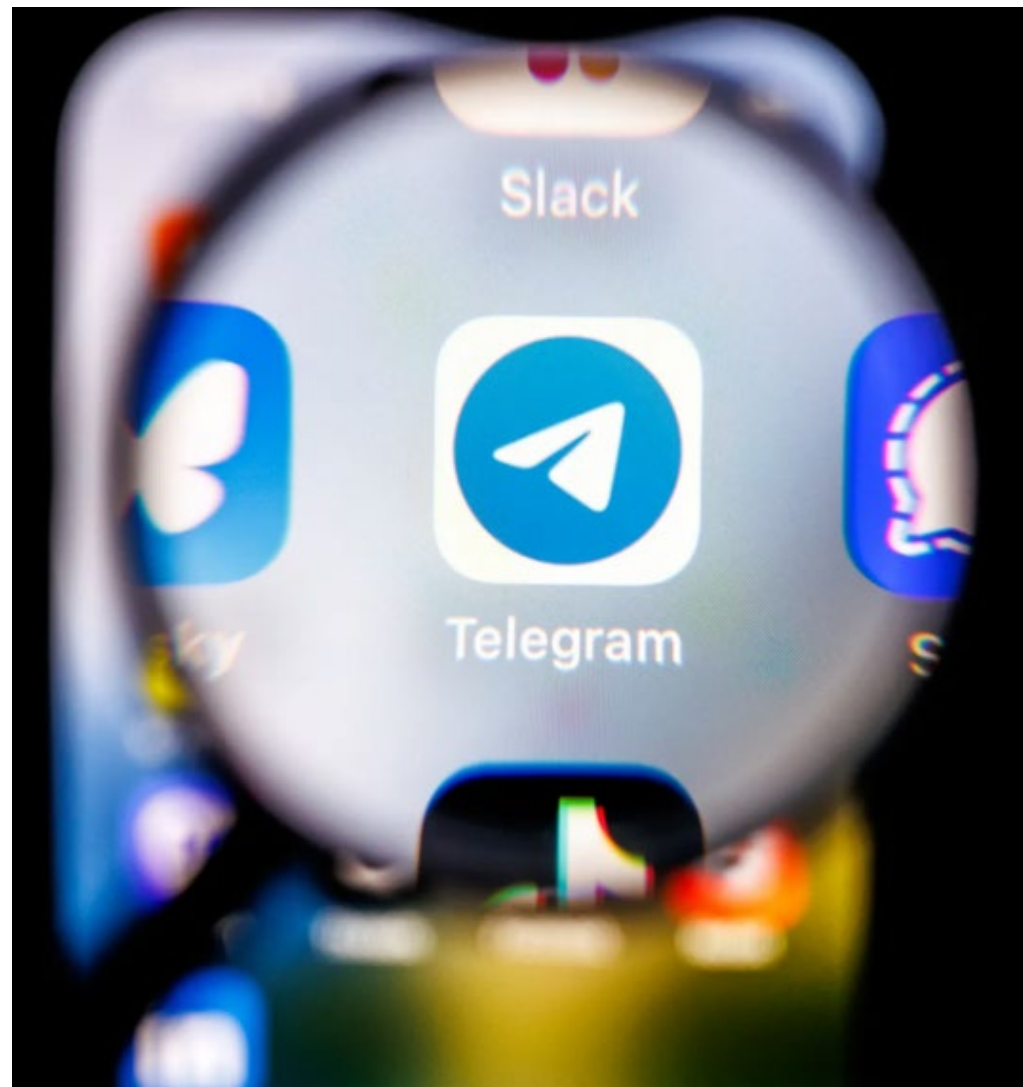
WIRED SECURITY

ANDY GREENBERG

SECURITY APR 14, 2026 2:56 PM

Telegram Is Still Hosting a Sanctioned \$21 Billion Crypto Scammer Black Market

The UK designated Xinbi Guarantee as an enabler of crypto scammers and human trafficking weeks ago. Telegram is still hosting it in plain sight.



Xin Bi is 100% criminal.

This was their vendor menu



新市公群频道 @gqdh
577 199 subscribers

①卡商公群: 1. [卡商大群](#) 2. [卡商小群](#) 3. [卡商业务细分](#)

②代收付公群: 1. [一道卡接回U](#) 2. [码接回U](#) 3. [群引导](#) 4. [二道卡接回U](#) 5. [app跑分](#) 6. [救火卡扣](#) 7. [NFC远程刷卡](#) 8. [购汇](#) 9. [收U放料](#)

③承兑公群: 1. [现金业务](#) 2. [三方承兑](#) 3. [POS承兑](#) 4. [实物承兑](#) 5. [礼品卡](#) 6. [平台币核销](#) 7. [门票核销](#)

④白资公群: 1. [白资收U](#) 2. [白资代付](#) 3. [收U出U一体](#) 4. [海外白资代付](#)

⑤招商合作"窗口": 1. [招车队/招料主](#) 2. [彩票/六合彩内幕/蛇货协议球](#) 3. [招聊手/后续代打](#) 4. [背债](#) 5. [危机公关](#) 6. [苞养窗口](#) 7. [跟车承兑](#) 8. [招快递站点](#) 9. [招挂号信](#) 10. [多种类窗口群](#) 11. [招电销团](#)

⑥服务类: 1. [天眼查](#) 2. [票务代付](#) 3. [租社交账号](#) 4. [美工设计](#) 5. [接码注册实名](#) 6. [账号/交易所解封](#) 7. [代办/代打电话](#) 8. [高端外国](#) 9. [ID贷款](#) 10. [AI换脸](#) 11. [其他服务](#)

⑦搭建类: 1. [平台搭建](#) 2. [机器人](#) 3. [服务器](#) 4. [拉码插件](#) 5. [远控](#) 6. [域名](#) 7. [定制IP](#) 8. [签名上架](#)

⑧加密货币相关: 1. [NewPay](#) 2. [现货与合约](#) 3. [混币与跨链兑换](#) 4. [trx能量与兑换](#)

⑨买卖类: 1. [各种账号](#) 2. [手机卡](#) 3. [888匿名号NFT](#) 4. [烟酒](#) 5. [保健品/奢侈品](#) 6. [TG号/会员](#) 7. [金包钨/高仿手机](#) 8. [其他买卖](#)

⑩游戏公群: 1. [PC2.0/PC高倍/PC网盘](#) 2. [骰子](#) 3. [综合盘/电子](#) 4. [百家乐](#) 5. [体育](#) 6. [六合彩](#) 7. [德州扑克](#) 8. [红包娱乐](#) 9. [其他娱乐](#)

⑪引流类: 1. [地推贴纸](#) 2. [手机口/短信口/接听口](#) 3. [收粉/出粉](#) 4. [收数据/出数据](#) 5. [短信代发/短视频代发](#) 6. [电销](#) 7. [拉手/话术单](#) 8. [TG引流](#) 9. [留群](#) 10. [免费VPN](#)

已退押公群招商中: [新市招商频道](#)

① SIM/Card Vendor Groups:

1. Large-scale vendor groups
2. Small-scale vendor groups
3. Specialized business segments

② Payment Collection & Disbursement Groups:

1. Tier-1 card processing (crypto settlement)
2. QR code processing (crypto settlement)
3. Group-based traffic routing
4. Tier-2 card processing (crypto settlement)
5. App-based transaction processing
6. Emergency card processing
7. NFC remote card transactions
8. Currency exchange
9. Crypto-to-fiat/asset exchange

③ Acceptance/Settlement Groups:

1. Cash-based business
2. Third-party acceptance
3. POS-based acceptance
4. Physical asset acceptance
5. Gift cards
6. Platform token redemption
7. Ticket redemption

④ "Clean Capital" Groups:

1. Clean capital crypto acquisition
2. Clean capital disbursement
3. Integrated crypto acquisition & disbursement
4. Overseas clean capital disbursement

⑤ Partnership/Recruitment "Gateways":

1. Recruiting fleets/cargo owners
2. Lottery/Mark Six insider info/fixed-match agreements
3. Recruiting chat agents/follow-up operators
4. Debt assumption
5. Crisis PR
6. "Sugar baby" arrangement services
7. Logistics/freight acceptance services
8. Recruiting courier stations
9. Registered mail services
10. Various gateway groups
11. Recruiting telemarketing teams

⑥ Services:

1. Corporate data checks (e.g., [Tianyancha](#))
2. Ticket payment services
3. Social media account rentals
4. Graphic design
5. SMS verification/real-name registration services
6. Account/exchange unblocking
7. Proxy services/proxy calls
8. High-end escort services
9. ID-based loans
10. AI face-swapping
11. Other services

⑦ Infrastructure/Setup:

1. Platform setup
2. Bots/automation
3. Servers
4. Referral code plugins
5. Remote control software
6. Domain names
7. Custom IP addresses
8. App signing and store listing

⑧ Cryptocurrency-related:

1. [NewPay](#)
2. Spot and futures trading
3. Coin mixing and cross-chain swaps
4. TRX energy and exchange services

⑨ Trading/Sales:

1. Various accounts
2. SIM cards
3. "888" anonymous NFT numbers
4. Tobacco & alcohol
5. Health supplements/Luxury goods
6. Telegram accounts/Premium memberships
7. Tungsten-core gold/High-quality replica phones
8. Other trading

⑩ Gaming Groups:

1. PC 2.0/High-multiplier PC games/PC web-based games
2. Dice games
3. Comprehensive betting platforms/Electronic games
4. Baccarat
5. Sports betting
6. Mark Six lottery
7. Texas [Hold'em](#)
8. Red envelope games
9. Other entertainment

⑪ Traffic Generation:

1. Offline promotional stickers
2. Mobile/SMS/Call-in gateways
3. Lead acquisition/distribution
4. Data acquisition/distribution
5. SMS/Short video broadcasting services
6. Telemarketing
7. Recruiters/Scripted sales materials
8. Telegram traffic generation
9. Group placement/retention
10. Free VPNs

Category #1 卡商类 – 208 vendors (Bank Card Merchants & Money Mule Providers)

Operational Scope: Supplying personal retail bank cards, corporate bank accounts (公户), cryptographic hardware USB security tokens (U盾), and merchant POS terminals to serve as disposable drop accounts.

人头 (Rén Tóu - "Human Head"): A recruited identity mule whose personal identification documents are used to open bank accounts or shell corporate entities.

牛户 (Niú Hù - "Ox / Power Account"): High-tier banking accounts with pristine transaction histories capable of absorbing large transfers without triggering automated anti-money laundering (AML) circuit breakers.

无视地区 (Wú Shì Dì Qū): Bank accounts operable nationwide without municipal risk-control restrictions.



**Public Group K Group 123 -
1 Million USDT Deposit for
Jincheng International
(Beijing General Manager)
Card Merchant Public
Group (Monthly
Settlement)**

22,703 members, 3,430 online



**Public Group H (88888) -
Deposit of 680,000 U
Jiuzhou Regular/Regional
Collection/Card/Public
Account/Ren Tou Public
Group (Monthly
Settlement)**

7,453 members, 1,417 online

Choose Xinbi, choose Jiuzhou, choose
[@xingyun383](#)



**Public Group G, Group
2116 - Deposit 128888U
(Deposit Reduction
80000U) Tomorrow Group
(Public Account/Card)
Direct Collection Public
Group (Monthly
Settlement)**

16,018 members, 1,991 online



**Group F (5555) - Deposit of
110,000 USD worth of
Mercedes-Benz Group
credit cards (public/private
accounts) - Direct
collection from credit card
dealers (monthly
settlement)**

8,017 members, 1,067 online



**Public Group G, Group
3145 - Deposit of 110,000
USDT - MY Card Merchant
Direct Collection Public
Group (Monthly
Settlement)**

5,906 members, 566 online

Category 2 - 代收付类 – subcategories (Collection and Payment / Inflow Funnel)

Vendors	Subcategory	Subcategory translation
208	一道卡接回U (大混/综合)	First-Tier Card Refund (Mixed/Comprehensive)
42	一道常规卡接回U	First-Tier Regular Card Refund
14	一道三黑/无视卡接回U	First-Tier Blacklist/Ignore Card Refund
693	码接回U	Code Refund
265	群引导	Group Guidance
13	二道卡接回U	Second-Tier Card Refund
16	APP跑分	APP Scoring
107	救火卡扣	Fire-Rescuing Card Debit
33	NFC远程刷卡	NFC Remote Card Swiping
31	购汇 (香港公私户/跨境通)	Foreign Exchange Purchase (Hong Kong Public/Private Accounts/Cross-Border E-Commerce)
191	收U放料 (盘口料主放料)	Receiving and Releasing Credit (Indexing Credit)

Category #3 – 承兑类 – Subcategories (Settlement, Acceptance & Cash Liquidation)

Vendors	Subcategory	Subcategory translation
261	现金业务 (滴滴现金/闪送/上门)	Cash Services (Didi Cash/Flash Delivery/Door-to-Door Service)
11	现金业务 (证券拿现)	Cash Services (Securities Cash Withdrawal)
11	现金业务 (U商拿现/黄金承兑)	Cash Services (U-Merchant Cash Withdrawal/Gold Acceptance)
123	三方承兑 (微信/支付宝/网银二道承兑)	Third-Party Acceptance (WeChat/Alipay/Online Banking Second-Tier Acceptance)
15	POS承兑	POS Acceptance
69	实物承兑 (货拉拉/快递/黄金手机)	Physical Acceptance (Lalamove/Express/Gold/Mobile Phones)
160	礼品卡核销 (京东E卡/沃尔玛/大润发/苹果卡)	Gift Card Redemption (JD.com E-Card/Walmart/RT-Mart/Apple Card)
102	平台币核销 (游戏币/直播币/点卡充值)	Platform Coin Redemption (Game Coin/Live Stream Coin/Point Card Recharge)
12	门票核销 (景区/迪士尼/酒店餐券)	Ticket Redemption (Scenic Spot/Disney/Hotel Restaurant Vouchers)

Cash Pickup / Gold Pickup

There are easily THOUSANDS of individuals working in the United States as “Tap to Pay” Shoppers and “Cash/Gold Pickup Crews



Us. NFC碰碰车队, 寻求一手料站, 贴手工作室对接, 全美跑扫货, 有卡多的工作

la ge ★

1 Cash pickup truck, our Blue Sky Technology Co., Ltd. has been engaged in this industry for 6 years. We specialize in cash withdrawal, with an exchange rate of 76/84. Payment will be made within 2 hours after receiving the cash.

2 Withdrawal location

3 Los Angeles 90 91 92

4 San Francisco 94 95 96

5 Seattle 97 98 99

6 Phoenix 85 86

7 Boston 01 02 03 04 05 06 07

New York 08 09 10 11 12

Syracuse 13 14

Washington 19 20 21 22 23 24

Dallas 74 75 76 77 78

North Carolina 27 28 29

Atlanta 30 31 35 36 37 38 39

Chicago 53 58 59 60 61 62

St. Louis 40-46 61-66

Flights can be booked all over the United States

Canada

Over 10,000 parcels

whatsapp+852 5509 3802



Cash pickup and Gold pickup

1 419 members, 15 online

When you have any trading, please contact the administrator, do not trade privately, at your own risk

@vip98r

Info

t.me/cashpick001

Link

Caesar 🍷

🌟🌟🌟 24H WORK 🌟🌟🌟

🌟 My name is xiao. I'm from China. I'm a recipient 🌟

🌟 My main jobs are wire, cp, cc and gift cards 🌟

🇺🇸🇺🇸 cash/Gold pick 🌟

🌟 My people are distributed over Los Angeles/San Francisco/Seattle/Phoenix/Boston/New York/Syracuse/Washington/Dallas/North Carolina/Atlanta/Chicago/St. Louis 🌟

✅ Cash pickup 10K+

✅ Cash package 3K+

✅ Gold pickup 10oz +

✅ Reservations are accepted in all regions

✅ Without middlemen directly contacting runners, you can get better services and exchange rates

🌐 Wire 🌐

✅ US TO US US TO HK

✅ US TO Italy US TO Chile

✅ US TO Japan US TO Singapore

✅ Account holder. Providing feedback on time can offer you the wire solution with the best success rate, ensuring that every transfer you make is successful



“Collection Crew” / Cash/Gold Pickup groups depositing more than 100,000 USDT

hxxps://t[.]me/+1viBXdj8GK00N2Ux	588888588888U-AX Company Didi Cash Back U Public Group
hxxps://t[.]me/+BmGBB9sONtpmOTdl	486666Pledge 486666U Sanhe/Securities/U Merchant/Cash/Direct Takeout/Gold/Physical Commodities Public Group
hxxps://t[.]me/+y9JAKjVLGXAwZDM9	336888336888U-hy company Didi cash back U public group
hxxps://t[.]me/+BkLl7FhswFtjNWMx	319999319999U Rainbow Group Didi cash gold physical goods door-to-door return U public group
hxxps://t[.]me/+khkZMBJNjOtmYjNl	318888318888U No.9 Mansion Didi Cash/Door-to-Door U-Commerce Securities Public Group
hxxps://t[.]me/+UyDyVZjD7gU1NDZl	300000Deposit 300,000 USD/CHF, pay cash/gold, nationwide face-to-face transaction, direct collection public group
hxxps://t[.]me/+uyvpBWTgE9A5NDI9	299300Pledge 299300U Earth Gold Express/Liquor/Lalamove/Securities Direct Takeover Public Group
hxxps://t[.]me/+DIzjPsldUbhmN2Rl	292528292528U Tianji Group Didi Cash/Goods Hourly Delivery Public Group
hxxps://t[.]me/+L-YyVFMVah5jOTY1	270000270,000 U-Ahao/Securities/U-Business/Didi Lost Package/Gold Public Group
hxxps://t[.]me/+RugEn_9k6-U3YmUx	265888265888U Orange Full Cash Gold Public Group
hxxps://t[.]me/+daMFbLlL1Yw1OGJl	260000Deposit 260,000 U Global/Gold Express/U Merchant/Securities Door-to-Door Direct Collection Public Group
hxxps://t[.]me/+UKji5wFuz8E0MWMx	258888258888U Tianxing Group Cash Gold Public Group
hxxps://t[.]me/+1n6UwDaJm0l2YWQ1	238888238888U-ZEO Didi Cash Back Group
hxxps://t[.]me/+7YJPvobXi3BmNjBl	200000Pledge 200,000 U of gold cash and mobile phone express delivery to receive it back in U public group
hxxps://t[.]me/+abCB9a-45nM5YjVl	188888188888U Phoenix Cash/Gold/Technology Direct Access Public Group
hxxps://t[.]me/+amIK6dW0Z7QxZWQ1	188888Pledge 188888U Xinyuan Group Didi cash/gold physical/door-to-door service public group
hxxps://t[.]me/+bB8VLsuDs19hMDJh	149200Pledge 149,200 U-GM Group Didi cash/U-merchant securities/physical return U public group
hxxps://t[.]me/+lvUD1GcMB1UzY2Rl	138088138088U Tianting Group Didi Cash and Physical Goods Return U Public Group
hxxps://t[.]me/+UoeKLw5vzClxYzk1	133333133333U Jinli Group Didi Cash Back U Public Group
hxxps://t[.]me/+qH9iHQcgBncyM2Y1	130000Deposit 130,000 U - Wanbang International Didi Cash Flash Delivery Back to U Public Group
hxxps://t[.]me/+QB_IHfs-p5lOWY1	112666112666U-TMT Group Cash Back Public Group
hxxps://t[.]me/+Q7sMlD7TaTUwYWMx	111111111111U Huixin Group Didi Cash Back U Public Group
hxxps://t[.]me/+6cw4FeI0GX0zYjk1	110888110888U Niu Niu Didi Cash Back U Public Group
hxxps://t[.]me/+fc8_65ivYkwwYWU1	109488Deposit 109488U Gemini full slap Didi cash back U public group
hxxps://t[.]me/+ioP2ed0R4_Y0ZDk1	108888Pledge 108888U-AK Didi Cash/Express Mobile Gold Public Group
hxxps://t[.]me/+d-zlXhrnQuYwNmEx	106666Pledge 106666U Hongxing Payment/Door-to-Door/U Merchant/Securities/Cash/Gold Public Group
hxxps://t[.]me/+d6OsOTX2KhA5ZDAx	103333103333U Three Kingdoms Group Didi Cash (Fish Delivery) Return U Fast Public Group
hxxps://t[.]me/+yXfb2ONIHws0ODhl	102000The group that deposited 102,000 U and Tianxia Group slapped Didi cash back U public group
hxxps://t[.]me/+lpi-ZKzD9CczMWFl	100888Lin Jie, who is a Didi driver, is a public group for returning real money.
hxxps://t[.]me/+vGA2fBe1zd5iN2Y1	100188100188U Litong Group Didi Cash Flash Delivery Back to U Public Group



DARKTOWER

Breaking the Spell

Banks need to help 'break the spell' of romance scams

Key findings

- Intervention and prevention are made difficult for firms because victims may be 'under the spell' of the fraudster and reluctant to accept they are being defrauded. In nearly half (42%) of the cases the FCA reviewed, victims did not disclose the true reason for making a payment when asked.
- Despite examples of good practice, there were multiple instances of firms missing opportunities to identify seemingly suspicious transactions. This indicated that firms could calibrate their monitoring systems to be more effective.
- A key area of improvement is for firms to ensure their staff are trained to spot red flags and critically probe customer explanations. This was not consistent across all firms.
- Many firms are providing a high level of support, occasionally exceeding the FCA's expectations, through compassionate and tailored engagement, although this wasn't consistent across all firms.

FinCEN “pig butchering” Red Flags

Behavioral Red Flags

-  1 A customer with no history or background of using, exchanging, or otherwise interacting with virtual currency attempts to exchange a high amount of fiat currency from an existing or newly opened bank account for virtual currency or attempts to initiate high-value transfers to VASPs.
-  2 A customer mentions or expresses interest in an investment opportunity leveraging virtual currency with significant returns that they were told about from a new contact who reached out to them unsolicited online or through text message.²¹
-  3 A customer mentions that they were instructed by an individual who recently contacted them to exchange fiat currency for virtual currency at a virtual currency kiosk and deposit the virtual currency at an address supplied by the individual.²²
-  4 A customer appears distressed or anxious to access funds to meet demands or the timeline of a virtual currency investment opportunity.

* - VASP = Virtual Asset Service Provider – usually a Cryptocurrency Exchange

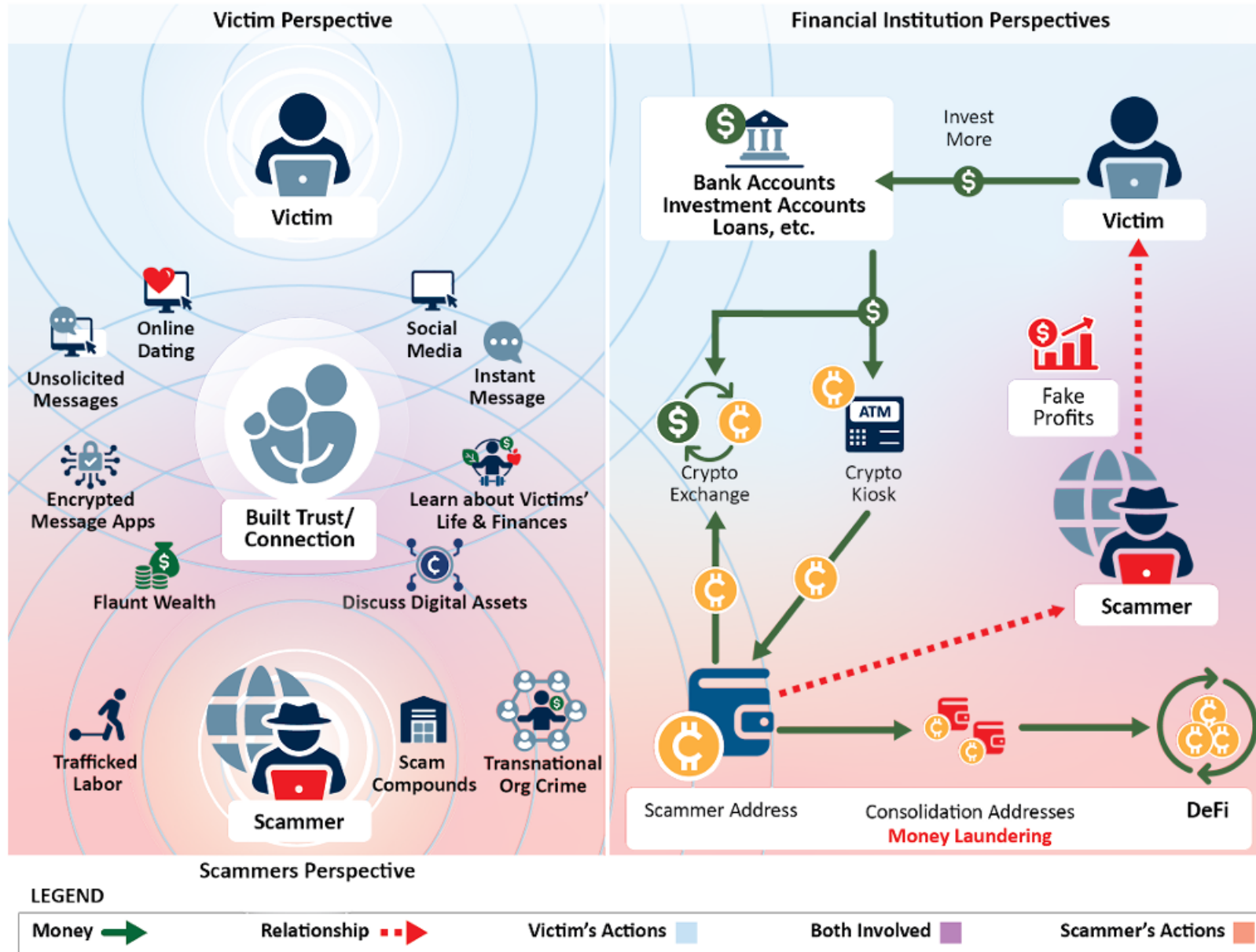
Financial Red Flags

-  5 A customer uncharacteristically liquidates savings accounts prior to maturation, such as a certificate of deposit, and then subsequently attempts to wire the liquidated fiat currency to a VASP or to exchange them for virtual currency.
-  6 A customer takes out a HELOC, home equity loan, or second mortgage and uses the proceeds to purchase virtual currency or wires the proceeds to a VASP for the purchase of virtual currency.
-  7 A customer receives what appears to be a deposit of virtual currency from a virtual currency address at or slightly above the amount that the customer previously transferred out of their virtual currency account. This deposit is then followed by outgoing transfers from the customer in substantially larger amounts.
-  8 Accounts with large balances that are inactive or have limited activity begin to show constant, uncharacteristic, sudden, abnormally frequent, or significant withdrawals of large amounts of money being transferred to a VASP or being exchanged for virtual currency.
-  9 A customer sends multiple electronic funds transfers (EFTs) or wire transfers to a VASP or sends part of their available balance from an account or wallet they maintain with a VASP and notes that the transaction is for “taxes,” “fees,” or “penalties.”²³
-  10 A customer with a short history of conducting several small-value EFTs to a VASP abruptly stops sending EFTs and begins sending multiple high-value wire transfers to accounts of holding companies, limited liability corporations, and individuals with which the customer has no prior transaction history. This is indicative of a victim sending trial transactions to a scammer before committing to and sending larger amounts.

Technical Red Flags

-  **11** System monitoring and logs show that a customer's account is accessed repeatedly by unique IP addresses, device IDs, or geographies inconsistent with prior access patterns. Additionally, logins to a customer's online account at a VASP come from a variety of different device IDs and names inconsistent with the customer's typical logins.
-  **12** A customer mentions that they are transacting to invest in virtual currency using a service that has a website or application with poor spelling or grammatical structure, dubious customer testimonials, or a generally amateurish site design.²⁴
-  **13** A customer mentions visiting a website or application that is purported to be associated with a legitimate VASP or business involved in investing in virtual currency. The website or application shows warning signs such as a web address or domain name that is misspelled in such a manner as to resemble that of another business, a recently registered web address or domain name, no physical street address, international contact information, or contact methods that include only chat or email.²⁵
-  **14** A customer mentions that they downloaded an application on their phone directly from a third-party website, rather than from a well-known third-party application store or an application store installed by the manufacturer of the device.
-  **15** A customer receives a large amount of virtual currency such as ether at an exchange, subsequently converts the amount to a virtual currency with lower transaction fees such as TRX, and then abruptly sends it out of the exchange.

Figure 3: Example Flow of Digital Asset Investment Funds



Wire Transfers: “Purpose of Funds” check

What happens after a victim sends crypto to a scammer? Now it needs to be laundered.

Just like with Mr. D, the scammers are often working with Professional Money Launderers. Often-Chinese individuals who have established LLCs and opened business banking accounts with those LLCs.

The individuals who are told to send money to those accounts rarely have a full “cover story.” They are usually given a 3-5 word phrase to indicate “purpose for funds.”

Crypto Transfers:

“ask about investment” check

The customer is being deceived – but often the deceiver has spent MONTHS building trust. The deceiver may be “**the most important person**” in the victim’s life. A five-minute conversation with a banker is not going to over-ride that trust factor.

Show “genuine interest” in their investment! Ask if they have an app on their phone. Learn about their website.



Gov Impersonation: “large cash withdrawals” “Who are you talking with?” check

As a point of control and coercion, when a Government Impersonation scam is happening, the victim is usually required to stay on the phone the entire time. This can often run into phone calls lasting multiple hours.

It is important to understand that they have often been told that they will be arrested and/or deported if they do not obey the “FBI/HIS/DEA Agent” they believe they are speaking with. They have been ordered by who they perceive to be Law Enforcement that they **MUST NOT REVEAL** to the bank why they are withdrawing their funds.

If a Cash Withdrawal fails, they may be instructed to purchase Gold by wiring funds to a nearby gold dealer. A Failed cash withdrawal should be flagged for any suspicious outbound wire transfers.

The FBI will never:

- Call or e-mail private citizens to demand payment or threaten arrest. You will also not be asked to wire a “settlement” to avoid arrest.
- Ask you to use large sums of your own money to help catch a criminal.
- Ask you for wire transfers or gift cards.
- Call you about “frozen” Social Security numbers or to coordinate inheritances.

Intervention: The guy in the car

I bank with PNC.

Recently my PNC branch started having a “greeter” ... the door is opened by a friendly banker who welcomes me to the branch.

But he is also trained to notice if there is someone waiting for me in the vehicle I arrived in.

Scenario One: “Heads”

A person recruited by a fraudster is being paid (possibly in drugs) to enter the bank using a counterfeit identity to withdraw funds from an account.

They will have a Drivers License with their photo, but the address of your account holder.

Scenario Two: “Elder Abuse”

An elder or recent immigrant believes that they must withdraw their funds to avoid harm, arrest, or deportation to themselves or a loved one.

They will likely show signs of nervousness or anxiety and may have been driven to the bank by the criminal.

https://www.fbi.gov/how-we-can-help-you/common-frauds-and-scams

Did you receive a message from the FBI?

The FBI will never call or email private citizens to request they move money via wire transfer, cryptocurrency, gift cards, or prepaid cards. You can always reach out to **your local field office** to confirm whether or not an email or message is actually from the FBI. And if you think you're the victim of a scam, report it to **ic3.gov**.



Adoption Fraud

Unethical adoption service providers can take advantage of an emotionally charged process to deceive and defraud prospective adoptive parents or birth parents considering adoption. Learn what to look out for, how to protect yourself and your family, and what to do if you're a victim.



Business and Investment Fraud

Scammers are always looking to separate you from your money in business transactions. If it sounds too good to be true, it is. Common scams include advance fee schemes, Nigerian letter or 419 schemes, Ponzi schemes, pyramid schemes, and telemarketing fraud schemes.



Business Email Compromise

Business email compromise (BEC) is one of the most financially damaging online crimes. It exploits the fact that so many of us rely on email to conduct business—both personal and professional.



Charity and Disaster Fraud

Charity fraud scams can come in many forms: emails, social media posts, crowdfunding platforms, cold calls, etc. They are especially common after high-profile disasters. Always use caution and do your research when you're looking to donate to charitable causes.



Election Crimes and Security

Fair elections are the foundation of our democracy, and the FBI is committed to protecting the rights of all Americans to vote. If you suspect a federal election crime, contact the FBI.



Healthcare Fraud

Healthcare fraud is not a victimless crime. It affects everyone and causes tens of billions of dollars in losses each year. The FBI is the primary agency for investigating healthcare fraud, for both federal and private insurance programs.



Holiday Scams

When shopping online during the holiday season—or any time of year—always be wary of deals that seem too good to be true, and do your part to avoid becoming a scammer's next victim.



Money Mules

A money mule is someone who transfers or moves illegally acquired money on behalf of someone else. Some money mules know they are supporting criminal enterprises; others are unaware that they are helping criminals profit. Don't be a mule.



Consumer Fraud Schemes

Learn more about common fraud schemes that target consumers, including identity theft, non-delivery scams, online car buying scams, and theft of ATM/debit and credit cards.



Cryptocurrency Investment Fraud

Cryptocurrency investment fraud, which the media commonly describes as pig butchering, is one of the most prevalent and damaging fraud schemes today.



Cryptocurrency Job Scams

These scams begin when scammers, masquerading as employees of legitimate companies, recruit victims and require them to deposit their own money in order to complete the job.



Elder Fraud

Each year, millions of elderly Americans fall victim to some type of financial fraud or confidence scheme. Common scams that target older citizens include romance scams, tech support scams, grandparent scams, government impersonation scams, sweepstakes and lottery scams, home repair scams, and TV/radio scams.



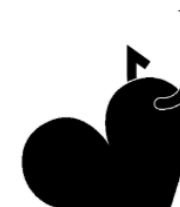
Operation Level Up

The FBI's proactive approach to identify and notify victims of cryptocurrency investment fraud and prevent further financial loss.



Ransomware

Ransomware attacks are becoming more targeted, sophisticated, and costly. Learn more about this type of malware, including how to respond and report if it happens to you.



Romance Scams

Protect your heart—and your wallet—by learning to spot and prevent romance scams.



Sextortion

Sextortion is a crime that involves adults coercing kids and teens into sending explicit images online. The FBI has several resources to help caregivers and young people better understand what sextortion is, how to

<https://www.staysafeonline.org/campaigns/thenandnow>



Defense against cybercrime, scams, and fraud in understandable terms designed for older adults.

In an increasingly digital world, it's important to make sure we all know how to stay safe online. With an online curriculum, a printed workbook, and volunteer toolkit, Then & Now has everything you need to protect yourself, your friends, and your loved ones.

Learn Online

Printed Workbook

Volunteer Toolkit

Partner with Us



<https://www.aarp.org/lp/banksafe/>

Register Now

Be proactive. Be Bank*Safe*.

The AARP BANKSAFE™ INITIATIVE is a free online intervention platform developed in collaboration with more than 2,000 industry professionals to help financial organizations spot—and, more importantly, stop—suspected financial exploitation.

REGISTER NOW



Much more on LinkedIn ...



Gary Warner

DarkTower / Intelligence For Good:
Fighting Cybercrime with Intellig...



The Prince Group CEO Chen Zhi has been extradited to China ... now his scam compounds are being evacuated!



When
"Crypto Investment Scams"
aren't Crypto



Is Potato Guarantee
shutting down?

Perhaps ...



"I didn't invest in Crypto!
I invested in Green Energy!"



Sailor Phishing Platform



Scam compound:
Crown Casino Poipet-
Cambodian enforcement?
Or sleight of hand?



GhostHacker OS
BEC on Steroids:

one West African
Scammer's Toolset



The new "QR code" Notice of Hearing spam
has gone through several generations



Version 1 used sloppy AI "state seals"
Version 2 got the seals right and enlarged the QR code
Version 3 moved the seal to the top, often in color, and added a border
Version 4 adds a red "Failure to Act" bar and chooses names other than "John Smith"