Connecting Chinese and American Scam Victims

Bitrace [*] & ChainArgos [†]

January 9, 2024

1 Introduction

The world is experiencing an epidemic of online scams with at least tens of billions of dollars lost across dozens of countries (4). One particular class of scam known as "pig butchering" [1] has grown dramatically and often involves the use of cryptocurrency both to collect funds from victims and to launder the proceeds (6). Here we are going to explore the use of cryptocurrency in pig butchering scams beginning with victims in both the People's Republic of China and United States of America, and demonstrating the remarkable degree of similarity for cases that have no reason *a priori* to be similar at all.

Specifically we will show that scammers with victims in both these countries share cryptocurrency addresses, use overlapping sets of money-laundering services, and are therefore likely parts of the same group or syndicate. Our analysis begins with reports from victims in both countries where we find source victim and scam wallet addresses. From there we are able to trace scam proceeds through the cryptocurrency ecosystem to prove these connections. Finally, a range of exchanges and other service providers are identified through a combination of on-chain and documentary research, to demonstrate the cross-border nature of modern scams leveraging cryptocurrencies, and highlight the challenges facing law enforcement agencies globally when it comes to such scams.

1.1 A Note On Presentation and Documentation

To keep this discussion accessible, and the figures useful, all wallet address details are presented in the appendix. While we would encourage parties with the expertise to check and reproduce this work we recognize that the vast majority of readers are not interested in that level of detail.

This is not an attempt to obfuscate or otherwise make checking our findings difficult. Rather it ensures all the charts of flows are readable and all the long strings required to check them can be

[*]Bitrace is a Chinese blockchain data analysis company that provides leading cryptocurrency data analysis, risk management, law enforcement collaboration, and other compliance and regulatory tool products and service support to web3 enterprises, financial institutions, and regulatory and law enforcement departments. Email: bitracecn@gmail.com

[†]ChainArgos is a blockchain intelligence firm, providing on-chain data for insight into protocols, transactions, and flow, for hedge funds, venture capital, investment firms, regulators, law enforcement agencies, research academies, and financial institutions. Email: info@chainargos.com

[1] "Pig butchering" scams are a type of confidence trick and investment fraud in which victims are gradually lured into making increasing contributions, in the form of cryptocurrency, to a seemingly sound investment before the party they are dealing with disappears.

easily copied out of the document. The appendix is formatted such as we would choose as consumers of this data trying to reproduce the results.

Further, for the purposes of this analysis we take all presented documentation at face value, ascribe equal weights among them and generally consider the information they contain to be reliable. It is important to note that this analysis is not intended as a study of comparative legal systems or police procedures – it is about demonstrating a remarkable degree of overlap and similarity among scams active in both China and the United States.

2 Victims

Here we explore 4 different victims:

- one case from Florida: *the Florida Case*
- one case involving victims in both California and Florida: *the California Case* [2]
- two cases from China: *the China Cases*

The Florida case is significantly larger than the others where one victim was taken for over US$2 million. In that case, a wide range of laundering techniques were employed to manage the scammed proceeds. The remaining cases are smaller, with each employing fewer techniques.

2.1 Florida Victim

In *the Florida Case*, the victim fell for a relatively common pig butchering scam which court documents describe as follows:

> On April 15, 2022, Plaintiff and Defendant communicated through Facebook, an online social media and social networking service. Id. ¶ 10. Defendant represented that she was successfully engaged in investing in cryptocurrency and that her aunt was a prosperous cryptocurrency trading expert who managed an analyst group at Grayscale Investments, a legitimate third-party digital currency asset management company. Id. ¶¶ 11, 12. Defendant represented that, if Plaintiff were to join a margin trading platform called foundrypro.net ("Foundrypro"), Defendant would use sophisticated algorithms designed and implemented by Defendant's aunt to execute cryptocurrency trades in order to earn Plaintiff a profit. Id. ¶ 13. Neither Defendant nor Defendant's aunt had a relationship with Grayscale Investments. Id. ¶ 15.
>
> Based on these representations, Plaintiff joined Foundrypro on May 17, 2022 and began executing margin trades on that platform on Defendant's advice. Id. ¶ 17, 19. Over the course of Plaintiff and Defendant's relationship, Plaintiff invested 2,215,118 units of "Tether" (USDT), a form of cryptocurrency known as stablecoin that is pegged to the

[2] This case was handled by a court in Florida for jurisdictional reasons even though the California victim lost more money. The name was chosen to reduce confusion.

value of the U.S. Dollar. Id. ¶¶ 23, 24. From April 15, 2022 through the end of October, 2022, Defendant communicated with Plaintiff via SMS, WhatsApp, telephone calls, and email. Id. ¶ 16. Foundrypro featured a dashboard that displayed illusory investment gains which, together with Defendant's representations, encouraged Plaintiff to continue "investing" in Foundrypro. (1)

Following a number of legal steps the victim secured a default judgement.

Further documents in the case provide a range of cryptocurrency addresses in two categories. First the document lists those addresses where the victim originally transferred their funds, which we shall refer to as *scam entry* addresses. Second the documents present a list of cryptocurrency exchange deposit addresses [3] where some of the victim's funds were sent. All of these addresses are provided in appendix A.1.

2.2 California Victims

In *the California Case*, two separate individuals fell victim to romance-based pig butchering scams, but sent cryptocurrency to the same scam entry wallet provided in appendix A.2. The first scam involved about US$177,502.29 dollars and is described in court papers as:

> [Victim] met an individual known to him as "Bunny" through social media (Facebook) and started a romantic relationship with her. During the relationship, Bunny offered [Victim] a way to make money through cryptocurrency so they could afford to buy a farm and live together one day.
>
> During the relationship, Bunny convinced [Victim] to invest in cryptocurrency through "Pearcoin," a fake cryptocurrency trading application, unknown to [Victim] at the time.
>
> Ultimately, [Victim] attempted to withdrawal his funds from Pearcoin and was told he must pay the taxes up front or he would risk a 3 per cent penalty fee for each day he did not pay. At this point, [Victim] realized he was involved in a scam and subsequently contacted the Brevard County Sheriff's Office to report the incident. [Victim] was unable to transfer, withdraw, or access any of his funds through the investment platform. (3)

The second scam is similar and involved around US$300,000:

> The victim ... reported she had been romantically involved with an individual through social media. During the relationship, she was convinced to invest in cryptocurrency. (3)

[3] Cryptocurrency exchanges operate "deposit addresses" to simplify the process on depositing funds for their clients. When a client wishes to deposit funds they ask the exchange to create a special only-for-them address where they can send funds. In this way the exchage can assign all transfers in to that address to a specific client account automatically. Think of "deposit addresses" as a tool for ensuring money is sent to the correct internal account through the use of different external account numbers.

2.3 Chinese Victims

Information and data on *the China Cases* have been provided by Bitrace. The first victim, from Tianjin, reported losing USDT, a dollar-based stablecoin, after they were convinced to invest into an arbitrage trading strategy by setting up an account at the cryptocurrency exchange OKX, and withdrawing USDT to the trading apps WBF and 币胜. Following several smaller investments which paid returns totalling US$4,860 the Tianjin victim made further deposits and eventually lost approximately US$40,000. There was no report of a romance element in this scam and it more closely resembles the pig butchering scam in *the Florida Case*. The Tianjin victim's funds were traced to se_1^{china} provided in appendix A.3, a known scam-related wallet we will encounter again later.

A second victim, otherwise active in the OTC markets, reported a *drainer* scam involving se_2^{china} again using USDT. A *drainer* scam is one in which the victim is convinced to download malicious "Trojan horse" software which then drains their wallet, sending the funds to the scammer (7; 5; 9). This scam appears connected to a smaller network than the Tianjin victim, although Bitrace has clients in the OTC space that have encountered both of these scams.

We do not have court documents for these cases in the same manner as the American ones, but we can point to local reporting about similar cases to further reinforce these patterns. Similar scams were reported in Ningbo (2) and Wenzhou (8) by local authorities. For example, a press release from Wenzhou law enforcement describes a scam involving "Trojan horse" software similar to that reported by one of Bitrace's clients:

> It has been found that since February 2022, the gang has published advertisements selling discounted gas cards on multiple overseas social software, using the guise of detecting the authenticity of virtual currency wallets and virtual currencies to trick victims into clicking on Trojan horse program links. Secretly control his wallet, and when the time is right, he illegally obtains the virtual coins in the wallet, committing more than 30 crimes in just one month, involving more than 1 million yuan. (8)

This sounds similar both generally to scams reported around the world and specifically to the drainer scam reported by the Chinese victim active in OTC markets.

In *the Chinese Cases* documentation similar to *the Florida and California Cases* is unavailable to provide comparative analysis, given differences in the two countries' legal systems, but does not detract from the similarity in their *modus operandi*. As we will see, proceeds from all the scams analyzed pass through entangled collections of wallets and service providers which provides compelling evidence they are linked.

3 Service Providers

The Florida victim's court documents reference four cryptocurrency exchanges: Binance, Bitkub, FTX and OKX, all of which are large, well-known services. Binance has long been the world's largest cryptocurrency exchange and FTX was founded by Sam Bankman-Fried who is currently awaiting

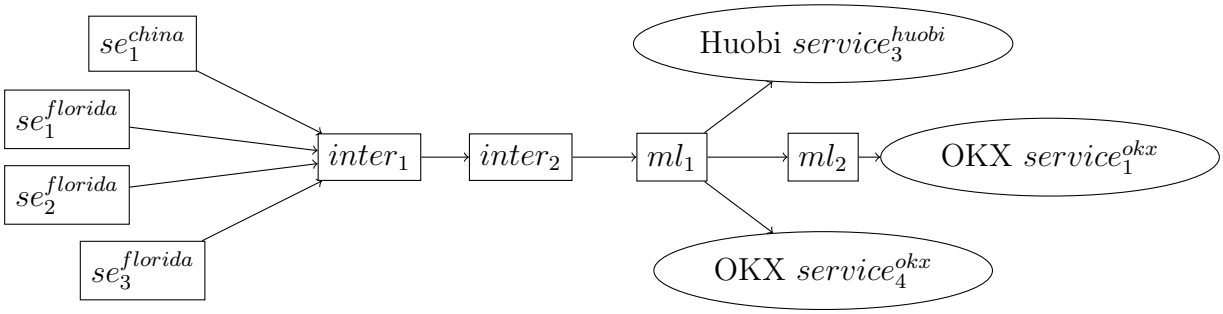

Figure 1: Connecting the Florida victim to a Chinese victim. And connecting both scam incidents to the same money laundering service provider. Note this exchange deposit address is not named in the Florida documents – this is an additional downstream off-ramp.

sentencing following an extremely high-profile fraud trial. OKX is a large cryptocurrency exchange which, while less well-known than Binance and FTX, sponsors several high profile sports teams and events around the world. Bitkub, the smallest of the four listed, is Thailand's largest cryptocurrency exchange and similarly maintains high-profile sponsorships within its market.

Further analysis finds deposits to Coinbase, Huobi, Maicoin, Maskex, Paribu, and Peatio, which are similarly, well-known exchanges. Coinbase is listed on NASDAQ, reports billions of dollars in annual revenue and currently has a market capitalization in the tens of billions of dollars. Huobi is a large exchange with several HKEX-listed subsidiaries and much like many other Asian exchanges, it sponsors sports including Spain's national men's football team. Maicoin refers to itself as Taiwan's leading cryptocurrency exchange. Maskex is a UAE-based cryptocurrency exchange which holds a VASP license there. Paribu is a Turkish exchange that has partnerships with several Turkish football clubs. Peatio was a Chinese cryptocurrency exchange that shut down years ago and open-sourced their exchange software, and while the exchange may be defunct, its wallet addresses are still active.

Here we merely wish to establish that these service providers are large, well-known, visible entities that do not require further analysis or any sort of documentary evidence as to their existence or involvement in cryptocurrency trading.

Further discussion will involve smaller parties operating between the scam entry points and exchanges. While these are less visible in the press and sporting worlds, we are going to see that they are very clearly involved in managing scam proceeds.

4 Tracing Downstream

Analyzing downstream flows from *the China Cases*, and *the Florida Case* reveals common destinations for the scam proceeds. In figure 1 we plot flows from the three Florida addresses and a Chinese one through the same intermediaries to two wallets we have labelled ml_1 and ml_2, with ml intended to denote "money launderers" because they receive proceeds from a collection of scams and deposit the money on to exchanges and are the functional equivalent of forwarding addresses.

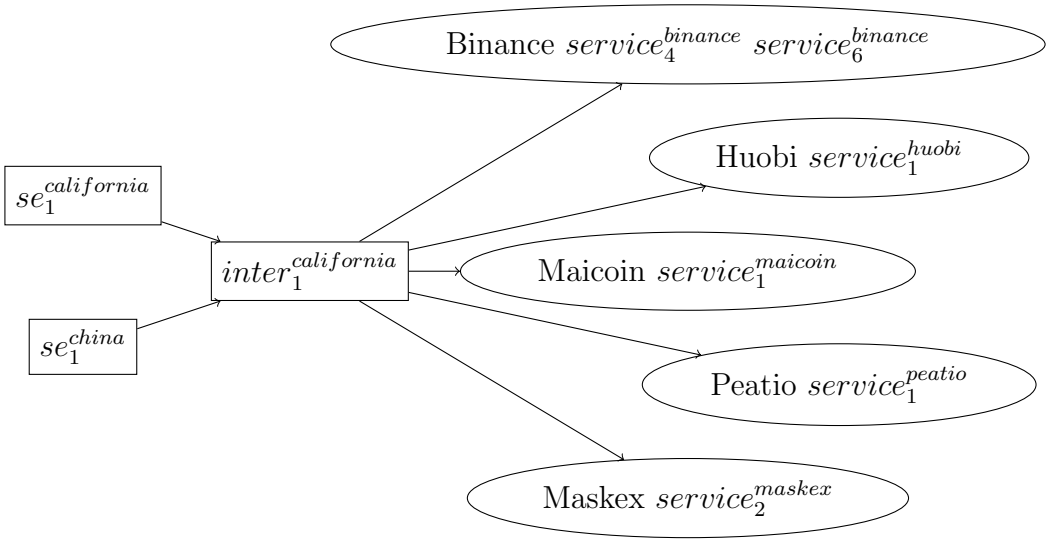

Figure 2: Connecting the California entry address to the Chinese one. Their shared downstream intermediary has connections to many exchanges.

It is important to note that scam proceeds are not transferred by the laundering addresses in back-to-back sequential transfers. It is not the case that each unit of scam proceeds was fed through this exact sequence of wallets at the same time. Instead, we are merely establishing that the ingestion and laundering of these scam proceeds involved the same parties, around similar times, in the same way, and therefore are likely to be part of the same overall group. This is particularly convincing as these trails all head towards common money laundering services en route to off-ramps.

Now let us connect *the Chinese Case* to *the California Case*. Here we see overlapping flows in a somewhat different configuration in figure 2. The same wallet appears one step downstream from both entry points.

Also note the intermediary $inter_1^{california}$ is connected to many of the deposit addresses given in *the California Case's* civil forfeiture order (3). Further, one of the Binance deposit addresses in this chart [4] was brought to ChainArgos' attention months ago by reporters from Reuters as being associated with a lot of scams in connection with (6). The link in this chart processed only US$45,000 and this connection was only discovered near the end of the analysis, but establishes a connection between this work and the reporting by Reuters.

Next we present a different configuration of intermediaries and exchange off-ramps in figure 3. The *China Cases'* scam entry address also has direct connections to the exchange deposit addresses from figure 4.

A similar structure is seen downstream from se_2^{china} where, after passing through two intermediary wallets, the funds are deposited to $service_5^{okx}$.

While this is not an exhaustive list of connections, it demonstrates that these scams are well-connected both among themselves and to a wide range of exchanges.

[4] $service_6^{binance}$

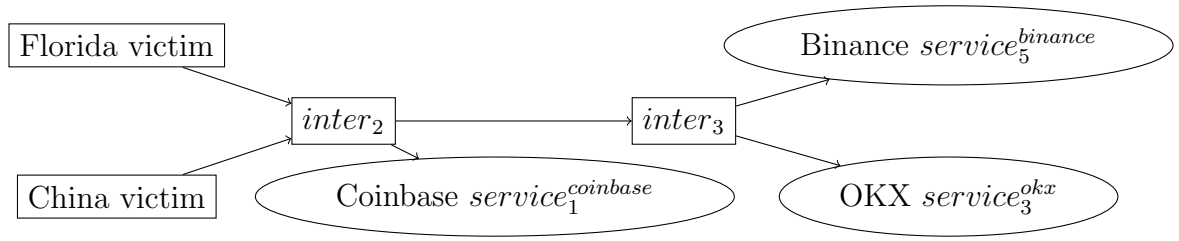

Figure 3: Further connections.

Binance	Huobi	Maskex	OKX	Paribu
$service_1^{binance}$	$service_1^{huobi}$	$service_1^{maskex}$	$service_1^{okx}$	$service_1^{paribu}$
$service_2^{binance}$				
$service_3^{binance}$				
$service_4^{binance}$				

Figure 4: Exchange deposit addresses directly connected to the Chinese victim's scam entry address.

5 Total Amounts

The analysis up till now examined individual scams and traced funds through common sources, which establishes these scams are large and parts of the same organization or meta-organization. At present, there is insufficient information to document all the scams perpetrated by this group or related groups. Given the nature of these crimes and victims it is unlikely we will ever have a reliable exhaustive list. So the next logical step is to look at the gross quantum of funds passing through the service provider addresses used in these cases, to ascertain the potential scale of this meta-organization. Our analysis of the scale of the operation begins three separate but related questions:

1. How much money passed in to "scam entry" addresses we know about?
2. How much money passed through service providers?
3. How much money passed out to off-ramps like exchanges?

5.1 Scam Sizes

If we look at the se_1^{china} address which scammed the Tianjin victim, we find a total of US$20.7 million passed through that address commencing at the beginning of 2021 and continuing until the time of preparation of this analysis. As the Tianjin victim lost about US$40,000 we know we are looking at only a small sliver of overall activity and there are surely more cases centered on this address.

In *the Florida Case* the victim claims losses of approximately US$2.2 million but those three addresses show a total inflow of just under US$6.5 million, confirming there are surely more victims. Across the six "scam entry" addresses used to map these flows we find total inflows of:

$se_1^{florida}$	US$3 million
$se_2^{florida}$	US$4 million
$se_3^{florida}$	US$2 million
$se_1^{california}$	US$350 thousand
se_1^{china}	US$21 million
se_2^{china}	US$285 thousand
Total	US$30 million

Uniquely among these addresses most of the scam inflows to $se_1^{california}$ were denominated in the cryptocurrency ether, rather than the stablecoin USDT and $se_1^{california}$ received 156.04 ether in total. We have dollarized ether at the price of US$2,000 which reflects the approximate average conversion price at the time of transfers.

5.2 Service Provider Sizes

Next we look at the total amount of flow through some of the intermediary addresses. For the six intermediaries in the examples above we find total USDC and USDT inflows to be:

ml_1	US$79 million
ml_2	US$2 million
$inter_1^{california}$	US$15 million
$inter_1$	US$2 million
$inter_2$	US$6 million
$inter_3$	US$2 million
Total	US$106 million

Some of these are the same tokens flowing through more than one address, and an example above even shows flows from ml_1 to ml_2. Despite the flows, a reasonable estimate is these intermediaries processed somewhere between US$80 and US$100 million, with no intention for this figure to be exhaustive.

By far the largest group of flows are those to the exchanges. Examining deposits in to the exchange addresses named in (1) we find the following totals:

Exchange	Amount
Binance	US$159 million
Bitkub	US$27 million
FTX	US$249 million
OKX	US$13 million
Total	US$447 million

If we now add the additional addresses connected via the other cases we get:

Exchange	HQ	Florida Amount	Additional Amount	Total
Binance	Malta/Seychelles/?	US$159 million	US$35 million	US$194 million
Bitkub	Thailand	US$27 million	US$76 million	US$103 million
Coinbase	USA		US$2 thousand	US$ 2 thousand
FTX	Bahamas	US$249 million		US$249 million
Huobi	Seychelles		US$10 million	US$10 million
Maskex	UAE		US$ 3 million	US$ 3 million
Maicoin	Taiwan		US$177 thousand	US$177 thousand
OKX	Seychelles	US$13 million	US$28 million	US$41 million
Paribu	Turkey		US$10 thousand	US$10 thousand
Peatio	China?		US$8 million	US$8 million
Total		US$447 million	US$188 million	US$635 million

While this does not mean this meta-organization is responsible for all these flows, it provides strong evidence there are large flows and large amounts of related crime still to be found in this area.

Note the data includes several exchanges with small volumes. These are included for completeness as, again, this is not an attempt to be exhaustive. Even within exchanges with large totals we find individual deposit addresses that vary by orders of magnitude in total flow.

Also note that nearly all of the exchange volume occurred on exchanges outside China and the United States. The vast majority was handled by businesses headquartered in offshore jurisdictions.

5.3 Exchange Withdrawals

In *the California Case*, investigations also yielded an exchange withdrawal address on the Tron blockchain controlled by the scam meta-organization ("the Tron Address"). Flows through the Tron Address totaled about US$1.1 million dollars, an amount far in excess of the approximately US$500,000 lost in *the California Case* suggesting further investigation on Tron – and other blockchains – is likely to turn up additional connections.

6 Discussion

This analysis demonstrates three key facts:

1. Similar simultaneously-run scams have victims in both China and the United States.
2. Funds taken from both jurisdictions flow through common service providers.
3. The sums involved range from the tens to possibly hundreds of millions of dollars.

It is important the analysis is understood with the following limitations:

1. We are not claiming that *all* US$30 million of inflows to these "scam entry" wallets are scam

proceeds, only what can currently be tracked.

2. Although US$635 million in exchange deposits were identified, we are not claiming that all of this can be attributed to scams.

3. Given the cycling of transactions, the numbers above may not be entirely free of double-counting. [5]

Instead, the analysis should be understood from the context of the scope and scale of the scams being perpetrated. First, only four cases were analyzed, where victims came forward and some form of formal or legal process had been commenced. Second, we have demonstrated these scams are connected to those discussed in (6), which suggests the scale and magnitude of such scams are potentially more far-reaching and larger than previously understood.

It seems probable there are a lot more common flows to be discovered, and the quantum of scam proceeds passing through the cryptocurrency ecosystem is likely to be significantly larger than our current estimates. Further, it is noteworthy that while the victims in these cases were located in the world's two largest economies, at most a tiny fraction of the exchanges processing these scam proceeds are domiciled in those countries. A tremendous amount of international cooperation will be necessary to address these problems.

[5] For example it is possible some money deposited on one exchange is then withdrawn and re-deposited somewhere else.

References

[1] Bowen v. Xingzhao Li, 23-cv-20399-BLOOM/Otazo-Reyes (S.D. Fla. Jul. 26, 2023).

[2] China Ningbo Net. A large amount of virtual currency was stolen from a ningbo citizen by a hacker., 7 2022. URL http://news.cnnb.com.cn/system/2022/07/19/030371164.shtml. English version translated from the original Mandarin with Google Translate.

[3] Florida Circuit Court. Eighteenth Judicial Circuit In And For Brevard County, Florida Case No: 05-2002-CA- Filing 162250539 Civil Forfeiture.

[4] Global Anti-Scam Alliance. The global state of scams - 2022 report, 2022. URL https://www.gasa.org/product-page/the-global-state-of-scams-2022-report.

[5] Ledger. Security incident report, 12 2023. URL https://www.ledger.com/blog/security-incident-report.

[6] P. McPherson and T. Wilson. Crypto scam: Inside the billion-dollar "pig-butchering" industry. 11 2023. URL https://www.reuters.com/investigates/special-report/fintech-crypto-fraud-thailand/.

[7] ScamSniffer. From google to x ads: Tracing the crypto wallet drainer"s $58 million trail, 12 2023. URL https://drops.scamsniffer.io/post/from-google-to-x-ads-tracing-the-crypto-wallet-drainers-58-million-trail/.

[8] Wenzhou Public Security Bureau. 743 cases were solved and 2,093 people were arrested! the results of the wenzhou clean network 2022 operation are announced!, 11 2022. URL https://mp.weixin.qq.com/s/hU5_jxtoVUHpmmKOYmg6Jw. English version translated from the original Mandarin with Google Translate.

[9] ZachXBT. Monkey drainer twitter thread, 10 2022. URL https://twitter.com/zachxbt/status/1584955933452484613.

A Appendix: Addresses

A.1 Florida Victim

Type	Exchange	Name	Address
Scam entry		$se_1^{florida}$	0xBA109c48264785070E35963592540324e8612d09
Scam entry		$se_2^{florida}$	0xb285CA276C96c47b546d0Ca88F77905fAdC8eb3A
Scam entry		$se_3^{florida}$	0x9800322CA41c512265A0B14C49a834C4A2c448Aa
Exchange deposit	Binance	$florida_1^{binance}$	0x54414a636b5439b14266f1ec9504a34b50cb5b9b
Exchange deposit	Binance	$florida_2^{binance}$	0x753173f4a680796f98e6b824a0f2da6fef191b39
Exchange deposit	Binance	$florida_3^{binance}$	0xb90f30f9f279fc07f33c3cd3942dc028f97400a4
Exchange deposit	Binance	$florida_4^{binance}$	0xb90a40957179711a53d09ade855bc5f45eeca1e1
Exchange deposit	Binance	$florida_5^{binance}$	0x38f6e7dd38954102b8471e7985d2420d23b3f35d
Exchange deposit	Binance	$florida_6^{binance}$	0x94bf1e38da59c7df90566883a3525c5fa3ca215c
Exchange deposit	Binance	$florida_7^{binance}$	0xc52b9dfb82490d14d76f0efd7ce76e82f2b5adfc
Exchange deposit	Binance	$florida_8^{binance}$	0xf380135d44be7e08a95c74c01c53deaec3a1701f
Exchange deposit	Binance	$florida_9^{binance}$	0xea5331f5f39c6e3801e4fd63d99e75b2a527d032
Exchange deposit	Binance	$florida_{10}^{binance}$	0xf1d60bb0958a79cbaf2145a929cd395173a37149
Exchange deposit	Binance	$florida_{11}^{binance}$	0x98a3b01609867a066524f78b33c72feef598d78d
Exchange deposit	Binance	$florida_{12}^{binance}$	0x54414a636b5439b14266f1ec9504a34b50cb5b9b
Exchange deposit	Binance	$florida_{13}^{binance}$	0xa14e0972a9d1ecdd7b8eb3be27b3901ebb24518f
Exchange deposit	Binance	$florida_{14}^{binance}$	0x9f7db89d141521517a553fbb704b8b05566c08a5
Exchange deposit	Binance	$florida_{15}^{binance}$	0x5768a6c7a29cea444bbdd454b03a288d0e1d113e
Exchange deposit	Bitkub	$florida_1^{bitkub}$	0x2bc47f91bfc8d848abfce3b81f3ce07e647fbc2d
Exchange deposit	Bitkub	$florida_2^{bitkub}$	0xdb752832678b48e0ab53e023f054f62a09ca852c
Exchange deposit	Bitkub	$florida_3^{bitkub}$	0xe51d0faa62f279e45938edd494f92720126bcf4f
Exchange deposit	FTX	$florida_1^{ftx}$	0x56f60315bee850b6a212c797ee1ed43503a9536c
Exchange deposit	FTX	$florida_2^{ftx}$	0x0f4c6cc5492dbbeb567ad752afa4ea16f44e51c6
Exchange deposit	OKX	$florida_1^{okx}$	0x29b71e4e2d12a6aa2f3cf330f0d79e75e58f54f0
Exchange deposit	OKX	$florida_2^{okx}$	0x967d6bc2696935b305dc42023e8e7453bbef5f6c
Exchange deposit	OKX	$florida_3^{okx}$	0x8c379e714c01a8f8b3cb328f46bc249f918a5df4

A.2 California Victims

Type	Exchange	Name	Address
Scam entry		$se_1^{california}$	0xcCC2F333e57cB739a3a62ED1e7A76EE17D3C3911
Intermediary		$inter_1^{california}$	0x346eF244464679b031750f70D750B3FA65165443
Exchange deposit	Binance	$cali_1^{binance}$	0x8459dd488c507b20331e0F6aC481F75Ee9f4ae97
Exchange deposit	Binance	$cali_2^{binance}$	0x1d43DC389993cB3818724E0d06746BbaA6A9e02e
Exchange deposit	OKX	$cali_1^{okx}$	0xc3b15B326C0eD1576f918a3B36c9dE789f936d0b
Exchange deposit	Bitkub	$cali_1^{bitkub}$	0x5453fd1ef17c8c4F2042b07416573c3eCa19D247
Withdrawal	Binance	$cali_{withdrawl}^{binance}$	TWLy3aGGkRck2uoZenQQPVi7AapyTVNebC

A.3 Chinese Victims

type	name	address
Scam entry	se_1^{china}	0xe0f807bbb43ece93dde44869d9a5324d5771bd67
Scam entry	se_2^{china}	0x41f0725de3f24a8ac2974a66e3a9b53567a70e0a

A.4 Service Providers

Description	Name	Address
Money laundering	ml_1	0xd7ee3b0fffd6a0d9d26a79129159942d29665fe1
Money laundering	ml_2	0xab557fcc296231ca252857b64bd6373d8c5ed0e1
Intermediary	$inter_1$	0x7ece0eff6631de8bf0717f65264945164fef019d
Intermediary	$inter_2$	0x197b81d8593bC8dFbBB689DfD102E91217028baf
Intermediary	$inter_3$	0x4fF0043D87900Ac1c64D63ad22f1e3cF781A9Aa3
Binance deposit	$service_1^{binance}$	0x4517779153917fe9342443DEA08681894a62bBe1
Binance deposit	$service_2^{binance}$	0x8d9e3622651E920a0Ed392d1B72a4a4F70fABB59
Binance deposit	$service_3^{binance}$	0x65e84F275dF40295a53CA0215720F350198De1Aa
Binance deposit	$service_4^{binance}$	0x101ae4fa34ae5fdb538c1e0161a3632d51a15392
Binance deposit	$service_5^{binance}$	0x8DaE1F79fe75A6B55d548B725973611C886496cD
Binance deposit	$service_6^{binance}$	0xaf9e1ff950337cb623a12467301d63c3ce803005
Bitkub deposit	$service_1^{binance}$	0x08c3ae0DBd53D6E01F9e8EB21E20be2e0da97Eb8
Coinbase deposit	$service_1^{coinbase}$	0x03d6cf0f90387132cbd60a3d6a4151179eb9fdce
Huobi deposit	$service_1^{huobi}$	0x8868df97a1ce9c1a091c6836d988a430cc0ffe35
Huobi deposit	$service_2^{huobi}$	0xeAb7461efeEFaB80ca7CC98708E5319C7F3F4B44
Huobi deposit	$service_3^{huobi}$	0xc32eA9c68AaB7f1CDc8E251dEFFffFbC1271B092
Maicoin deposit	$service_1^{maicoin}$	0x1646651e9C35Fdd8484082d37aB17d0AA4a51457
Maskex deposit	$service_1^{maskex}$	0x1C8321acbe4CA3e9AD0287b8E5c262Ce343B27D2
Maskex deposit	$service_2^{maskex}$	0x19231f73cdcb01c346f23c58e388f79d7480a0a9
OKX deposit	$service_1^{okx}$	0x7bAF3e10BfB2177061dbc576B126Ffd605751bC0
OKX deposit	$service_2^{okx}$	0x34cF51e60B2997e544Da263dfBac4562d14b7DAB
OKX deposit	$service_3^{okx}$	0xCebc7962ECFe1A268810C928C467c5c4A63905c8
OKX deposit	$service_4^{okx}$	0x2C72dDd368c4B50d99Aa2bBA0a7F3e49Ad346b8E
OKX deposit	$service_5^{okx}$	0x90B5a0893189F9B0264e238f9EFE0df92A41BA2d
Paribu deposit	$service_1^{paribu}$	0x27f72A97951135EB63aEb37d91eE02bA94fF1175
Peatio deposit	$service_1^{peatio}$	0x01d05E050172ECf22A3374905822302296D71b1d