ASC
Alberta Securities Commission

Fraudulent Investment Websites

Cynthia Campbell

March 17, 2023

Presentation to WITS-Warwick Gillmore Centre for Financial Technology Feeder Workshop on Frontiers of AI and FinTech

Overview

1. Background: Binary Options
2. Fraudulent crypto websites and how they work
3. Victimization in Canada and the U.K.
4. Current response in Canada by securities regulators
5. Response internationally
6. Challenges
7. Research opportunities

Background: Binary Options

In 2014-17, significant increase in online frauds relating to binary options

- At the peak, the FBI's Crime Complaint Center reported "hundreds of complaints" with "millions of dollars in reported losses" in 2016*
- CSA Binary Options Task Force engaged in extensive efforts to reduce harm
- CSA Investor Education campaign raised awareness

Whack-a-mole

* https://www.fbi.gov/news/stories/binary-options-fraud

Background: Binary Options

From education and disruption to prohibition

- September 2017 - CSA banned binary options < 30 days
- July 2018 – European Securities and Markets Authority (ESMA) imposed a temporary prohibition on binary options
- April 2019 – FCA placed a permanent ban on binary options
- Other international bans followed, putting an end to binary options schemes

Organized criminal networks, not Binary Options, were the root cause of the problem

Fraudulent investment websites remain

- The organized criminal networks continue to operate
- Networks and their associates are now dispersed across more countries
- It has become faster, easier, cheaper and more lucrative to commit online investment fraud, and harder to trace it
- Fraudulent investment websites evolved from binary options to forex to crypto

23366.42 -1.436% | Ethereum (ETH) $1629.28 -1.684% | Tether (USDT) $1.00 -0.02% | XRPL (XRP) $0.38 -1.3% | Cardano (ADA) $0.35 -3.681% | Bitcoin (BTC)

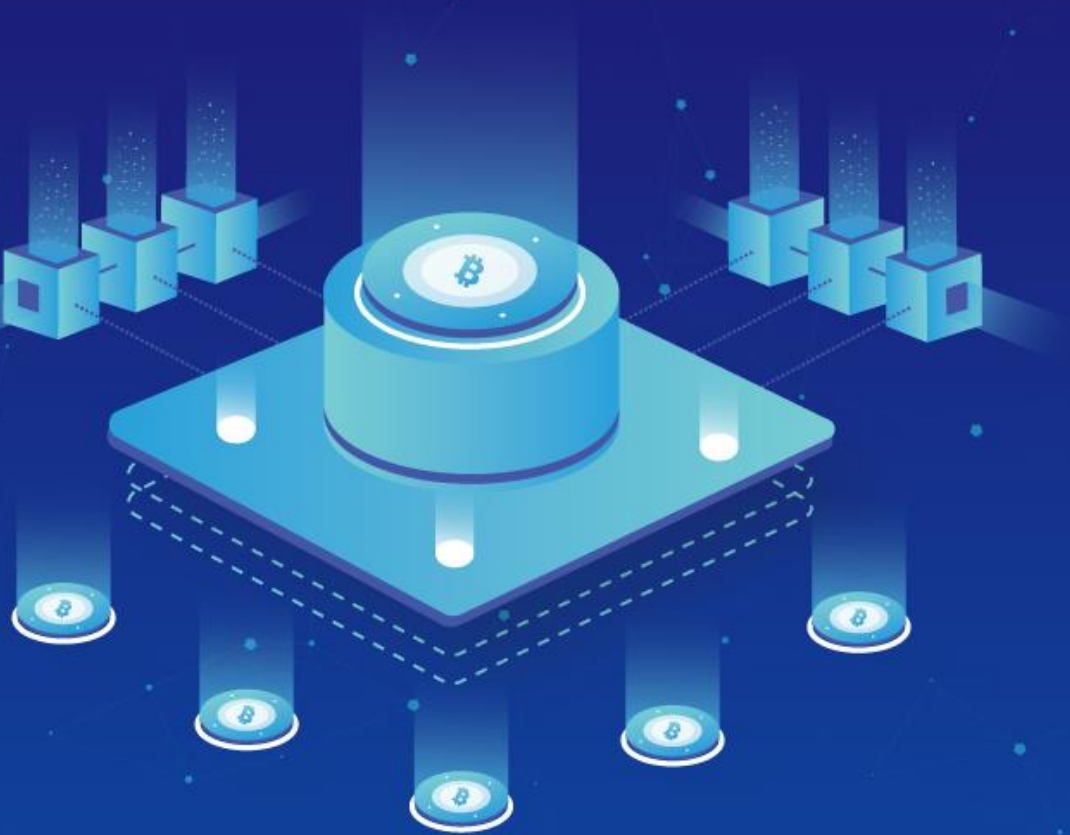
Golden Eagle

Investments

Golden Eagle Investments allows you to copy all cryptocurrency investors that you think you can make profit from. You don't need to have knowledge about cryptocurrencies or trading at all.

WHITEPAPER →

BUY TOKEN NOW →



Decentralized criminal network

The binary options “business model” lives on in fraudulent crypto investment websites

- Criminal organizations create fake investment websites from templates and generate unique branding
- Partners operate call centres with multiple websites
- Call centre staffing involves forced labour in some instances
- Other involved actors include law firms, software developers, webhost providers, domain registrars, marketing firms, payment processors and crypto trading platforms

Europol Spotlight: Cryptocurrencies

Fraudsters create websites devoted to cryptocurrency investments or advertise lucrative investments and encourage investors to create accounts on online trading platforms. Alternatively, operators from established callcentres offer opportunities requiring small initial investments that end in high profits. The victims have the impression to be able to monitor their investments thanks to internet platforms. However, the whole process is a deception. Brokers try to obtain information about the victims using social engineering techniques, while gaining their trust with simulated trading activities.

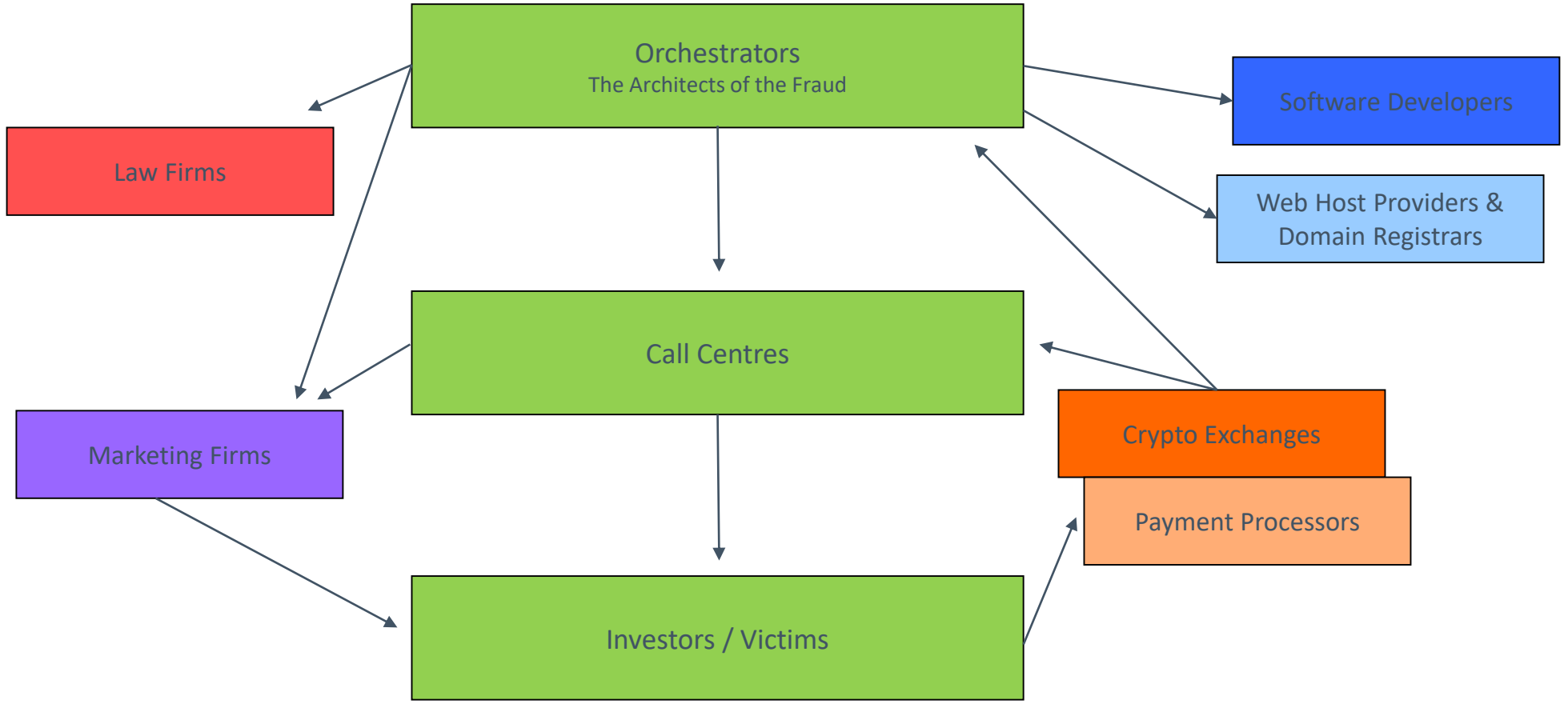
Europol Spotlight - Cryptocurrencies: Tracing the Evolution of Criminal Finances, at page 13

Fraudulent crypto-investment websites

These schemes exist within a complex, multi-national and multi-regulatory ecosystem

- Dispersed responsibility for regulating cryptocurrencies, the internet and investment fraud among many regulatory and law enforcement agencies across Canada and internationally
- Pyramid, Ponzi and Multi-Level Marketing schemes are all in play, resulting in “investors” bringing in more victims
- Canadians are being heavily targeted by these fraudulent websites

Fraudulent Investment Website Ecosystem



How do these websites reach victims?

There is a scam outreach for everyone!

- Social media advertising
- Internet searches
- Account hacking
- Romance scam
- Emails
- Celebrity endorsements
- Texts
- Referral bonuses
- Infomercial
- Phone calls

Canadian Anti-Fraud Centre

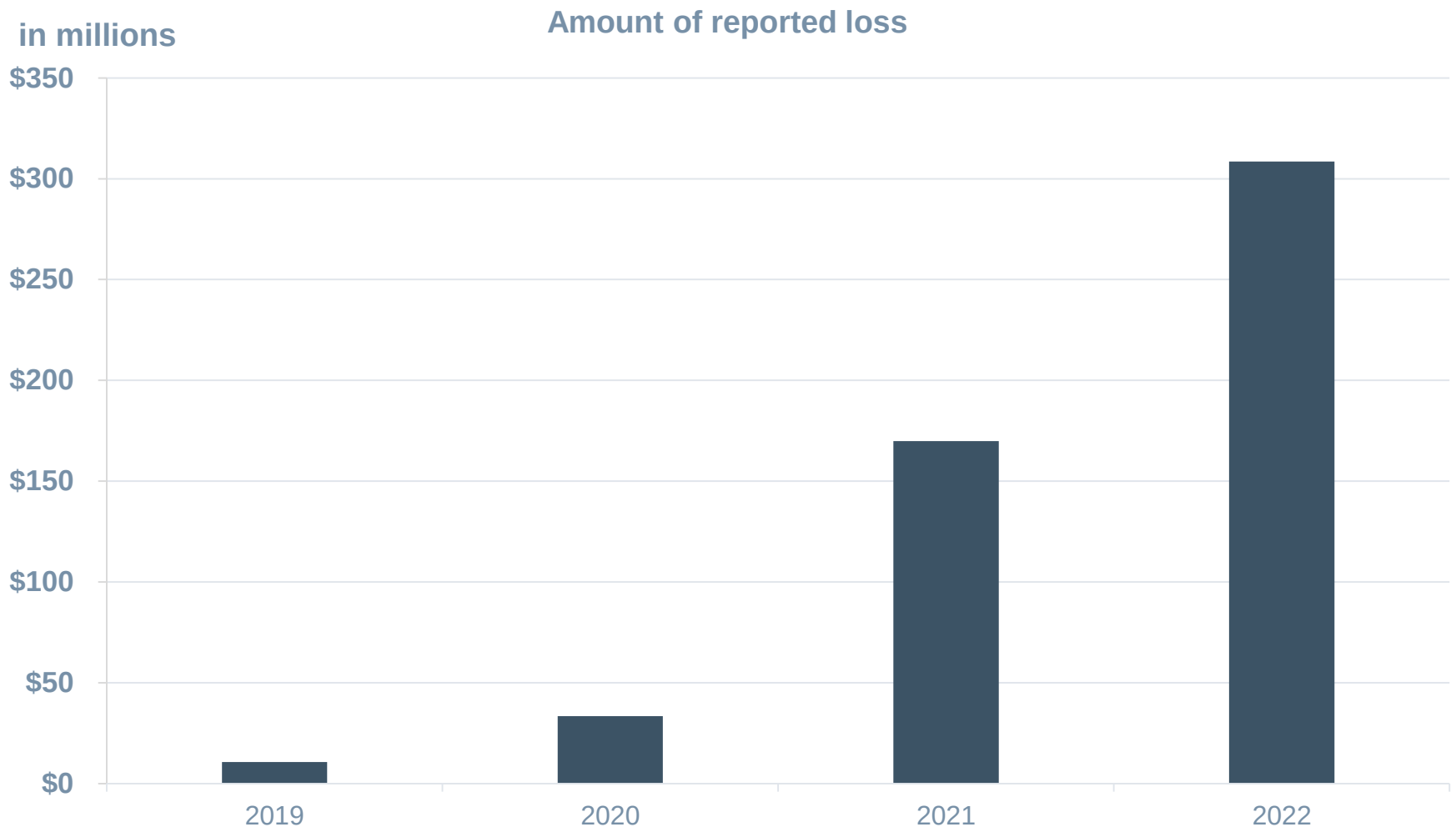
Reports of investment fraud now exceed reports of all other types of fraud *combined*

- The vast majority of these investment frauds are crypto-related
- CAFC estimates only 5-10% of fraud is reported

	2020	2022	% change
Reported losses to investment fraud	$33.5 million	$308.6 million	**820%**
Number of reported victims of investment fraud	428	4,251	**893%**
Total reported of all types of fraud	$165 million	$531 million	**222%**

CAFC Reports of Investment Fraud - Victims

CAFC Reports of Investment Fraud - $



U.K. Crypto Scams

Action Fraud reports £226 million lost (Oct 2021-Sept 2022)

- The Telegraph, 24 Jan 2023

> **Britons conned out of life savings by crypto scam run from lawless compounds in Southeast Asia**

- The Guardian, 29 Jan 2023

> **'Everything is fake': how global crime gangs are using UK shell companies in multi-million pound crypto scams**

Consequences of these scams

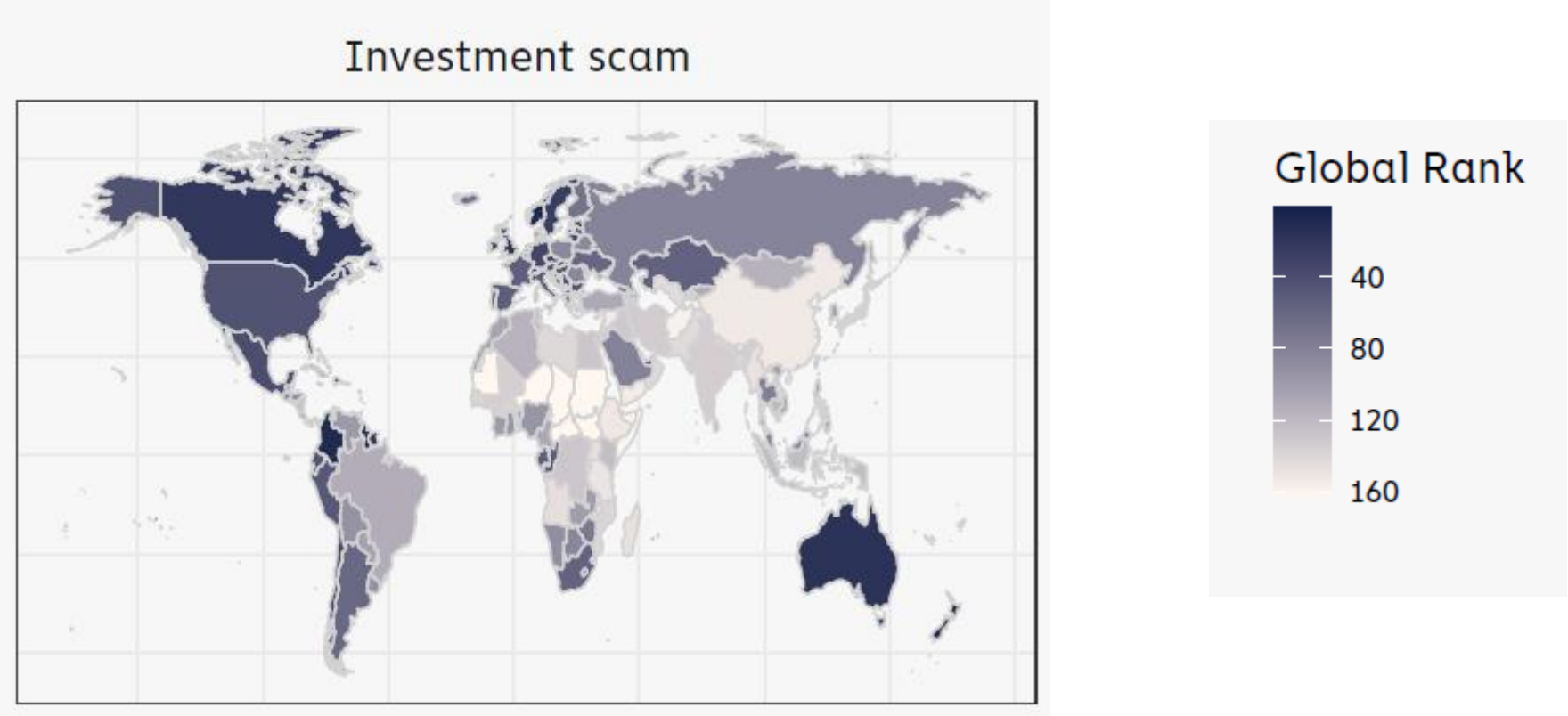
Financial

- Financial loss
- Indebtedness
- Bankruptcy
- Capital markets: opportunity loss for legitimate investments
- Enforcement costs

Other

- Loss of trust in people
- Loss of trust in investing
- Relationships break down
- Mental health impacts – guilt, shame, embarrassment, depression
- Suicides

Canada and U.K. among hardest hit countries for investment scams



Source: Chainalysis, *The 2023 Crypto Crime Report*, February 2023

By 2021 whack-a-mole became much harder

By 2022 it became impossible

The pillars of public protection remain

Policy & Law

Educate

Detect

Disrupt

Investigate

Prosecute

Deter

Current response in Canada by securities regulators

CSA members are engaging in investor education efforts

- CSA Investor Alert Jan. 17, 2022 CSA Investor Alert Fraudulent Investment Websites
- Caution/warning lists by CSA members CSA Investor Alerts

Year	# of CSA Investor Alerts
2023 YTD	133
2022	**510**
2021	197
2020	130

Current response in Canada by securities regulators

CSA and its members are engaging in investor education

- CSA publishes list of authorized CTPs CSA Authorized CTPs
- CSA Investor's Guide: Cryptocurrencies
- Search engine marketing (SEM) campaign in effect
- CSA social media advertising campaign

Current response in Canada by securities regulators

CSA members engage in coordinated detection & disruption

- CSA Investment Fraud Task Force - share intelligence and strategize on disruption
- identify points of leverage in the ecosystem:
  - request removal by webhost providers of identified websites
  - contact payment providers to seek assistance in detecting and preventing payments to the bad actors, and to identify potential victims
- share intelligence with other regulators and law enforcement agencies
- pursuing collaboration with securities regulators in Europe

International response

U.K. Financial Conduct Authority (FCA)

- FCA Warning List
- 1,800 potential scam warnings in 2022 (400 more than previous year)
- Removed or amended 8,000 potentially misleading adverts in 2022 (14 times more than previous year)
- FCA ScamSmart Tool

IOSCO – Investor Alerts Portal

Action Fraud is warning the public to remain vigilant when making investments, as criminals cheat hundreds of millions of pounds out of victims through cryptocurrency fraud.

International response

Europe

- Coordinated law enforcement action in Europe leading to arrests and searches of call centres
- Europol news release

- Analysis of newly registered domain names to identify new fraudulent websites, based on URL and site content

Despite efforts, investor losses are rapidly increasing

Challenges:

- These websites have a short shelf life; by the time victimization is reported, the website may no longer exist, making investigation difficult
- New fraudulent investment websites are being spawned daily
- Regulatory and law enforcement agencies are grappling with oversight responsibilities / authority re: crypto
- Pursuing traditional enforcement action against the perpetrators is resource-intensive and often ineffective due to offenders being outside the country

Challenges (cont'd):

- Often not feasible to have these websites taken down:
  - Registrant anonymity
  - Hosting Provider anonymity
  - Resistance from Hosting Providers, Registrars and Registries (intermediaries)
  - Limited resources and expertise
  - Cross jurisdictional (multiple jurisdictions outside Canada)
  - Complex set-ups
- Disruption efforts are time-consuming

Opportunities for the research community?

Use of technology and analytics to:

- Detect and predict newly spawned fraudulent investment websites
- Quickly and efficiently alert public to the new websites
- Allow public to reliably check trustworthiness of an investment website
- Find cost-effective means to place warnings on scam websites
- Improve search results of warning lists (FCA, CSA, IOSCO) – defeat counteracting measures

Opportunities for the research community?

Use of technology and analytics to:

- Build tools to aid in the detection of **networks** of fraudulent investment websites, beyond relying on content or visible features
  - e.g. Chainalysis uses blockchain analysis to identify scam networks based on deposit address overlap
- Other ideas?

Discussion