Privileged Access

The Threat of Insider Trading

On The Dark Web & Encrypted Platforms



Agenda

- Introduction & Background
- Unprecedented Technological Change
- Insider Trading Investigations and Challenges
- Technology Challenges
- What Is The Dark Web
- Cryptocurrency
- Encrypted Messaging Apps
- Cases
- Technology Benefits
- Summary
- Q&A

Introduction & Background



“All Of Our Exalted Technological Progress, Civilization For That Matter, Is comparable To an Axe In The Hand Of A Pathological Criminal. ”

Albert Einstein

Unprecedented Technological Change

Fraudulent crimes are rising

Motivation = financial gain

Use of technology for an edge

Insider Trading covert on encrypted platforms and Dark Web



Protecting
The Integrity Of Our Markets

Financial markets require fair & level playing field

Trust is implicit between a company & investors

Insider Trading erodes that trust

Undermines confidence in the financial system

Insider Trading Investigations and Challenges

Profitable trading based on **Material, Non-Public Information**

Two statutes define securities fraud – Title 15 (Exchange Acts of 1933 and 1934), and Title 18 (Sarbanes Oxley)

Title 15 Case Law:

-*Dirks* (Breach of fiduciary duty, benefit to tipper)

-*Newman* (Personal benefit, knowledge of benefit by tippee)

-*Salman* (Expanded personal benefit definition)

Title 18 – A "scheme to defraud". *Blaszczak* decision held Title 18 1348 does **NOT** require tippee's knowledge of the benefit to the tipper

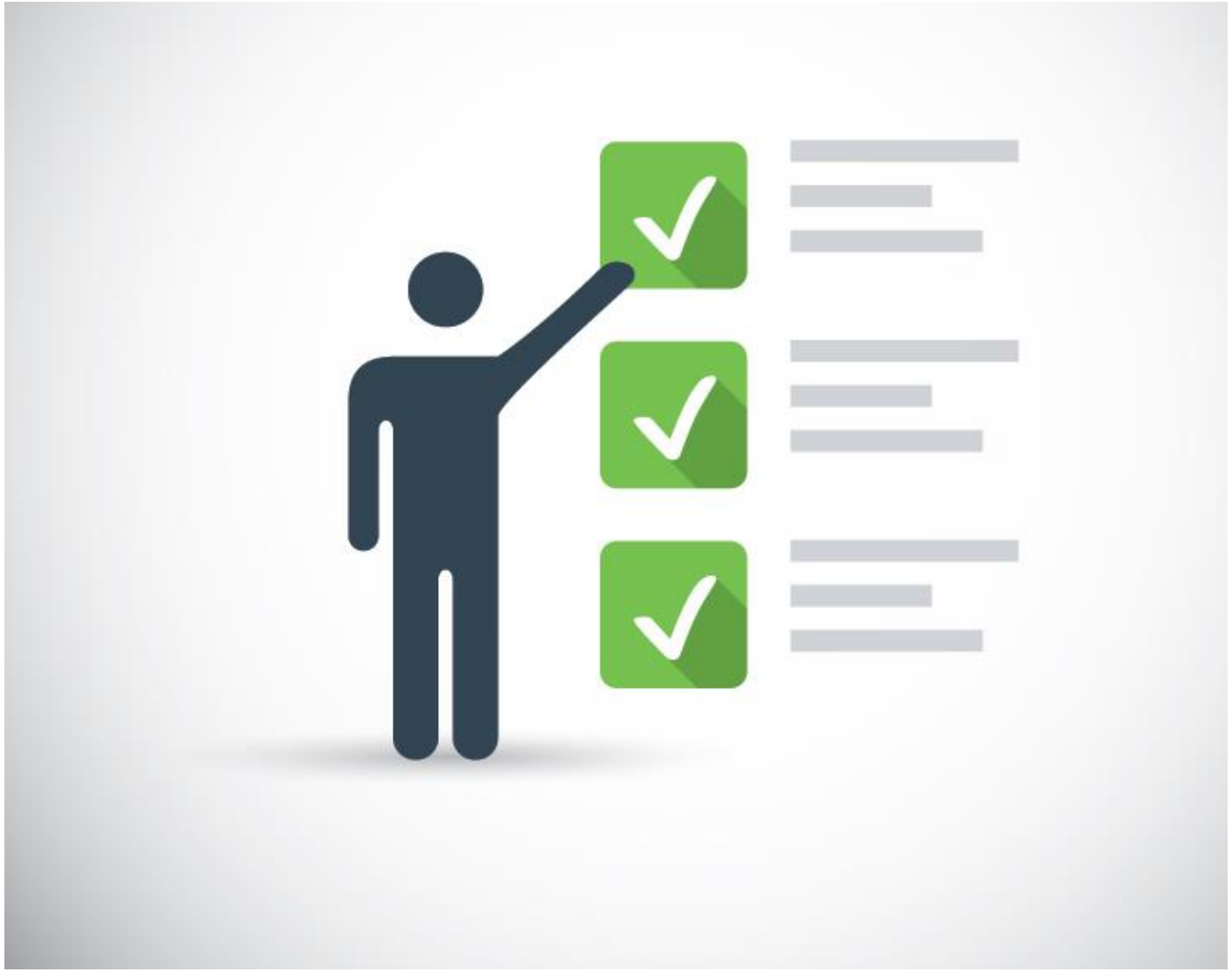
Congress continues to propose an insider trading statute

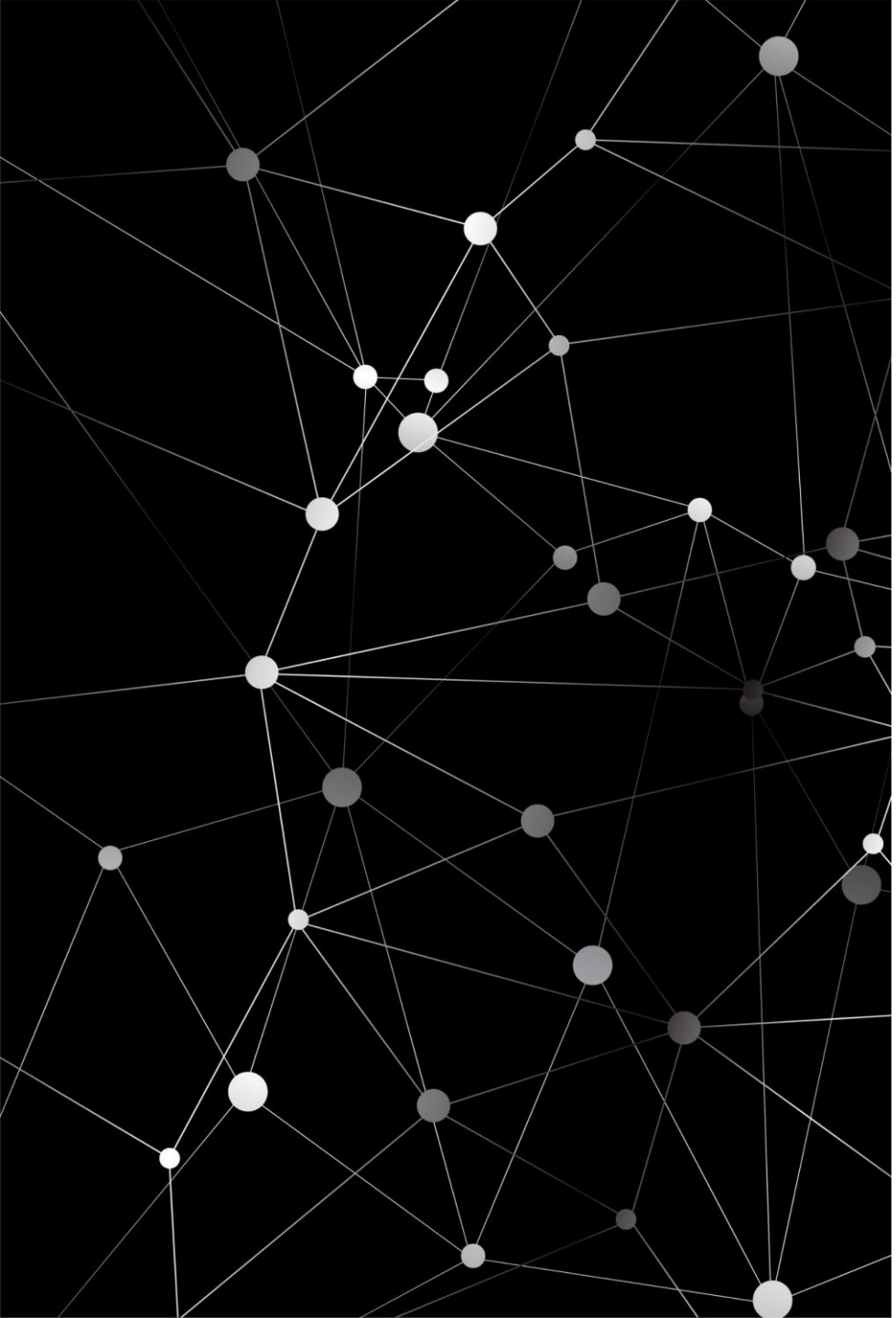
Technology Challenges

Dark Web, Encrypted Platforms & Messaging, & Cryptocurrency

Poll Question #1

Is It Illegal To Access The Dark Web?





What Is The Dark Web?

Encrypted online content not indexed by conventional search engines that requires specific configuration, tools, or authorization to access (Tor Browser)

Privacy and anonymity for exchanging proprietary business information or communication by groups such as political activists

Criminals leverage the Dark Web to hide their illegal activity

Web Overview

SURFACE WEB

Known as “Clearnet”

- Indexed & Easily Searchable
- Wikipedia, Google, Bing
- IoT

4%
Content of the Web

DEEP WEB

Content that cannot found by conventional search engines

- Government
- Human Resource Information
- Corporate Intranets
- Financial Information
- Not indexed, more difficult to find
- Medical records
- Academic information

90%
Content of the Web



DARK WEB

The encrypted network that exists between TOR Services and their Clients such as anonymous or hidden marketplaces.

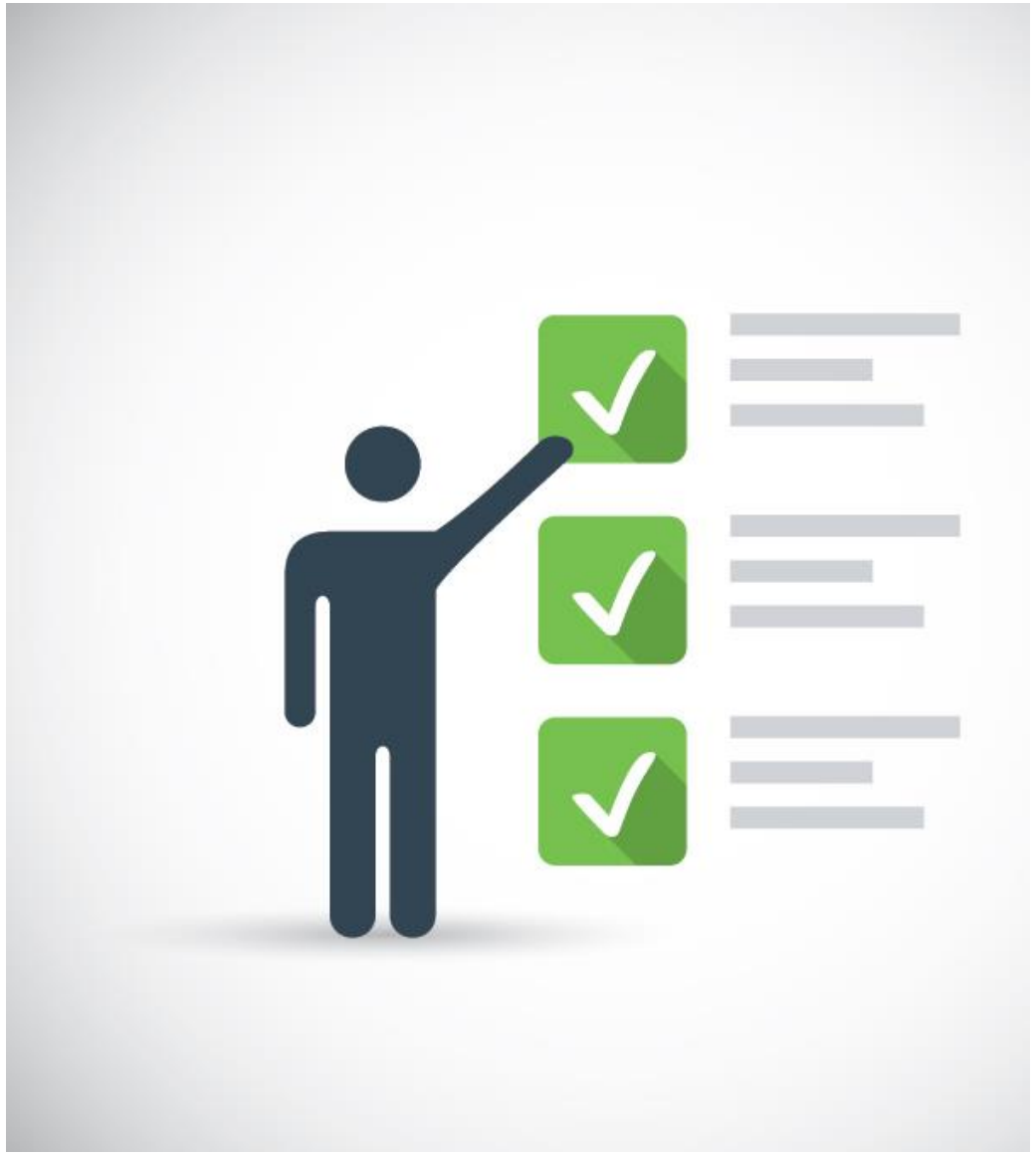
- Not indexed
- Tor encrypted sites
- ZeroNet
- IRC
- Private Communications

6%
Content of the Web

Poll Question #2

TRUE OR FALSE?

The U.S. Navy is responsible for creating Tor.



The Onion Router (Tor)

Free and open-source software for enabling anonymous communication

The name is derived from an acronym for the original software project name "The Onion Router"

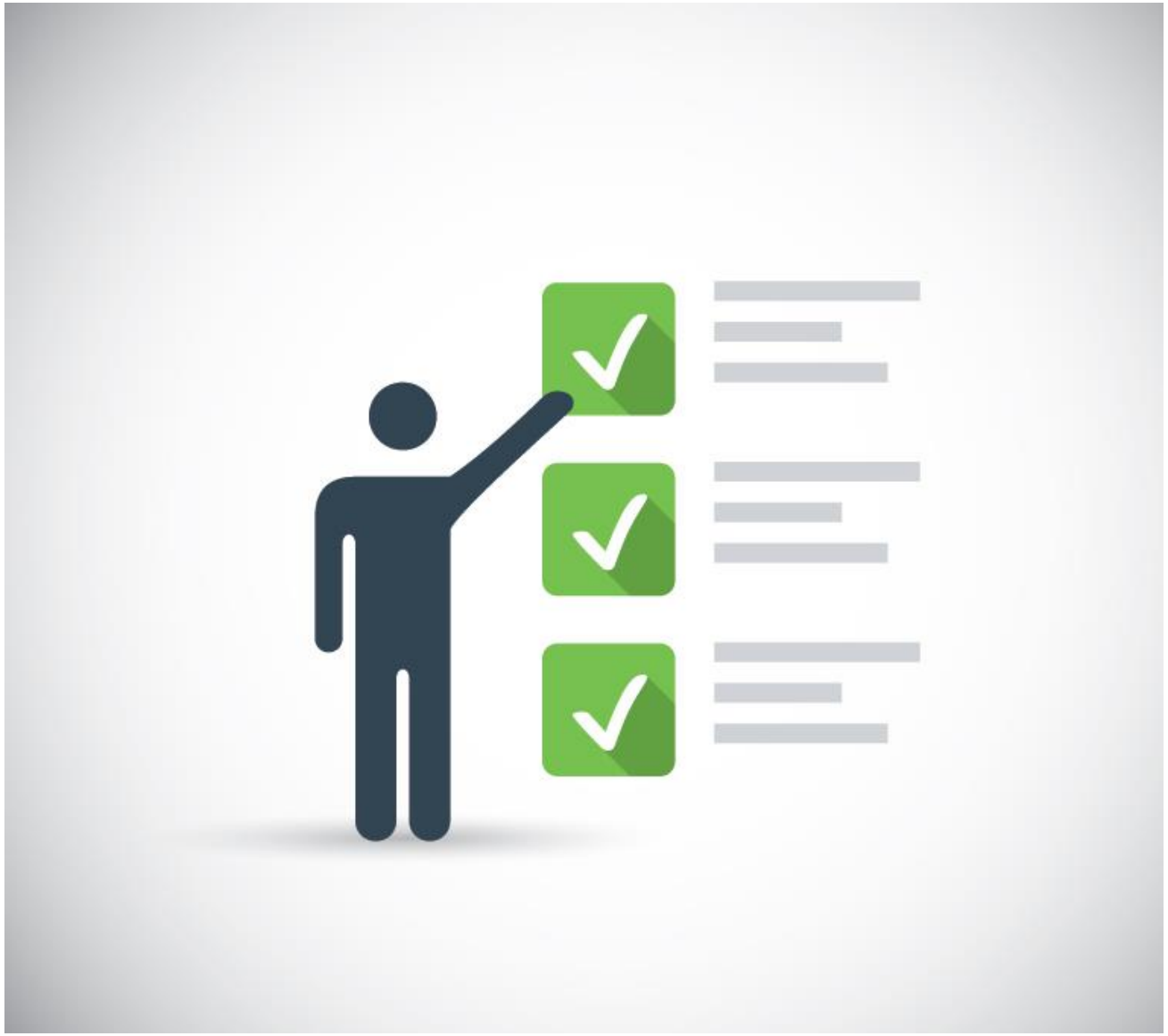
Tor directs Internet traffic through a free, worldwide, volunteer overlay network consisting of more than seven thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis.



Poll Question #3

TRUE OR FALSE?

The first commercial Bitcoin transaction was for pizza.



Cryptocurrency

Cryptocurrencies are a tokenized form of digital currency that use cryptography for their creation and security.

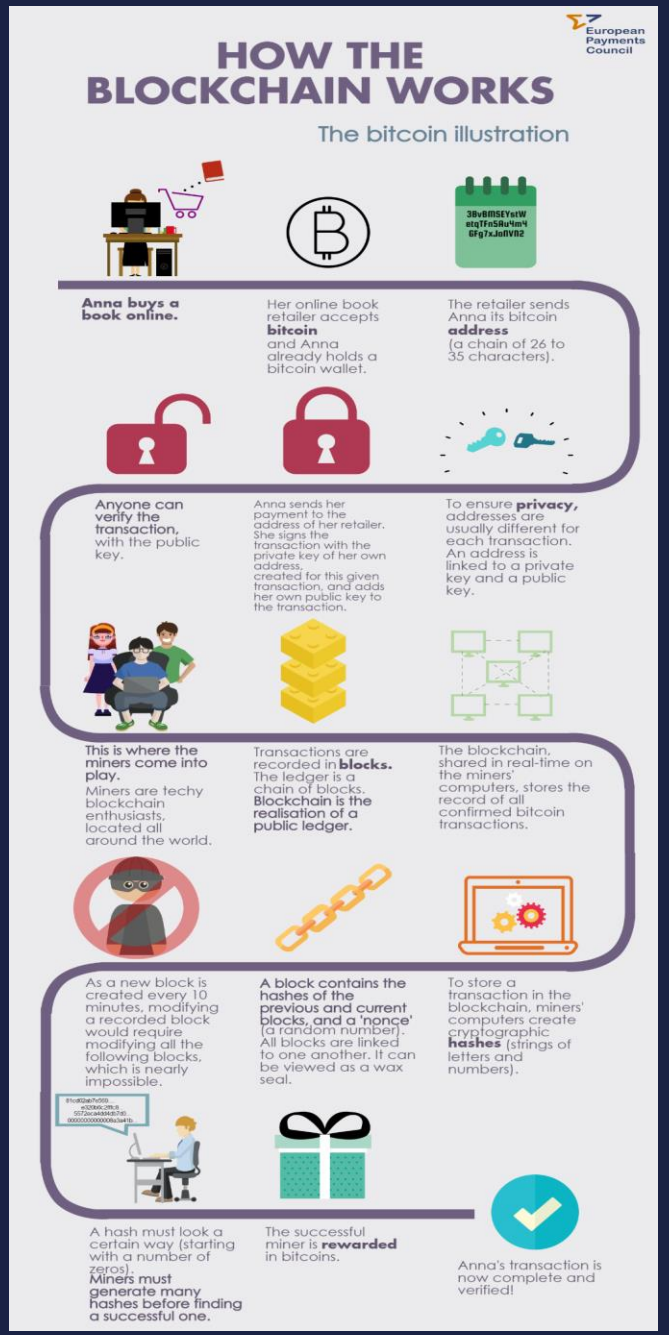
In 2009 Satoshi Nakamoto mined* the first Bitcoin, at the time, perceived to be an untraceable cryptocurrency.

The appeal of using untraceable/anonymous currency led to a rise in cryptocurrency use on the darknet for money laundering and other criminal activity.

*Mining is the process used to create a cryptocurrency.



How The Blockchain Works



Cryptocurrency: Tumblers and Mixers

There is a paid service that's known as a cryptocurrency mixer. This service splits and mixes coins with other coins to hide them. In a typical transaction, Jennifer might send one Bitcoin to Paul, who then sends the same Bitcoin to Dora, who sends it elsewhere. These transactions are visible on the blockchain through wallet addresses.

For those who are trying to hider their transaction activity, they leverage crypto mixers.

There are marketplaces for these services on the Dark Web.

Cryptocurrency mixing takes the original coin, splits it with other coins, and returns to random addresses for random, different amounts, fractions of the original quantity (adding up to the same original total).One transaction could now appear as four or more transactions for various amounts.

While this does obscure transactions, it doesn't render them untraceable

Insider & Threat Actor On A Dark Web Forum

"On the forum, the attacker explains the approach to a potential collaborator, indicating that he needs direct access to computers that access accounts and handle wire transfers, and that he offers to pay "7 figures on a weekly basis" for continued access."


[redacted]: I am going to have to check it more thoroughly, but specifically I can say the branch I work at has zero security awareness so I have quite a free access

(17:19:11) **lacazatte@dukgo.com/Home:** Great

(17:19:18) **lacazatte@dukgo.com/Home:** When will i hear from you?

(17:20:37)

[redacted]: Well its a 9 to 17 work, so I'm guessing in the evening

(17:20:53) **lacazatte@dukgo.com/Home:** I need access to the computers that handle transfers. If you can't get direct access to those computers, a lesser one will do. It means i'll have to escalate my privilege to the right computer, but if you give me direct access to it, that would be great.

(17:21:00) **lacazatte@dukgo.com/Home:** wire transfers.

(17:21:28)

[redacted]: got it, I don't think it will be a problem honestly

(17:21:53) **lacazatte@dukgo.com/Home:** and accounts. I don't transfer funds from the accounts of customers. I mainly create new ones stealthily. Most times no one knows what happened for a very long time.

(17:22:37)

[redacted]: fuck! that's genius! it is quite stealthy

[redacted]: how much money do I get from it?

(17:23:31) **lacazatte@dukgo.com/Home:** There's no limit to be honest with you.

(17:24:00) **lacazatte@dukgo.com/Home:** As long as i continue to have access you can earn 7 figures on a weekly basis.

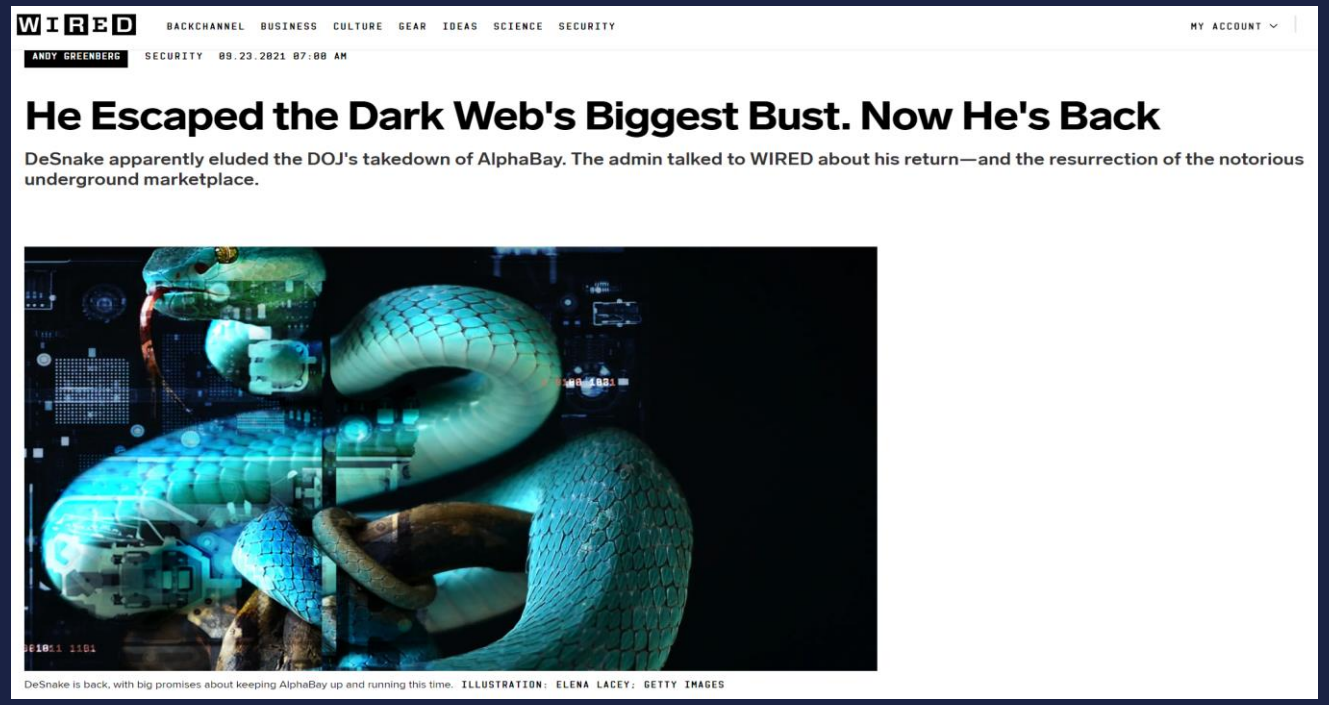
(17:24:39)

[redacted]: I'll talk to you tomorrow evening

(17:24:56) **lacazatte@dukgo.com/Home:** Alright

Source: Monetizing the Insider, The Growing Symbiosis of Insiders and the Dark Web, REDOWL, Insights

AlphaBay Relaunch



WIRED BACKCHANNEL BUSINESS CULTURE GEAR IDEAS SCIENCE SECURITY MY ACCOUNT

ANDY GREENBERG SECURITY 09.23.2021 07:00 AM

He Escaped the Dark Web's Biggest Bust. Now He's Back

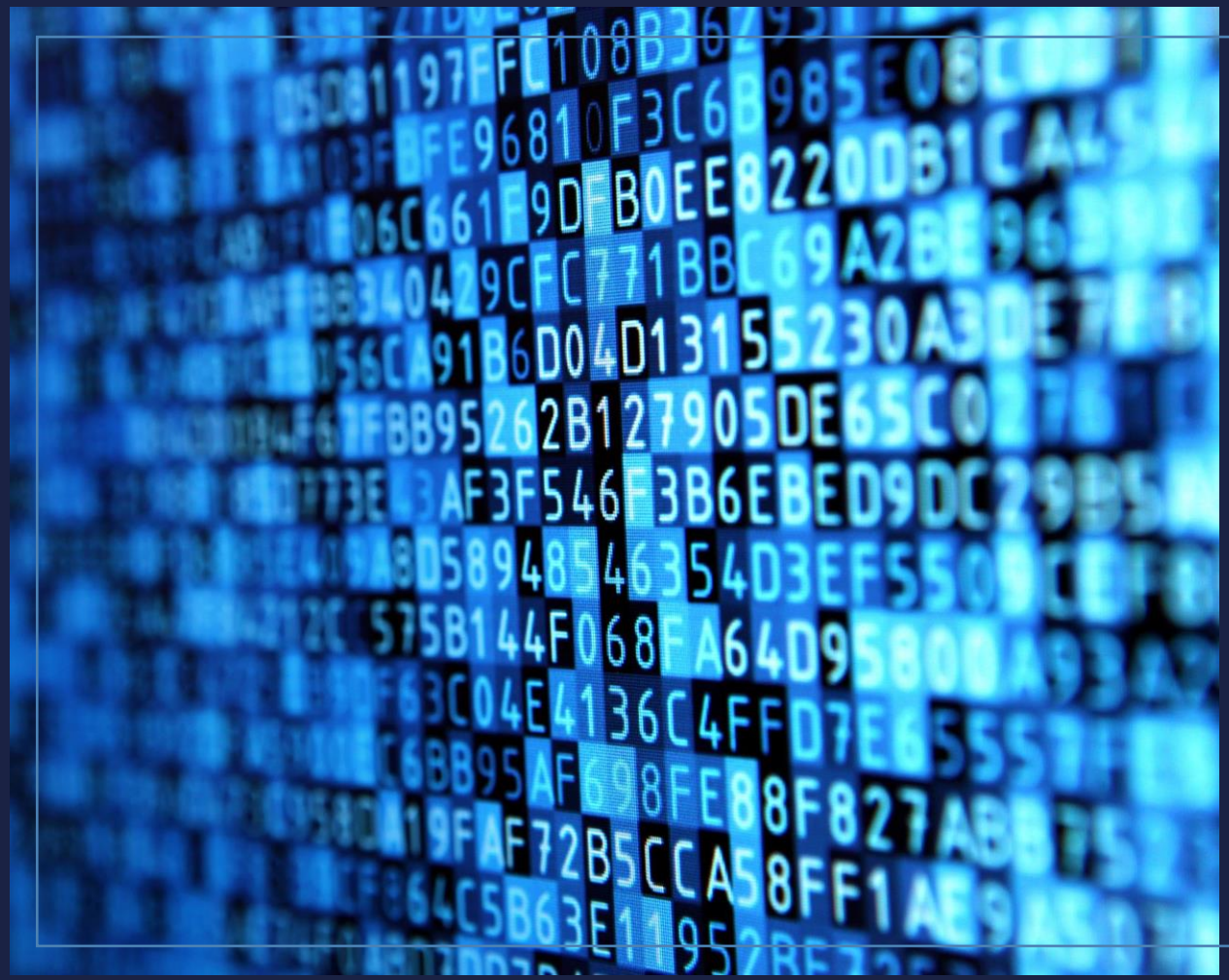
DeSnake apparently eluded the DOJ's takedown of AlphaBay. The admin talked to WIRED about his return—and the resurrection of the notorious underground marketplace.

DeSnake is back, with big promises about keeping AlphaBay up and running this time. ILLUSTRATION: ELENA LACEY; GETTY IMAGES

"The revived version of AlphaBay, for instance, allows users to buy and sell only with the cryptocurrency Monero, which is designed to be far more difficult to trace than Bitcoin, whose blockchain has proven to sometimes allow powerful forms of financial tracking. AlphaBay's dark web site is now accessible not only via Tor, like the original AlphaBay, but also I2P, a less popular anonymity system that DeSnake encourages users to switch to. He repeatedly described his wariness that Tor may be vulnerable to surveillance, though he provided no evidence."

Wired, Interview with DeSnake, August 2021

https://www.wired.com/story/alphabay-desnake-dark-web-interview/



Encrypted Messaging Apps

From The Dark Web To Encrypted Messaging Apps

In 2017 there was a surge of activity in Dark Web marketplaces for Insider Trading and other Corporate financial crime

Following the seizure of some of these large, marketplaces, and the evolution of encrypted messaging apps, a shift began to move to using these platforms for operations.

Telegram and WhatsApp, promise end-to-end encryption and include tools for forwarding messages to larger groups of people while remaining anonymous.



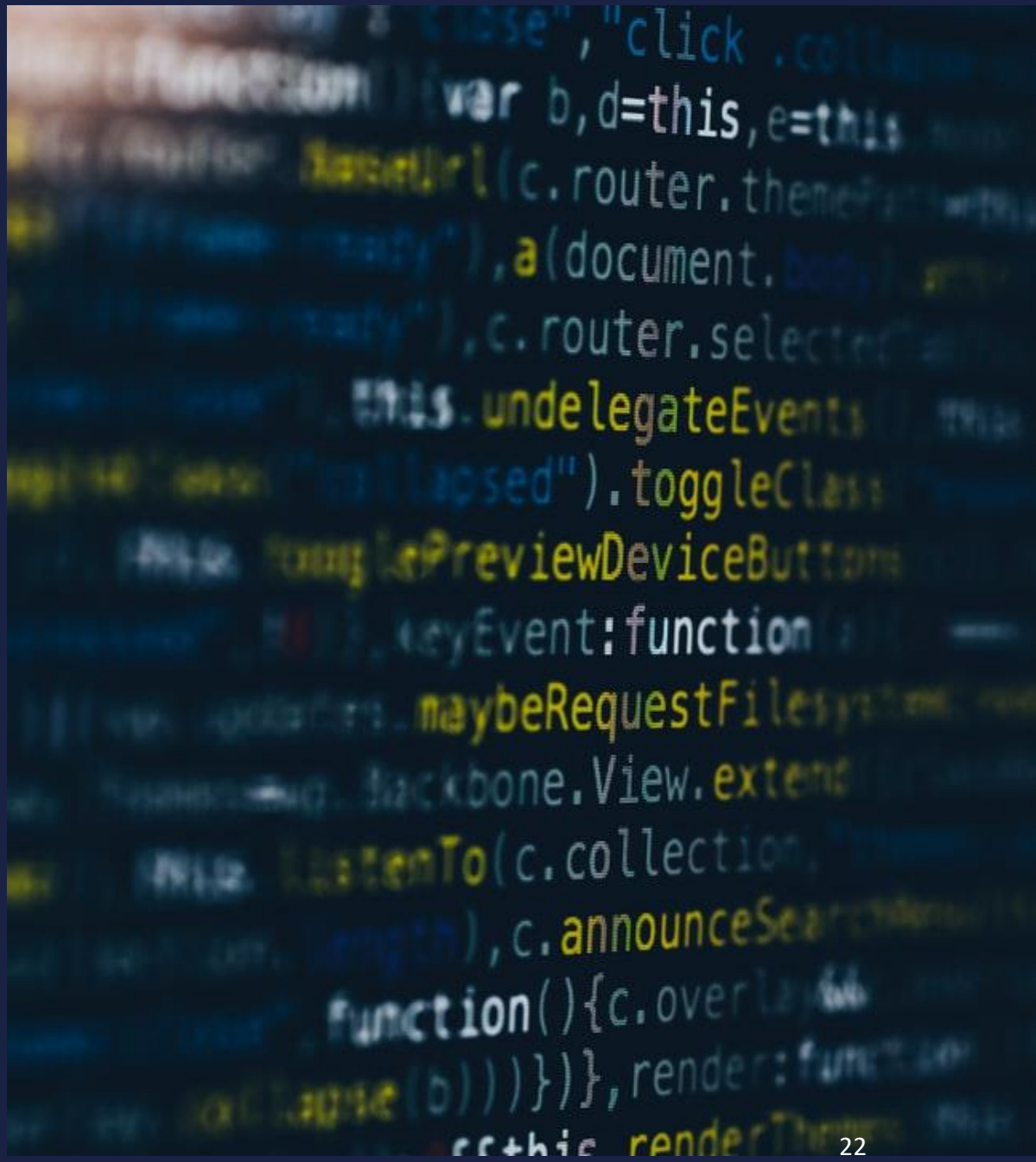
Encrypted Messaging Apps

Encryption requires an end-user device to access messages on these apps – messages from the server are unreadable

Many of these services are hosted in countries unfriendly to US Law Enforcement

Some of these will provide access to unencrypted messages – but they will notify the end users when their information is provided

This is not unique to insider trading – “Going Dark” is an issue across all crime threats



Examples of Encrypted Messaging Apps

silent circle

ProtonMail



WhatsApp

wickr

Telegram

Key Takeaways

The Dark Web refers to encrypted online content that is not indexed by conventional search engines.

Specific browsers, such as Tor Browser, are required to reach the Dark Web.

The Dark Web pulls up sites using information that isn't indexed online, such as bank accounts, email accounts, and databases.

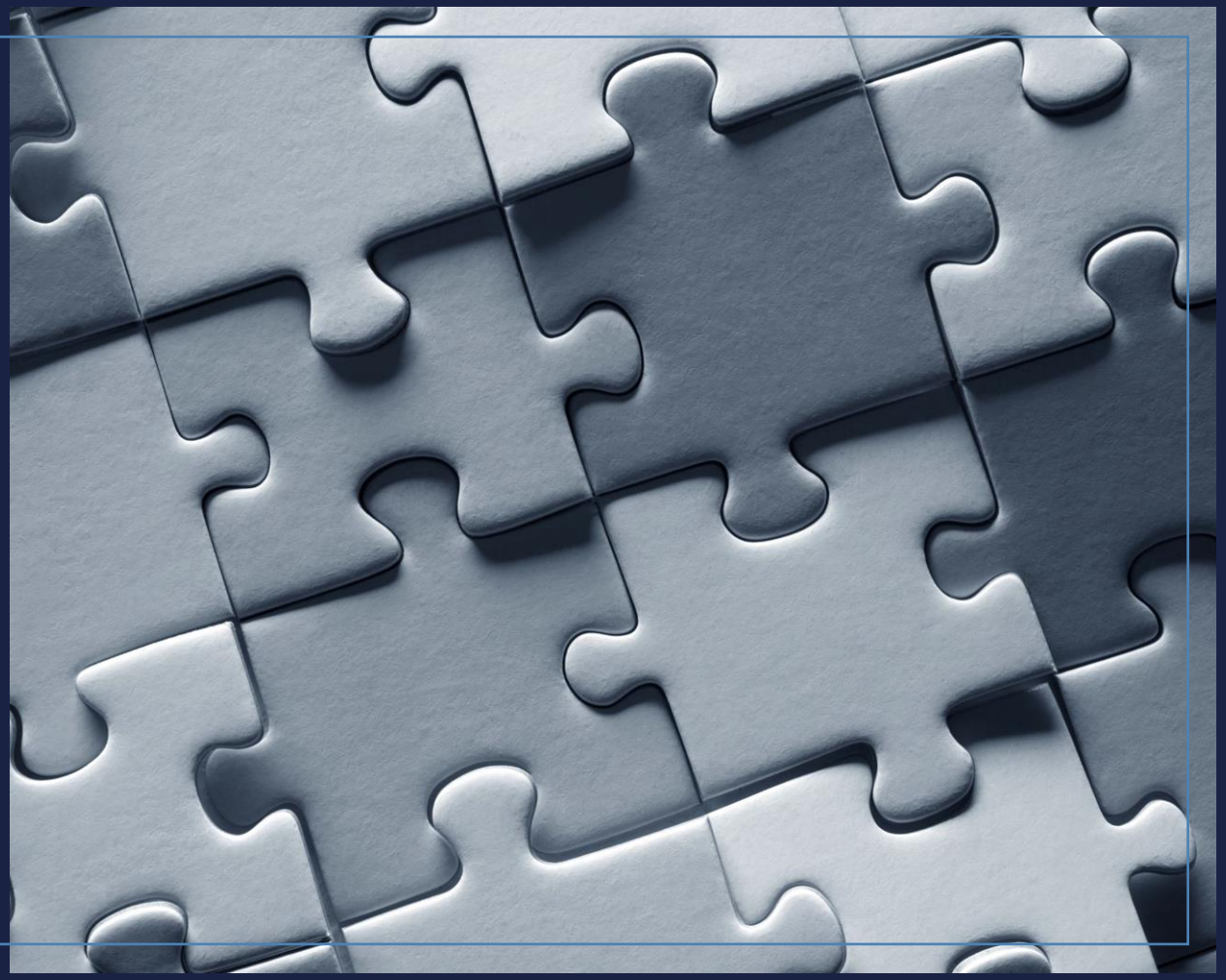
People use the Dark Web to maintain their privacy and freely express their views

Criminals also use the Dark Web to remain anonymous and conduct illicit activity .

Criminals seek new technology out to maintain anonymity and following the seizure of several Dark Web marketplaces, criminals are moving to encrypted messaging apps & forums.

Anonymous and untraceable transactions are appealing to criminals, making cryptocurrencies the currency of the Dark Web markets.

Cases





Challenges

The challenges posed by the encryption and anonymity features of software used on the dark web & across encrypted messaging apps

Acquiring technical data and turning it into evidence that can be conveyed in a way that will be understood by a jury

Shifting operations - bad actors adapt quickly and move quickly to evade law enforcement

Multijurisdictional nature of Dark Web crimes

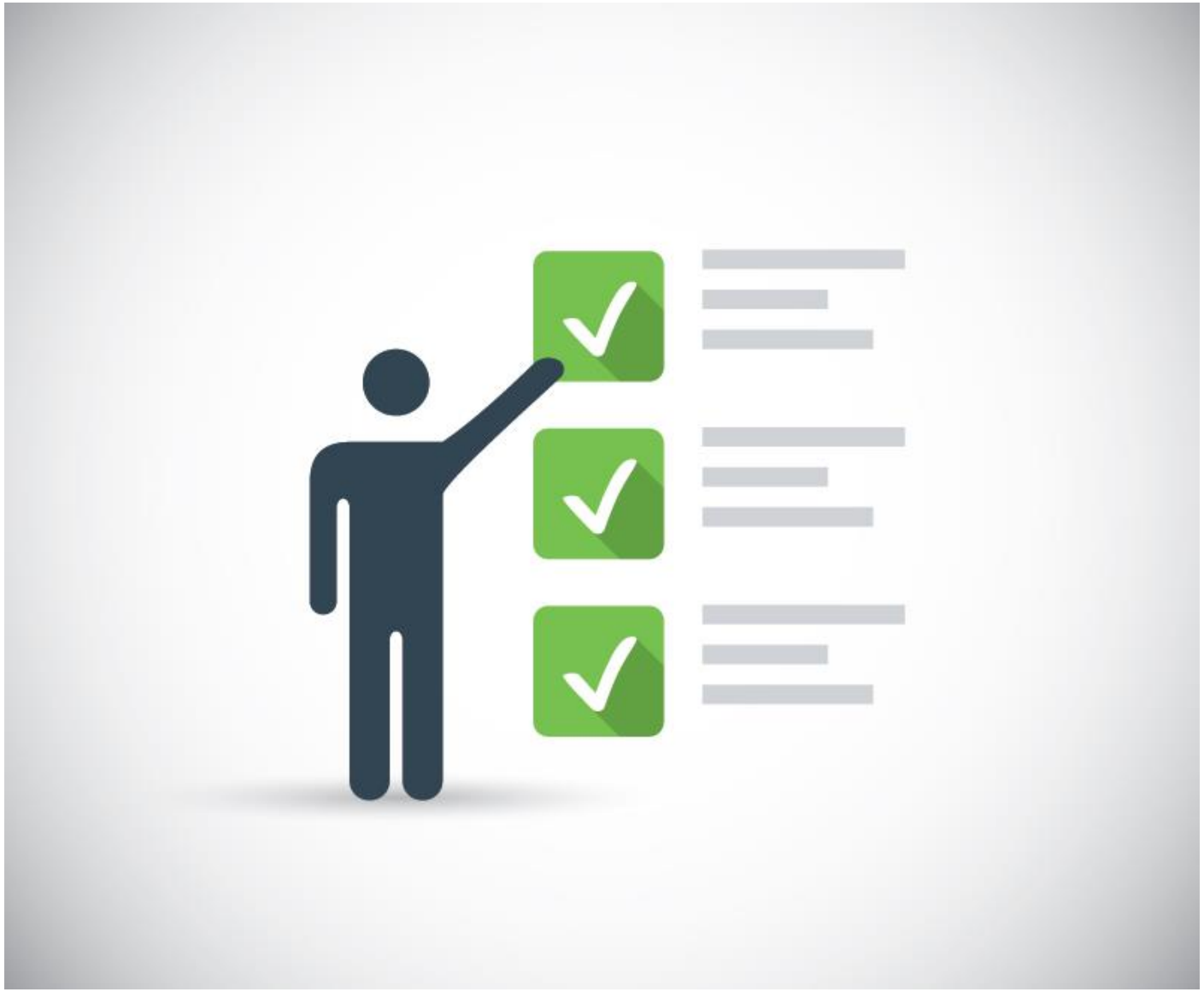
Crimes committed in countries who don't cooperate with the U.S. pose a challenge (Dark Web marketplaces like the AlphaBay relaunch)

Following the money - tracking cryptocurrency

Poll Question #4

TRUE OR FALSE?

In 2021 the SEC took the first action against an individual for fraudulently offering insider stock trading tips on a darknet marketplace



MillionaireMike

In 2021 The SEC took their first action the first action against an individual for fraudulently offering insider stock trading tips on a darknet marketplace.

That individual, James Roland Jones, worked at SpaceX and was known on the Dark Web by the Moniker, MillionaireMike.

The 33-year-old SpaceX engineer pleaded guilty to conspiracy to commit securities fraud.

A criminal complaint by the Justice Department details the investments that Jones made in the spring of 2017 leading to this action.



Apostolos Trovias aka “TheBull”

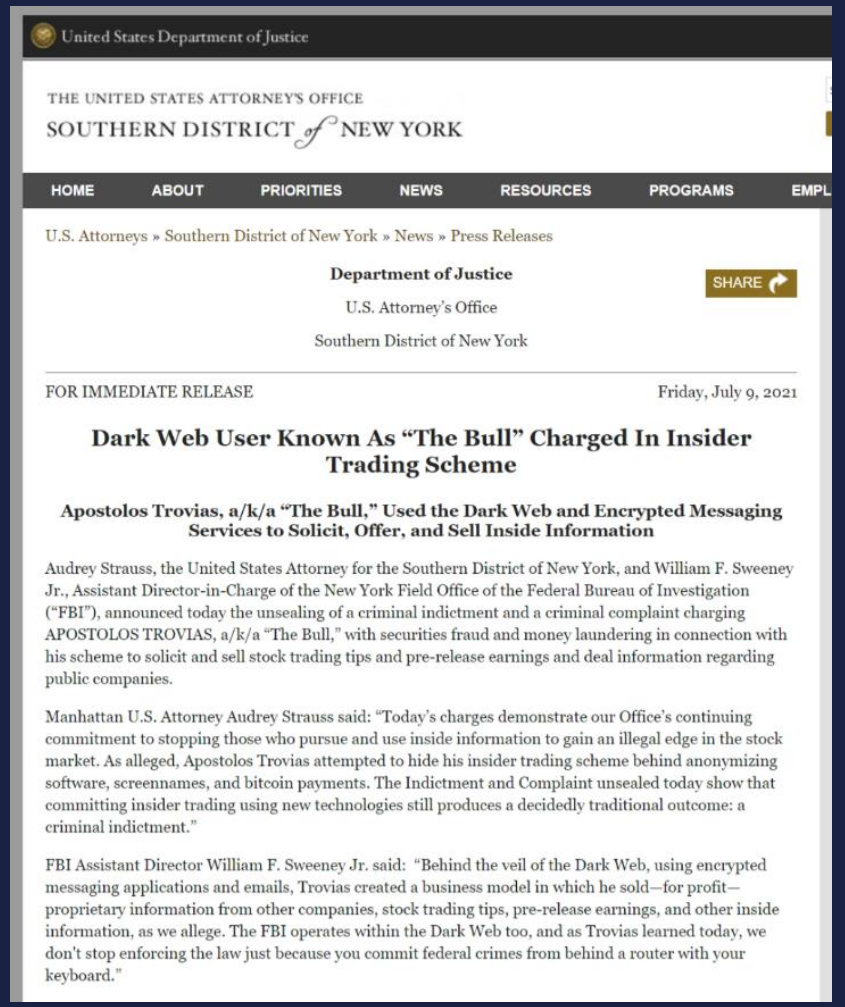
FBI New York received a referral from a private sector partner regarding the potential sale of inside information on the Dark Web

An individual using the handle “TheBull” was selling a subscription-based MNPI service, with the ability to purchase additional MNPI for larger amounts

TheBull had several customers – one happened to be an undercover FBI Agent

After the shutdown of AlphaBay, TheBull wanted to start his own MNPI marketplace

In July 2019, Apostolos Trovias, aka “TheBull” was arrested in Peru after being indicted in SDNY on securities fraud charges



United States Department of Justice

THE UNITED STATES ATTORNEY'S OFFICE
SOUTHERN DISTRICT of NEW YORK

HOME ABOUT PRIORITIES NEWS RESOURCES PROGRAMS EMPL

U.S. Attorneys » Southern District of New York » News » Press Releases

Department of Justice
U.S. Attorney's Office
Southern District of New York

SHARE

FOR IMMEDIATE RELEASE — Friday, July 9, 2021

Dark Web User Known As “The Bull” Charged In Insider Trading Scheme

Apostolos Trovias, a/k/a “The Bull,” Used the Dark Web and Encrypted Messaging Services to Solicit, Offer, and Sell Inside Information

Audrey Strauss, the United States Attorney for the Southern District of New York, and William F. Sweeney Jr., Assistant Director-in-Charge of the New York Field Office of the Federal Bureau of Investigation (“FBI”), announced today the unsealing of a criminal indictment and a criminal complaint charging APOSTOLOS TROVIAS, a/k/a “The Bull,” with securities fraud and money laundering in connection with his scheme to solicit and sell stock trading tips and pre-release earnings and deal information regarding public companies.

Manhattan U.S. Attorney Audrey Strauss said: “Today’s charges demonstrate our Office’s continuing commitment to stopping those who pursue and use inside information to gain an illegal edge in the stock market. As alleged, Apostolos Trovias attempted to hide his insider trading scheme behind anonymizing software, screennames, and bitcoin payments. The Indictment and Complaint unsealed today show that committing insider trading using new technologies still produces a decidedly traditional outcome: a criminal indictment.”

FBI Assistant Director William F. Sweeney Jr. said: “Behind the veil of the Dark Web, using encrypted messaging applications and emails, Trovias created a business model in which he sold—for profit—proprietary information from other companies, stock trading tips, pre-release earnings, and other inside information, as we allege. The FBI operates within the Dark Web too, and as Trovias learned today, we don't stop enforcing the law just because you commit federal crimes from behind a router with your keyboard.”

Technology Benefits

Detection

While technology provides opportunities for criminals to conduct their activity shrouded in secrecy, technology innovation also offers new capabilities for regulators to detect insider trading and law enforcement to see illegal activity and enforce the law. Technological advances offer a broader range of tools to conduct surveillance of securities markets more effectively and track digital footprints that may be left behind.



Insider Trading Mitigating Actions

- Education
- Compliance programs as deterrents
- Monitor for data leaks
- Track digital footprints
- Map relationships through internal investigative teams using technology
- Monitor for recruitment efforts, for insiders in general and specifically for references to closed market trading groups
- Monitor Trading in employee accounts, where permissible

Cryptocurrency-Specific Considerations



Use technology tools available for internal intelligence team to monitor marketplaces for accounts or terminology relevant to your enterprise.



Evaluate how third-party companies within your supply chain handle or process cryptocurrency transactions to ensure they are adhering to regulatory requirements.



Monitor how fraudulent activity adapts in response to the changing demands of consumers of commodities that circulate within underground sources, as exemplified by the rise of new laundering schemes based around NFT technology.

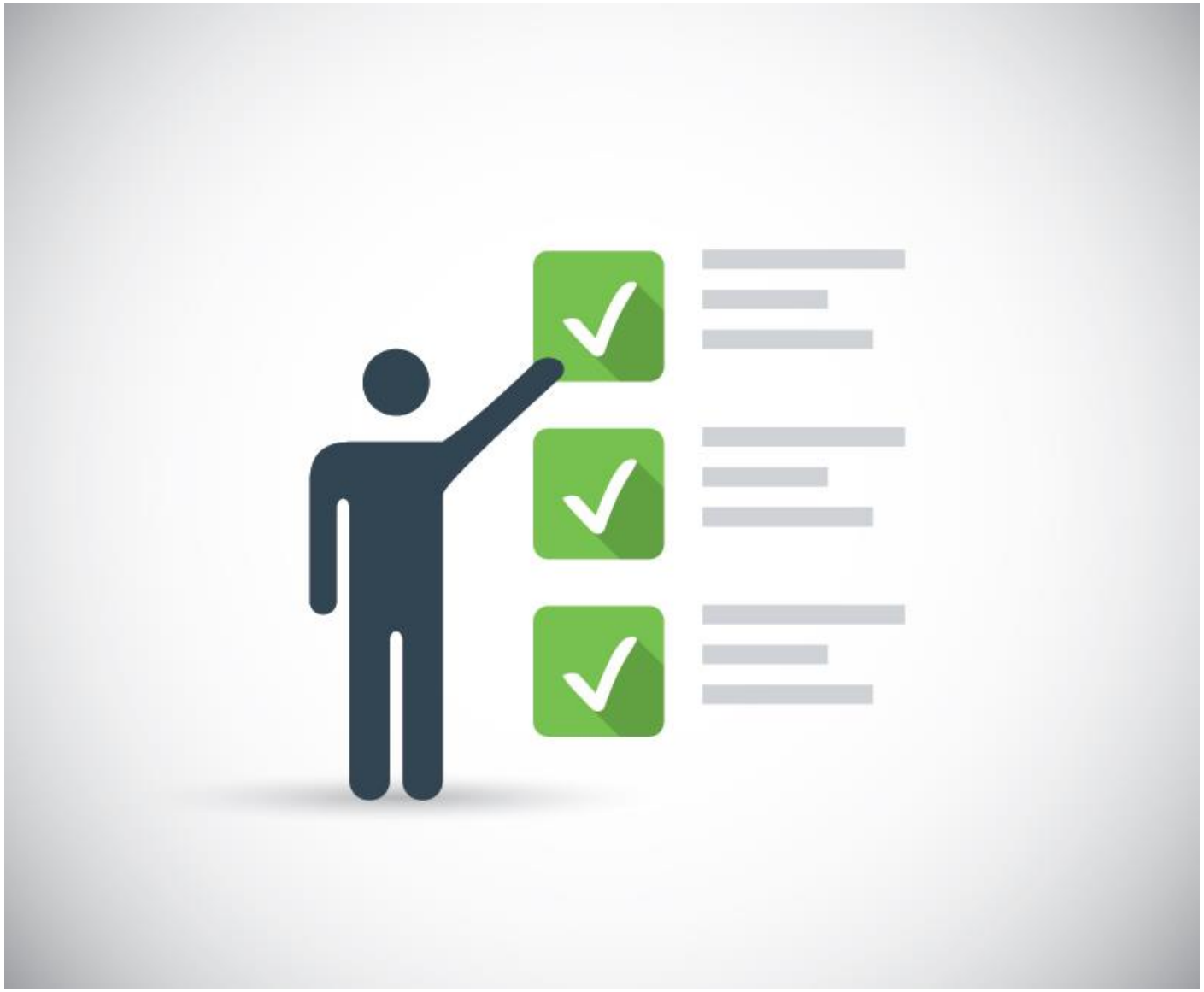


Consider pursuing opportunities internally to have your organization participate in information sharing initiatives to send and receive intelligence associated with laundering activity.

Poll Question #5

TRUE OR FALSE?

You make a trade based upon a tip that your Uber driver gave you on the way to work today. This is Insider Trading.



Summary

- Trading Isn’t New, The Ways That Technology Innovation is Leveraged by Bad Actors is something to be cognizant of
- The threat is against the integrity of our markets; the trust in our economy
- Build digital tools and intelligence
- Training & Education is the key
- Know Your Customer (KYC)
- Establish and strengthen public-private partnerships

Thoughts?
Questions?



Thank You