



*Demystifying*  
**THE DEPARTMENT OF JUSTICE**  
*A Quarterly Series*


# CARE

*Community Awareness,  
Response, & Engagement*

**We will begin our  
presentation shortly.**

# Closed Captioning

- Find the menu bar at the bottom of your zoom window | *Busque la barra de menú en la parte inferior de su ventana de zoom*
- For closed captioning, select “more” and select CC Captions | *Para subtítulos, seleccione “more” y “CC Captions”*

A screenshot of a dark rectangular button with a white 'cc' icon in a square on the left and the word 'Captions' in a blue, sans-serif font to its right.

# Agenda

## **I. Welcome**

- Efrain Botello-Cisneros, Community Outreach Manager

## **II. Introduction**

- Jamal Anderson, Special Assistant Attorney General

## **III. Presentation on the Cybercrime Section**

- Sam Terry, Senior Legal Assistant
- Lawrence Wold, Supervising Investigative Auditor

## **IV. Questions & Answers**

## **V. Thank You & Survey**



# Victoria (Sam) Terry

- Senior Legal Analyst
- Started with DOJ January 2007
- False Claims/Special Crimes 2008
- 3 years Private - Real Estate Litigation Firm
- Utilized the Upward Mobility program
- Degree in Paralegal Studies & Administration of Justice

## Fun Facts:

- Firefighter for 6 years for CDF
- I dove the Blue Hole in Belize
- I'm a true crime junkie



# Cybercrime Section Historical Timeline

1998	1998	2001	2008	2009	2010	2011
<ul style="list-style-type: none"><li>•SB-1734</li><li>•High Technology Theft Apprehension and Prosecution Program (HTTAP), the task force program supports five regions covering 31 counties created.</li></ul>	<ul style="list-style-type: none"><li>•AB-821</li><li>•The High Technology Crime Advisory Committee is hereby established.</li></ul>	<ul style="list-style-type: none"><li>•HTTAP Program was expanded to address the ever-growing problem of identity theft.</li></ul>	<ul style="list-style-type: none"><li>•CDAA/AG's</li><li>•Added to the program DA's and DAG's – included one DAG to each task force to move prosecution process along and free up smaller agencies.</li></ul>	<ul style="list-style-type: none"><li>•Crypto Currencies is created.</li><li>•First transaction was January 2009.</li></ul>	<ul style="list-style-type: none"><li>•Rampant reporting of identity theft.</li><li>•eBay, Craigslist, PayPal, Amazon, and dating apps.</li></ul>	<ul style="list-style-type: none"><li>•August 2011 announcement: "Today's criminals increasingly use the Internet, smartphones, and other digital devices to victimize people online and offline."</li></ul>



**Sacramento Valley High-Tech  
Crimes Task Force (SVHTCTF)**



**Southern California High Tech  
Task Force (SCHTTF)**



**Northern California Computer  
Crimes Task Force (NC3)**



**Rapid Enforcement Allied  
Computer Team  
(REACT)**



**Computer And Technology Crime  
High-Tech Response Team  
(CATCH)**

## SPIKE IN REPORTED INTERNET CRIME

### Top Three U.S. Crimes Based on Americans' Self-Reports

Please tell me which, if any, of these incidents have happened to you or your household within the last 12 months.



GALLUP®

KAMALA D. HARRIS  
Attorney General



State of California  
DEPARTMENT OF JUSTICE

*Demystifying*  
**THE DEPARTMENT OF JUSTICE**





# Types of Crime



Identity  
Theft  
2020



Hacking  
Intrusion



Money  
Laundering



Counterfeit  
Goods



Cyber  
Stalking



Burglary  
Theft



# Overview of Internet Crimes in 2010

In 2010, the Internet Crime Complaint Center (IC3) received over 300,000 complaints, with the most common issues being non-delivery of payment or merchandise, scams impersonating the FBI, and identity theft. The total financial losses reported from these crimes exceeded \$1.5 billion, highlighting the significant impact of online crime during that year.

## Key Statistics

Statistic	Value
Total complaints received by IC3	Over 300,000
Average monthly complaints	Over 25,000
Estimated number of cybercrime victims	431 million globally
Estimated financial losses due to cyber crime	\$388 billion
Most common complaint types	Non-delivery of payment, scams, identity theft

# Overview of Internet Crimes in 2024

In 2024, the FBI's Internet Crime Complaint Center received 859,532 complaints, with reported losses exceeding \$16.6 billion, marking a 33% increase from the previous year. The most common cybercrimes included phishing, extortion, and personal data breaches, with investment fraud causing the highest financial losses.

Key Statistics

Attribute	Value
Total Complaints	859,532
Total Financial Losses	\$16.6 billion
Average Annual Complaints (2018-2024)	863,000
Increase in Losses from 2023	33%
Crypto Loss	\$9,322,335,911

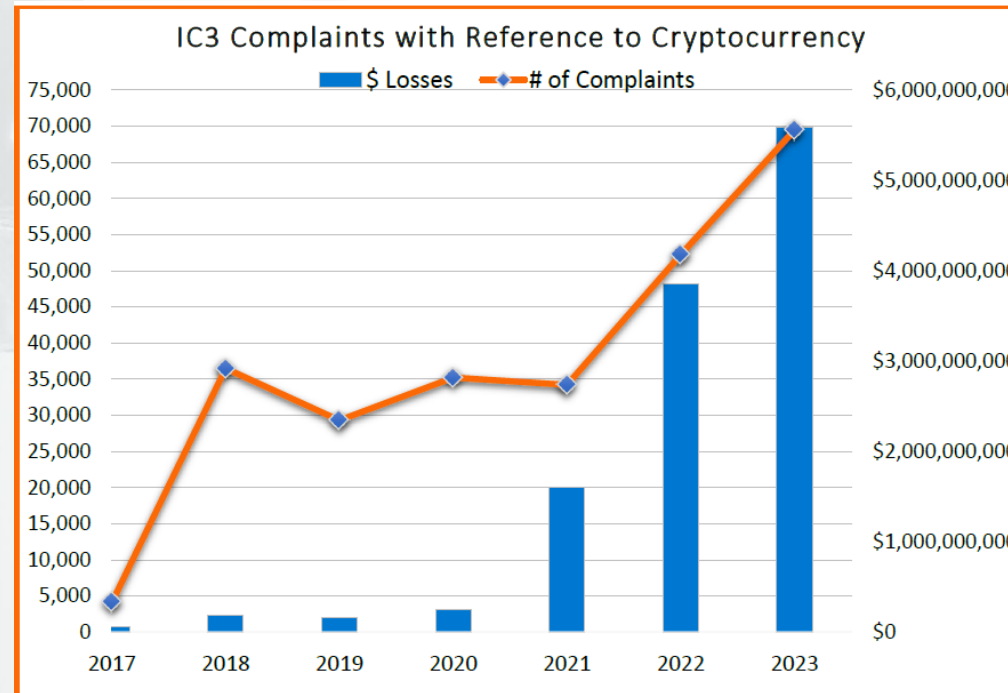
## 2012-2024 FBI Internet Crime Complaint Center (IC3) reported

YEAR	NUMBER OF COMPLAINTS	REPORTED LOSSES (IN BILLIONS)
2012	298,728	0.12
2013	262,855	0.78
2014	269,422	800 million
2015	269,422	1.07
2016	298,728	1.33
2017	301,580	1.4
2018	351,937	1.48
2019	467,361	3.5
2020	791,790	4.2
2021	847,376	6.9
2022	800,000+	10.3
2023	850,000+	16.0
2024	859,532	16.6



# Statistics on Complaints Reported to IC3 Over the Years

Charts depict the amount of Cryptocurrency complaints reported to the IC3 from 2017 – 2023.

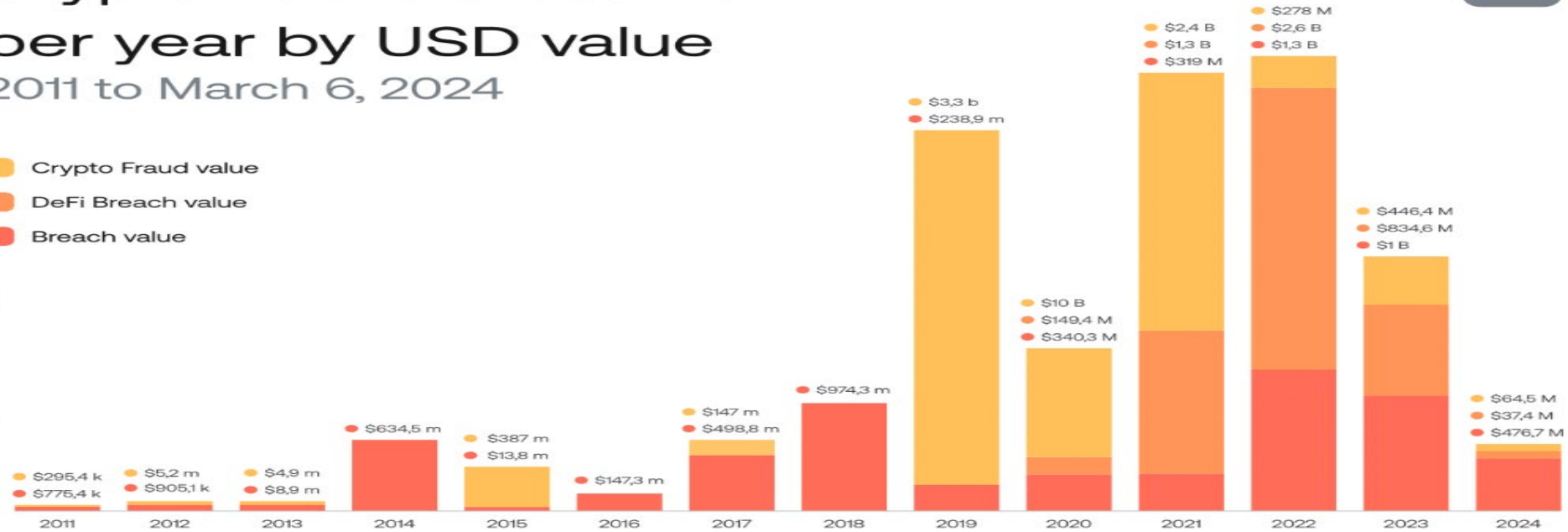


The cryptocurrency landscape is continually evolving, as are the methods of those exploiting it.

## Crypto hacks & scams per year by USD value 2011 to March 6, 2024

- Crypto Fraud value
- DeFi Breach value
- Breach value

© Crystal Intelligence 2024



# Lawrence Wold

- Certified Public Accountant
- MBA in Finance from UC Davis
- Joined DOJ Cybercrimes Section May 2023
- Find me on LinkedIn
- Opinions expressed are mine alone!
- [Lawrence.Wold@doj.ca.gov](mailto:Lawrence.Wold@doj.ca.gov)





# Some Basic Facts About Cryptocurrency



- It is all computer based
- It is nearly impossible to regulate
- Everyone has heard about it...
- ....but very few really know how it works
- Super easy to transfer around the globe

# Cryptocurrency Environment



- Wild Wild West – full of excitement and con artists
- Promises of huge profits
- Bitcoin has grown to over \$100,000
- Huge FEAR OF MISSING OUT (FOMO)
- HUGE possibility of fraud, scams, and thefts

# Different Types of Scams



- Random Text Messages
- LinkedIn messages
- Jury Duty scams, Tax Scam
- Sextortion Scams
- Employment Scams
- Postage Scams, Road Toll Scams
- Romance Scams
- **There is practically NO legitimate purpose for Crypto ATMS. Please do NOT use these.**



# How the Scams Typically Work



- Target nice people
- People that want to make quick profits
- Often a “romance” component, then redirects to investment
- Build confidence, fake profits that appear in the account
- Get victims to invest more and more
  - Deplete savings, refinance house, borrow money
  - Average scam victim is out \$132,000
- Cash out = “fees”, “taxes”, “commissions”
- It is called “Pig Butchering” ....they harvest everything.

# Scam Investment Websites



- On surface they are very well made
- Graphics, AI generated language
- Often try to sound like credible businesses  
“CoinbaseInvest.com”
- Very easy to create
- Based in Vietnam, Cambodia, Myanmar, Eastern Block countries
- Workers are often victims of human-trafficking

# What We Do

Investigate

Investigate leads and complaints using specialized software

Interview

Interview victims:

- Often embarrassed, emotionally distraught, feel betrayed – lost their life savings

Try

Try to get these websites shutdown:

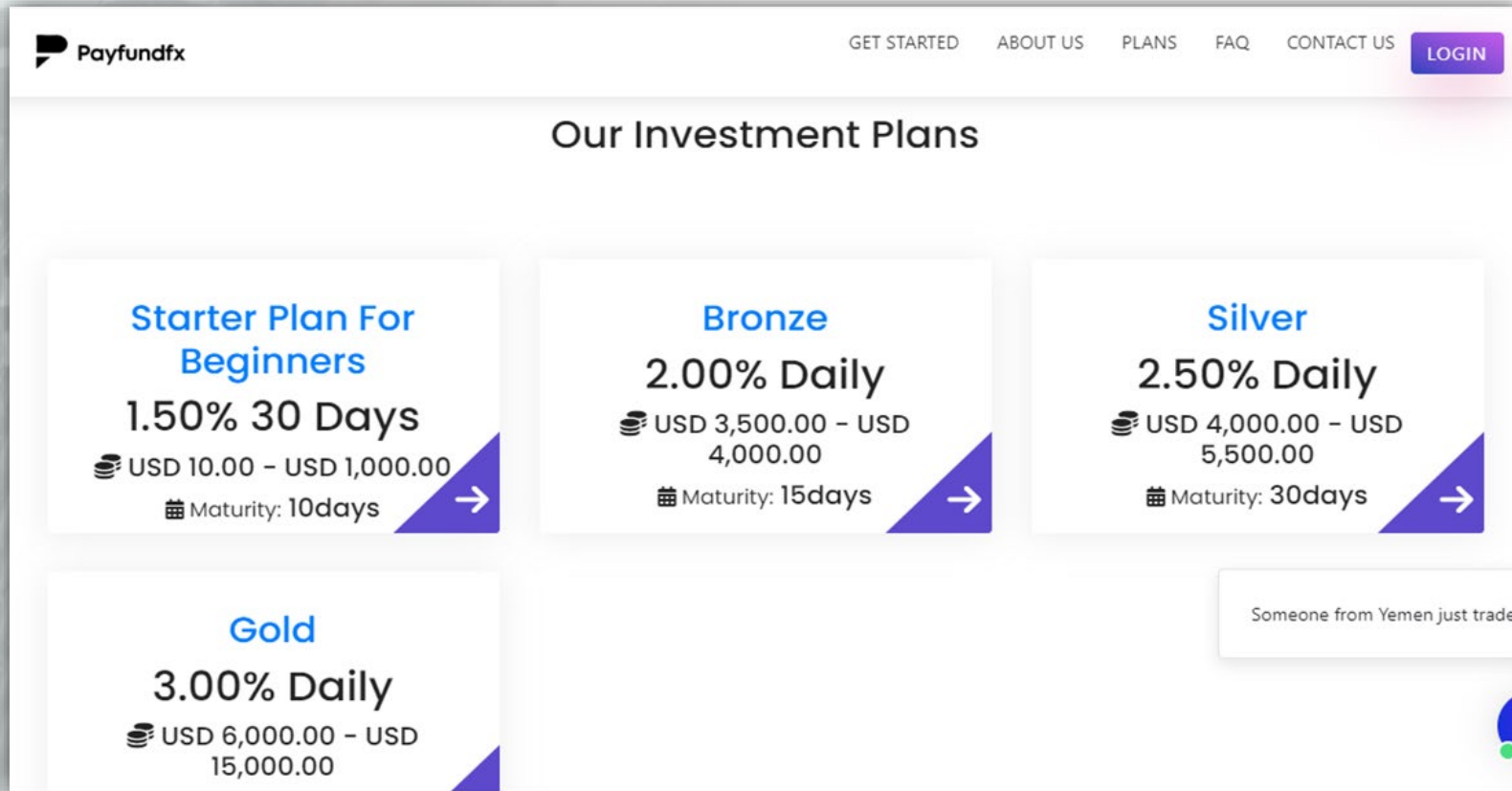
- Victim interview, tracing, Law Enforcement Databases, identify red-flags



# Some Red Flags That You're Dealing With A Scam Website



# FLAG #1 – Impossible Rate of Return



The screenshot displays the Payfundfx website's 'Our Investment Plans' section. The header includes the Payfundfx logo and navigation links: GET STARTED, ABOUT US, PLANS, FAQ, CONTACT US, and a LOGIN button. The main content area features four investment plan cards, each with a title, a daily interest rate, a 30-day rate, a USD investment range, a maturity period, and a right-pointing arrow. A notification bubble on the right states 'Someone from Yemen just traded'.

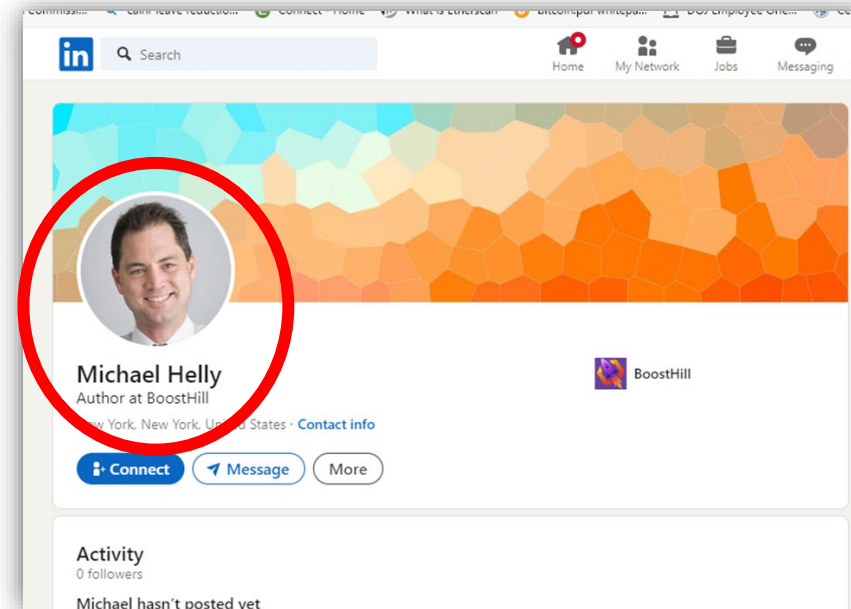
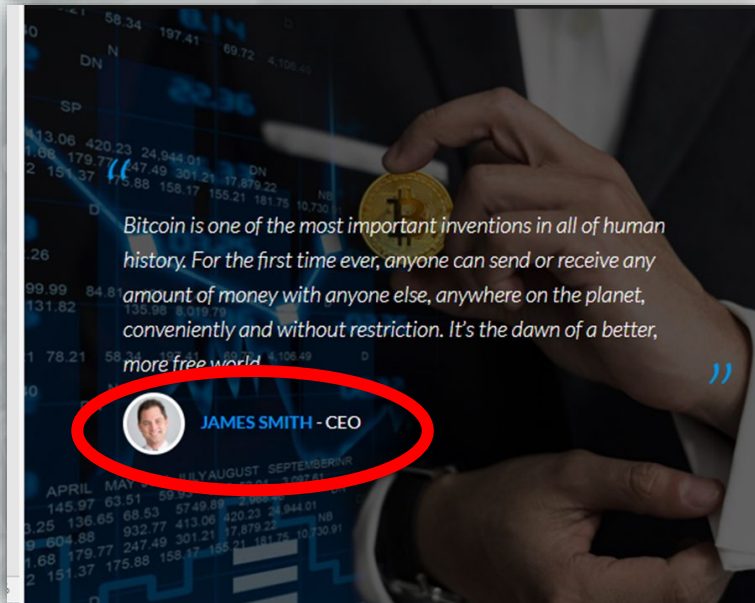
Plan Name	Daily Rate	30-Day Rate	Investment Range (USD)	Maturity
Starter Plan For Beginners	1.50%	1.50%	USD 10.00 - USD 1,000.00	10 days
Bronze	2.00%	-	USD 3,500.00 - USD 4,000.00	15 days
Silver	2.50%	-	USD 4,000.00 - USD 5,500.00	30 days
Gold	3.00%	-	USD 6,000.00 - USD 15,000.00	-

# FLAG #2 – No Contact Information

Legitimate websites will generally have:

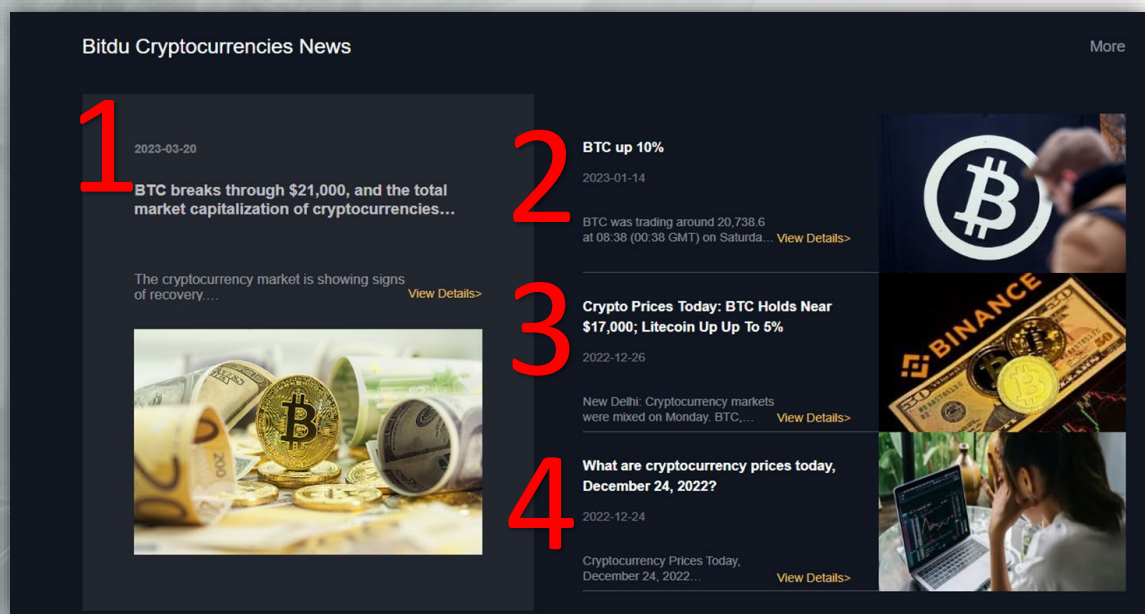
- Phone number
- Physical Address
- Email
- Not “Payfundsfx@gmail.com”
- ***The fraudulent websites will try to get their victims to use WhatsApp, Telegram, or online Chat functions.***

# FLAG #3 – They Steal Images or Dialog from other websites





# FLAG #4 – Website Has Not Been Updated Recently



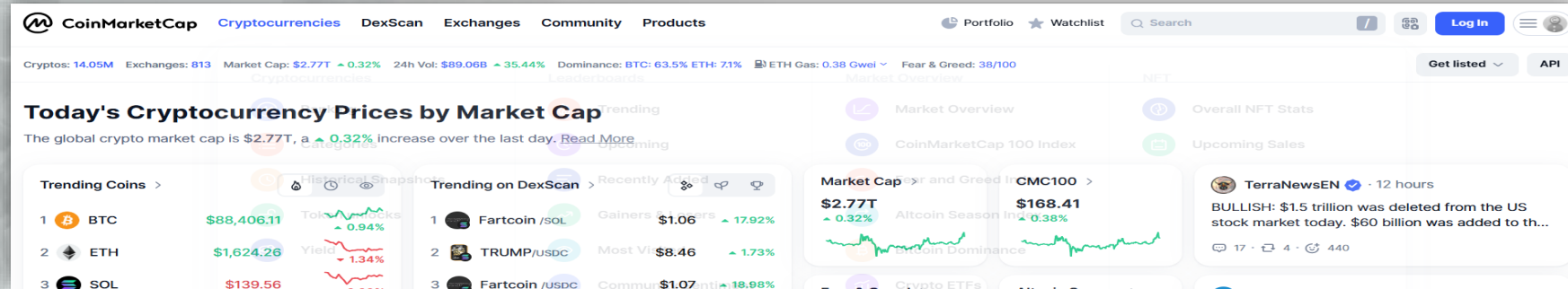
1. Date: 3/20/2023

2. Date: 1/14/2023

3. Date: 12/26/2022

4. Date: 12/24/2022

# FLAG #5 – Not On Coin Market Cap



CoinMarketCap.com lists the top 252 coin Exchanges (as of 8/23/2024)

- #1 is Binance with \$15.3 billion in daily volume
- #2 is Coinbase with \$2.5 billion
- #3 is OKX with \$2.1 billion

Almost all fraudulent websites claim to be a “leading” website, if they are not listed on CoinMarketCap.com’s list of exchanges – it is likely a scam.

# Key Takeaways

If you get a LinkedIn message, Facebook message, Instagram IM, email from someone that you might know, that says they made a bunch of money in cryptocurrency, chances are their account was compromised, and someone is trying to scam you.

If you get a call or text from anyone claiming to be law enforcement, a tax agency, a jury duty service and they want you to send bitcoin or put money into a bitcoin ATM....it is 100% a scam.

No one  
“invests” in  
cryptocurrency  
– it is  
**speculation.**

Once the cryptocurrency is sent or has been put into an ATM, it is generally gone for good.

Law  
enforcement  
agencies are  
fighting an  
uphill battle.



Please fill out the brief survey  
below. Thank you!

