coinbase

To:
Committee Secretary
Parliamentary Joint Committee on Law Enforcement
PO Box 6100
Parliament House
Canberra ACT 2600
le.committee@aph.gov.au

13 October 2025

Re: Parliamentary Joint Committee on Law Enforcement inquiry into Combatting Crime as a Service

Coinbase Global, Inc. together with Coinbase Australia, Pty. Ltd. and its other subsidiaries, (**Coinbase**) appreciates the opportunity to respond to the Parliamentary Joint Committee (**Committee**) on Law Enforcement's inquiry into Combating Crime as a Service.

Coinbase started in 2012 with the idea that anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, we are publicly listed in the United States and provide a trusted and easy-to-use platform that millions of verified users in over 100 countries rely on to access the crypto economy.

Understanding the changing landscape of crime in the digital age is important to ensure that Australia's Law enforcement agencies are able to protect Australians. The Committee should ensure that there is education, training and investment into dedicated analytical tools allowing for agencies to take advantage of crypto's unique visibility in order to reduce Crime as a Service—because while cryptocurrencies are used by criminals to transfer value, they are also uniquely bad for crime.

We commend the Committee on giving the phenomenon of Crime as a Service the intention it deserves by opening this inquiry. We look forward to continuing to engage with this work and encourage the Committee to contact us if we can be of further help.

Yours sincerely,

[redacted]

Tom Duff Gordon
VP, International Policy
Coinbase Global, Inc.

[redacted]

John O'Loghlen
Managing Director, APAC
Coinbase Global, Inc.

coinbase

Introduction

We welcome the Committee's inquiry into Combating Crime as a Service. These inquiries offer critical opportunities to ensure that Australia's existing legislative, regulatory, and policy frameworks are able to address evolving criminal methodologies. Coinbase encourages the Committee to contact us if it has any further interest or queries that we may be able to help with.

As an outcome of this inquiry, the committee should recommend that there is education, training and investment into staff and dedicated analytical tools allowing for agencies to take advantage of crypto's unique visibility, and enhancing opportunities for effective public–private relationships within the crypto ecosystem in order to reduce Crime as a Service within Australia.

The integration of the internet and digital payments has opened a new opportunity set for criminals. Rather than needing to physically interact with their victims, criminals are now able to act from behind a screen. This has led to the development of Crime as a Service, which consists of illicit 'plug-and-play' services which criminals either sell or rent, allowing others to commit crimes without deep expertise. These services are varied and include credential-stuffing and automation services, phishing and packaged exploit kits, info-stealers and deploying malware.

Underpinning these crimes is the ability to transfer value digitally via traditional intermediaries like banks, to intermediary-less forms of digital value transfer like cryptocurrencies. While cryptocurrencies are often considered to be a great medium for funding online crime, they are actually a uniquely bad form of value transfer to use when undertaking illicit activities.

What's often misunderstood is that **crypto isn't uniquely vulnerable to crime—it's uniquely visible**. In fact, Coinbase has helped law enforcement trace funds, identify repeat suspects, and proactively block known bad actors. We've used blockchain analytics to connect wallet addresses, flag suspicious behavior in real time, and prevent future losses.

Coinbase works with law enforcement globally at local, state and federal levels including both Europol and Interpol. We have aided law enforcement agencies within Australia including SAPOL, New South Wales Police, Queensland Police and the Australian Federal Police for their inquiries into the use of cryptocurrency by criminals. We have also spent time educating staff on cryptocurrency and blockchain technology, arming them with the knowledge needed to investigate and combat cryptocurrency related crimes effectively.

coinbase

Cryptocurrency usage in crime

The association of cryptocurrencies with illicit activities, particularly darknet markets and ransomware, has created a common perception that they are a primary tool for criminals. However, this perception is often disproportionate to reality. For many crimes, traditional fiat currency remains the preferred method for moving illicit funds.

The key difference lies in the technology itself. Unlike opaque traditional finance, cryptocurrencies operate on public, immutable ledgers known as blockchains. This transparency generally provides an unprecedented level of visibility into transaction histories, allowing businesses and investigators to conduct more informed risk assessments and making it significantly harder for criminals to hide their activities.

Data confirms that criminals still overwhelmingly prefer cash and traditional financial channels, especially for money laundering and terrorism financing. A 2024 Chainalysis report found that illicit activity accounted for just 0.14% of cryptocurrency transaction volume (approx. USD $40 billion).[1] When compared to the UNODC's estimate that global criminal proceeds constitute 3.6% of GDP (approx. USD $4 trillion),[2] cryptocurrency represents only around 1% of global illicit financial flows.

This finding is echoed by national authorities:

- **For Money Laundering:** AUSTRAC's 2024 National Risk Assessment confirms that criminals in Australia continue to rely on "established channels such as cash, luxury goods, real estate, domestic banks, casinos and remitters."[3] The United States' assessment concurs, noting "the use of virtual assets for money laundering remains far below that of fiat currency."[4]
- **For Terrorism Financing:** AUSTRAC observed in 2024 that financiers prefer "readily available and proven methods"[5] like banking and cash over complex digital schemes. While terrorist groups have solicited crypto donations, the blockchain's transparency has also enabled authorities to trace and dismantle their funding networks.

However, we acknowledge that cryptocurrency is the instrument of choice for a specific subset of digitally-native crimes. In these domains, its use is not just prevalent but central to the criminal business model. For example:

[1] Chainalysis, The 2025 Crypto Crime Report (Chainalysis, 2025)
[2] United Nations Office on Drugs and Crime, Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organized Crimes: Research Report (Vienna: United Nations Office on Drugs and Crime, 2011), 127
[3] AUSTRAC, Money Laundering in Australia National Risk Assessment 2024, 5
[4] U.S. Department of the Treasury, 2024 National Money Laundering Risk Assessment (2024)
[5] Ibid

coinbase

- **Ransomware:** Cryptocurrency, mainly Bitcoin, is the lifeblood of ransomware, with attackers extorting over $1 billion in 2023. The Ransomware-as-a-Service (RaaS) model has professionalised these attacks, making them more widespread.[6]
- **Scams and Fraud:** Scams are the largest form of crypto-based crime by volume, generating an estimated USD $9.9 billion in 2024. Tactics like "pig butchering" and "approval phishing" are increasingly sophisticated and supported by a professional criminal ecosystem.[7]
- **Darknet Marketplaces:** These markets, which generated over USD $2 billion in 2024, rely exclusively on cryptocurrency. Operators are increasingly shifting from Bitcoin to privacy-enhancing coins like Monero to obscure transactions.[8]
- **Cryptocurrency Theft:** Hacks and exploits remain a major threat, with $2.2 billion stolen in 2024. State-sponsored actors, particularly from North Korea (DPRK), are the most prolific offenders, responsible for a record $1.34 billion in 2024 alone.[9]
- **Distribution of CSAM:** Cryptocurrency is the "payment of choice" for the commercial trade of Child Sexual Abuse Material (CSAM). Despite perpetrators' belief in their anonymity, the blockchain has proven crucial in major law enforcement takedowns, such as the "Welcome to Video" marketplace bust.[10]

This presents a crucial paradox, while cryptocurrency is the undeniable payment of choice for a narrow but significant set of digitally-native crimes, the perception of it as a tool for widespread, anonymous criminality is largely misplaced. The very technological attributes that make cryptocurrency suitable for ransomware or darknet markets, particularly its digital traceability on a public ledger, are the same attributes that can fundamentally empower law enforcement. This inherent transparency creates a permanent record of illicit activity, offering investigators powerful new tools to follow the money, which stands in stark contrast to the often-opaque nature of conventional financial crime. For most predicate offences, criminals still prefer the relative anonymity and stability of cash and traditional financial channels.

The Europol & Basel Institute on Governance[11] have observed the relative differences between the use of crypto and other assets for laundering purposes, and the opportunities that the blockchain offers investigators:

---

[6] Chainalysis, The 2024 Crypto Crime Report (Chainalysis, 2024)
[7] Chainalysis (2025), Europol, European Union Serious and Organised Crime Threat Assessment 2025: The changing DNA of serious and organised crime (Luxembourg: Publications Office of the European Union, 2025)
[8] Chainalysis (2024), Chainalysis (2025)
[9] Chainalysis (2024), Chainalysis (2025), Europol, European Financial and Economic Crime Threat Assessment 2023: The Other Side of the Coin: An Analysis of Financial and Economic Crime (Luxembourg: Publications Office of the European Union, 2023)
[10] Chainalysis (2024), International Centre for Missing and Exploited Children, Cryptocurrency and the Trade of Online Child Sexual Abuse Material (Washington, D.C.: International Centre for Missing and Exploited Children, 2021)
[11] Europol and Basel Institute on Governance, Seizing the opportunity: Five recommendations for crypto assets-related crime and money laundering—2022 recommendations of the joint working group on criminal finances and cryptocurrencies (The Hague: Europol, 2022)

coinbase

> *"Despite talk of the "threats" of crypto assets and services, these pose no more of an inherent threat than cash, companies, property or even the global trading system – all of which are still far more likely to be used to launder illicit funds. Latest estimates indicate that the percentage of illicit activity in the crypto industry is decreasing, even as the use of cryptocurrencies expands and evolves.*
>
> *What the blockchain does offer is promising opportunities to investigate and disrupt organised crime networks and to recover illicit assets. With the right tools, techniques and data, law enforcement can (and does in many countries) "follow" illicit assets as they move across one or more blockchains."*

This is what we mean when we say that crypto is bad for crime. Unlike cash or even certain banking systems, every action onchain leaves a mark. And when platforms like Coinbase are proactive in reviewing, reporting, and assisting, the system becomes safer—not more vulnerable.

Cryptocurrency can empower law enforcement

The most significant shift offered by cryptocurrencies is the transparency derived from their public ledgers. Unlike traditional finance, where investigations can be slowed by jurisdictional barriers, the blockchain enables the real-time tracking of transactions as they happen. This level of visibility is a game-changer in Anti-Money Laundering (AML) and financial crime investigations, offering investigators an immediate starting point to follow the money, identify critical on- and off-ramps, and obtain actionable intelligence far faster than conventional methods allow. This not only speeds up the detection of suspicious activities but also provides opportunities for the proactive freezing and recovery of assets through established civil and criminal legal gateways.

Cryptocurrencies offer profound opportunities to identify patterns and connections within onchain data, a process commonly referred to as blockchain analysis. This specialised skillset allows investigators to reveal who or what is behind transactions and addresses for certain assets.

A core analytical technique is "clustering," which identifies relationships between different addresses and their associated wallets. Dedicated analytical tools further enhance this process, providing insights that, when combined with internal transaction data, device/event data, and Open-Source Intelligence (OSINT), can identify the underlying structure of criminal operations, helping authorities dismantle illicit networks more effectively.

coinbase

For both intermediaries and law enforcement, these capabilities give a proactive edge in combating financial crime that is not necessarily possible within traditional finance. By immediately looking upstream, we can identify opportunities for disruption.

We integrate this intelligence into our AML and payments risk frameworks, specifically leveraging blockchain analysis insights to tag and block known bad addresses. Our proactive approach allows us to prevent our users from sending funds to illicit services and protects our customers from becoming victims.

Coinbase's work with law enforcement

Intermediaries like Coinbase can be key to investigations. The Financial Action Task Force (FATF) recognises the importance of centralised intermediaries and requires them to adhere to global regulatory standards.[12] An approach consistent with the oversight applied to all financial sectors, from banks to real estate.

Due to the features of blockchain we are able to track stolen funds across wallets—tracing the money trail and easily identifying attempts to launder funds—as well as link criminals to other incidents —helping investigators reconstruct the full scope of the scheme. In traditional financial investigations, the equivalent information that is available from a simple query of the blockchain can take weeks or months to uncover—if it is even possible.

In April 2025, Chainalysis awarded Coinbase's Global Intelligence team with the "Impact Award"[13] for achieving measurable, transformative outcomes in relation to a deep dive into the role of cryptocurrency within fentanyl trafficking. This resulted in 68 law enforcement referrals across 9 countries, targeting networks involved in fentanyl distribution, including manufacturers of pill presses and laundering operations.

In May 2025, Queensland Police arrested a suspect linked to a DNM vendor as a direct result of Coinbase's intelligence concerning their association with fentanyl production[14]. The operation recovered a pill press, precursors, suspected fentanyl pills, and a cement mixer. The suspect, previously jailed for firearms and drug offenses, was charged with drug trafficking. Coinbase received the following feedback from the investigation team, *"Without your team's work, this result wouldn't be possible"*.

[12] Financial Action Task Force, FATF Report to the G20 Finance Ministers and Central Bank Governors on So-Called Stablecoins (Paris: FATF, 2020)
[13] Chainalysis Team, "Chainalysis Recognizes Global Customer Excellence at Inaugural Customer Awards Ceremony," Chainalysis Blog, April 16, 2025
[14] Queensland Police News, "Operation X-ray Toren: North Brisbane," Queensland Police News, May 22, 2025

coinbase

Coinbase has also been setting the standard for what good looks like globally when it comes to working with law enforcement since we began this work in 2013, including:

- identifying and block serial offenders in London targeting victims late at night
- tracing assets from a high-profile robbery in Toronto resulting in the sharing of intelligence
- helping secure a conviction in a tragic New York case involving drug-laced assaults and stolen funds
- helping take down a robbery ring in Birmingham targeting LGBTQ+ individuals through dating apps
- taking down a $20M spoofing scheme that exploited Coinbase's brand

We have included some of these examples that were published on our blog in the Annexure.

Recommendations

Coinbase recommends that the Committee considers two key pillars for improving Australia's capabilities regarding the use of cryptocurrencies in crime; investing in law enforcement capabilities and specialisation, and institutionalising global and public-private collaboration.

Investing in Law Enforcement Capabilities and Specialisation

The unique nature of onchain data analysis requires a significant investment in specialised training and dedicated technological resources within law enforcement agencies. To enhance the capabilities of law enforcement we recommend:

- **Developing the Blockchain Analysis Skillset:** Mandate and fund comprehensive training programs to cultivate the "Blockchain Analysis skillset" across financial crime units. This continuous learning is required to understand techniques like "clustering" (identifying relationships between addresses) and the "common spend heuristic."
- **Acquiring Dedicated Analytical Tools:** Invest in dedicated analytical tools that allow investigators to perform real-time tracking, clustering, data aggregation, and alerting. These tools must be capable of combining onchain data with traditional investigative information (like device/event data and OSINT) to identify and understand the underlying structure of criminal operations and effectively dismantle illicit networks.

coinbase

- **Shifting to Intelligence-Led Operations:** Move beyond purely reactive investigations. Law enforcement should utilise intelligence derived from blockchain analysis to look "upstream" and identify opportunities for immediate disruption, rather than waiting for a crime to be fully executed.

Institutionalising Global and Public-Private Collaboration

Given the borderless nature of cryptocurrencies and the need for private sector cooperation, effective policy must institutionalise formal partnerships. We recommend:

- **Formalising Information Sharing with Industry:** Create secure and mandatory mechanisms for financial institutions to share intelligence derived from their internal transaction monitoring systems with law enforcement. Including collaborating on methods to tag and block known bad addresses to prevent users from interacting with illicit services.
- **Facilitating Private to Private Information Sharing:** Leverage recent changes to the Anti-Money Laundering and Counter Terrorist Financing Act 2006 to enable private sector entities to share information and enable deeper collaboration to detect and disrupt criminal activity. This should be led by the government to ensure businesses have the right safeguards in place, particularly to protect privacy.
- **Strengthening International Regulatory Cooperation:** Prioritise strengthening cooperation with international regulatory bodies and law enforcement agencies to overcome "jurisdictional barriers." This collaboration is essential to ensure that the real-time traceability of the blockchain is matched by the agility of cross-border enforcement, preventing criminals from simply moving funds across national boundaries.

coinbase

Annex:

From Dating App to Robbery Ring: How Blockchain Helped Secure Justice in the UK

In July 2023, we received a message from a Coinbase user who had just experienced something horrifying. They'd been drugged, held for hours, and forced to unlock their phone using Face ID. Their ID documents were stolen. Their passport was used to initiate account transfers. And over the next several hours, funds began to disappear—slowly at first, then in larger amounts.

It was a clear case of robbery. But what followed revealed something much larger.

This blog is about a case that started with one report and ultimately helped lead to the conviction of five men, responsible for a coordinated campaign of assault, coercion, and theft—targeting LGBTQ+ individuals across Birmingham, UK.

What We Discovered

Our review of the victim's Coinbase account showed:

- Multiple identity verification attempts within hours of the attack
- Facial images clearly showing the victim flanked by others, seated in the back of a car
- Identity documents displayed by individuals other than the account holder

The third verification attempt succeeded. Analysis demonstrated the victims Ethereum was stolen and swapped for USDT via a decentralised exchange. Our team traced that USDT through a network of wallets to a Coinbase account belonging to Abubaker Al Ezawy, one of the five men later convicted.

But that wasn't all.

Our onchain analysis revealed:

- ETH top-ups (aka "fee funders") tied to other known Coinbase users Interconnected wallets receiving and dispersing stolen funds

In collaboration with Law Enforcement, our Global Intelligence team preserved evidence, and helped ensure the case had what it needed. Our data was entered into evidence, including both wallet attribution and links between suspects through supporting fund flow analysis.

coinbase

The Outcome

In January 2024, five men were sentenced to nearly 80 years in prison for a series of robberies involving drugging, assault, and financial theft. Their method:

- Use dating apps like Grindr to lure victims
- Assault them upon arrival
- Use Face ID to unlock phones and access financial accounts
- Steal phones, wallets, and identities
- Coerce victims into "verifying" high-value transactions

Their targets were chosen because of their perceived vulnerability—because the attackers believed members of the LGBTQ+ community would be too embarrassed or ashamed to come forward.

They were wrong.

Victims came forward. And the evidence, including blockchain forensics, was decisive.

Our Role

This was a powerful example of how crypto, when combined with diligent investigation and cooperation, can help law enforcement deliver justice.

The victims were the heroes of this case. We were honored to support them—and the officers who led the prosecution.

Crypto wasn't the problem. In fact, crypto made it possible to trace the stolen assets, identify suspects, and ultimately hold them accountable.

"The investigation proved that law enforcement doesn't have to tackle this alone—working closely with partners in the private sector can make a real difference in combating crime." - West Midlands Police

We couldn't agree more.

How Coinbase Helped Disrupt a Global Cybercrime Marketplace

One of the most high-impact cases we supported in 2024 involved the takedown of Chirag Tomar, who ran a global spoofing scheme that stole more than $20 million in crypto by impersonating Coinbase.

coinbase

Tomar and his co-conspirators created fake websites like “CoinbasePro.com” to trick users into handing over login credentials and two-factor authentication codes. In some cases, they posed as Coinbase customer support and used remote access tools to drain real user accounts. Victims lost hundreds of thousands in minutes—including one individual who was defrauded of over $240,000 in a single attack.

When we learned of the activity, we worked quickly to help law enforcement trace stolen funds, identify victims, and preserve key evidence. In December 2023, Tomar was arrested at the Atlanta airport. He pleaded guilty in 2024 and was sentenced to five years in federal prison.

This case was part of a larger pattern we’ve seen: criminals misusing trusted brands to defraud consumers at scale. But unlike cash—which remains the #1 tool for illicit finance worldwide, accounting for up to $2 trillion annually in laundered money—crypto leaves a permanent, traceable trail. That’s why you hear about crypto crime so often: not because it’s more common, but because it’s easier to uncover and stop.

Working closely with agencies like the U.S. Secret Service and FBI, we helped secure justice in this case and protected countless other users from falling victim to the same trap.

We’re proud of the role Coinbase played here. It reflects our broader approach: investing in onchain forensics, real-time fraud detection, and direct partnerships with law enforcement to protect consumers—on and off our platform.

As we reflect on wins with law enforcement, this case stands out as a powerful example of what’s possible when industry and government team up to fight cybercrime.

How Blockchain Helped Uncover a Pattern of Phone Theft, Coercion, and Crypto Drains in London

As mobile phones have evolved into financial hubs, they’ve also become high-value targets for criminals. And when those phones contain access to banking apps, payment platforms, and crypto wallets, the stakes are even higher.

In 2021, we received a referral from the City of London Police that marked the beginning of a troubling trend: thieves targeting victims late at night, stealing their phones, and then coercing access to their financial apps—including their Coinbase accounts.

The Setup: A New Type of Street Crime

coinbase

One victim's case stood out. They had been robbed, and shortly afterward, their Coinbase account was accessed and drained. Our investigation revealed the suspect had:

- Used the victim's own device to log in
- Completed an identity verification (IDV) refresh in the early hours of the morning Uploaded images where the victim was clearly present—coerced in the back of a car, holding their own ID, with others beside them

This wasn't opportunistic theft. It was calculated, coordinated, and designed to bypass every layer of digital security. And it worked because the attackers had the victim physically present to unlock apps, pass biometric checks, and approve transfers.

What We Did

From that single incident, our team was able to:

- Identify a cluster of similar cases, each involving late-night phone theft, coercion, and rapid unauthorised crypto sends
- Build a victim population of over >30 individuals by reviewing Coinbase data
- Map crypto addresses identifying a network of wallets used, creating a network of accounts used repeatedly across incidents

We then proactively:

- Blocked transactions to the identified addresses
- Flagged suspect wallets in our internal systems
- Referred the case to UK law enforcement

Our blockchain analysis, combined with account-level data, helped turn individual reports into a larger, actionable pattern.

Why This Matters

This wasn't a high-profile hack or headline-grabbing scam. It was traditional street crime—robbery and coercion—updated for the smartphone era. But here's what's different: with crypto, **the money trail doesn't disappear**.

Blockchain forensics allowed us to trace the flow of funds, connect separate cases, and help law enforcement go beyond one-off theft to uncover a linked series of coordinated crimes.

And in the end, that work mattered. UK law enforcement used our findings to help support

coinbase

the arrest and charges[15] of several bad actors with the potential for significant sentencing. Coinbase's analysis was included as part of the prosecution's case.

How Customers Can Help Protect Themselves

While our teams work hard behind the scenes to keep users safe, there are important steps you can take to protect your financial life:

- **Use a strong passcode**: Set a long, unique passcode on your device and apps—biometrics alone are not enough.
- **Stay aware in public**: Be mindful when entering your phone PIN or opening financial apps in crowded places.
- **Limit app access**: Use security settings to require reauthentication for sensitive apps like banking and crypto platforms.
- **Enable additional Coinbase security features**: Two-factor authentication (2FA) with an authenticator app—not SMS—is highly recommended.

Keeping your phone—and your accounts—locked down makes it harder for criminals to exploit quick-access scenarios.

- Telling your network provider straight away if your phone is stolen because they can blacklist and deactivate it remotely.
- If you've lost money or provided your financial information to someone, notify your bank immediately.

The Bigger Picture

This is exactly why we partner so closely with law enforcement. Not just to respond—but to prevent. By working together, we can disrupt patterns, protect users in real time, and build safer systems.

As crypto becomes part of everyday financial life, it's also becoming part of everyday crime investigations. That doesn't make crypto a risk. It makes it a **resource**—one we're proud to offer.

[15] City of London Police, "Five Serial Thieves Sentenced after Stealing £157,000 Worth of Items from Victims on Nights Out in London," City of London Police, November 28, 2022