



J5 reviews cryptocurrency risk factors during Cyber Challenge

The J5 brought together investigators and analysts from its 5 member agencies as part of this year's Cyber Challenge.

Published 19 September 2024

BRISBANE, Australia – The Joint Chiefs of Global Tax Enforcement (J5) brought together more than 30 investigators and analysts from its five member agencies and each country's Financial Intelligence Units (FIUs) in Brisbane, Australia, September 16 to 20, for 5 full days of lead development as part of this year's Cyber Challenge.

The Cyber Challenge is an annual event where experts from J5 member countries join forces to review data and identify quality leads from a variety of open and investigative sources. This week's event was the sixth iteration of the "Challenge," and focused on data involving over-the-counter cryptocurrency trading desks, online cryptocurrency casinos and cryptocurrency payment platforms.

The J5 looked at money laundering and tax evasion risk factors associated with these businesses. More than 30 leads were prepared or developed by the J5 member countries and partner Financial Intelligence Units as part of the Challenge.

As part of previous Cyber Challenges, the J5 developed advisory documents for the tax and financial industries that provided insightful details about the focus of that particular Challenge. The J5 is looking to potentially create similar documents this time for over-the-counter cryptocurrency trading desks and cryptocurrency payment processors.

"The Challenge provided us an opportunity to exchange data on cryptocurrency-based platforms that lack anti-money laundering and

Know Your Customer controls. We know that without these controls in place, online platforms become playgrounds for criminal activity. Our goal is to stop criminals in their tracks, and the exchange of information that occurs during these Challenges allows us to embark on new investigations to do just that,” said U.S. Chief Guy Ficco, head of Internal Revenue Service Criminal Investigation (IRS-CI).

“The Australian Taxation Office is proud to have hosted this year’s challenge. This Challenge builds on the momentum of previous years where our top investigators and experts come together to collaborate and identify quality leads to stop cybercrime cryptocurrency fraud. This is the power of the J5 alliance, together with our public and private specialist partners we are getting ahead of the criminals in a rapidly changing cyber ecosystem,” said Australian Chief John Ford, Deputy Commissioner at the Australian Taxation Office (ATO).

“By working together with our J5 partners and FIUs, we are enhancing our abilities to detect and report money laundering, and tax evasion involving cryptocurrency assets,” said Eric Ferron, Canada’s J5 Chief, and Director General of the Criminal Investigations Directorate at the Canada Revenue Agency (CRA). “The J5 Cyber Challenge provides us a unique opportunity to work together and assist us in keeping pace with, and specifically targeting, criminals who are active in these platforms.”


“Criminals are early adopters of new technology that knows no country borders. International cooperation is therefore crucial for effective interventions,” said Niels Obbink, Director General, Dutch Fiscal Intelligence and Investigation Service (FIOD). “One of the goals of the Challenge was to explore and understand new illegal digital modus operandi for financial crime. The intelligence that was generated helps us to target the most influential digital criminal actors to investigate or to tackle with other disruptive interventions.”

“The Challenge has become a true staple of the J5 and demonstrates the sheer power of this global alliance. By bringing together our crypto experts and analysts from our respective FIUs, we’re able to clash vast datasets to unearth new and significant leads,” said Richard Las, Director, Fraud Investigation Service, His Majesty’s Revenue and Customs (HMRC). “So, while criminals may think they’re being innovative by exploiting over-the-counter crypto platforms like online casinos, our experts are all too aware and are ready to cash in.”

“As criminal actors continue to adapt and expand their operations globally, joint tabletop exercises like the J5 Challenge continue to highlight the value of international collaboration and the pivotal role these productive partnerships play in disrupting complex criminal networks that seek to exploit the global financial system,” said James Bissonnette, Team Lead, Intelligence Sector, Financial Transactions and Reports Analysis Centre of Canada. “Our work today would not be possible without the commitment from businesses who report financial transactions to their respective financial intelligence units. These businesses on the front lines have a vital role in detecting criminals and their networks who are using the global financial system to launder their illicit gains. Their work is important in combatting major financial crimes such as tax evasion, drug trafficking, human trafficking and online child sexual exploitation.”

FIOD hosted the first Challenge in 2018 in Utrecht with the aim of tracking down those who make a living facilitating and enabling international tax crime. The following year, the U.S. hosted a second Cyber Challenge in Los Angeles focused on cryptocurrency. In 2021, the COVID-19 pandemic caused the Cyber Challenge to be held virtually where the event focused on financial technology (FinTech) companies. In 2022, the Challenge focused on non-fungible tokens and decentralized exchanges, and in 2023, the Challenge focused on data mining and FIU data.

Using various analytical tools, members of each country are tasked with generating leads and finding cryptocurrency-related tax offenders, based on the new data available to them through the Challenge. Working within existing treaties, real data sets from each country were brought to the Challenge to make connections where current individual efforts would take years to make those same connections.

The Challenges have proven to be fruitful for the J5 as they generated significant leads for the organizations to investigate. [BitClub Network \(PDF 116KB\)](#) , a multi-million-dollar Ponzi scheme where thousands of people were scammed into buying into a bogus mining pool, is one of the first J5 successes that stemmed from the J5 Challenges.

The J5 works together to gather information, share intelligence and conduct coordinated operations against transnational financial crimes. The J5 includes the ATO, CRA, FIOD, HMRC and IRS-CI.

For more information about the J5, please visit www.irs.gov/j5 .

QC 103043

Our commitment to you

We are committed to providing you with accurate, consistent and clear information to help you understand your rights and entitlements and meet your obligations.

If you follow our information and it turns out to be incorrect, or it is misleading and you make a mistake as a result, we will take that into account when determining what action, if any, we should take.

Some of the information on this website applies to a specific financial year. This is clearly marked. Make sure you have the information for the right year before making decisions based on that information.

If you feel that our information does not fully cover your circumstances, or you are unsure how it applies to you, contact us or seek professional advice.

Copyright notice

© Australian Taxation Office for the Commonwealth of Australia

You are free to copy, adapt, modify, transmit and distribute this material as you wish (but not in any way that suggests the ATO or the Commonwealth endorses you or any of your services or products).