Law Enforcement Advisory Report

Demystifying Cryptocurrency Payment Processors

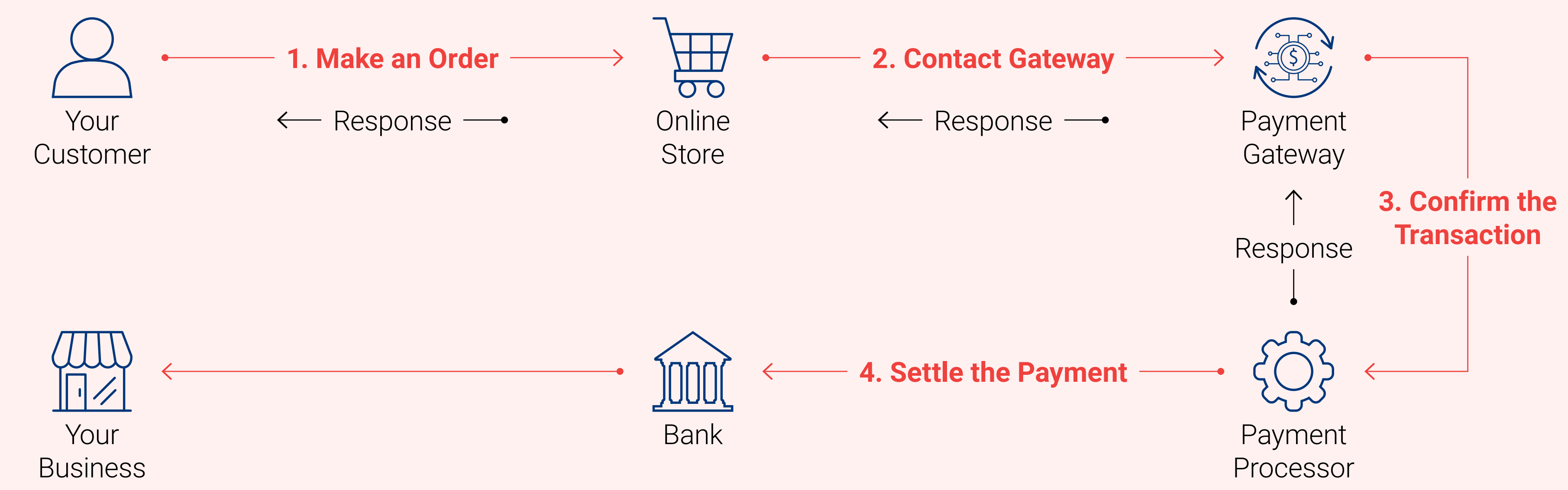
02
26

Demystifying Cryptocurrency Payment Processors

The utility of digital assets has grown significantly in the last decade, driven by greater adoption, investment, and online commerce. Parallel to this trend is the expansion of payment processor platforms that enable direct payments for goods or services using digital assets. While these platforms offer convenience and faster transactions, they can also be exploited to obscure and spend illicitly obtained digital assets or commit tax evasion.

Cryptocurrency payment processors act as intermediaries between a customer and a business merchant account. Also sometimes called payment gateways these services allow merchants to accept payments in cryptocurrencies. The business integrates the payment processor into their website or app, receives cryptocurrency, then the payment processor settles the transaction by converting the cryptocurrency into the business fiat of choice.[1] Withdrawals of cryptocurrency are also possible via cryptocurrency payment processors. Both customers and businesses benefit from transactions that occur in seconds or minutes. Cryptocurrency payment processors also allow for international payments that settle much faster than traditional processing. An additional benefit is the ease of use provided by integrating a cryptocurrency payment processor into a business payment system.[2]

How a Cryptocurrency Payment Gateway Works



The increased use of cryptocurrency payment processors implies that the use of cryptocurrencies to purchase goods and services is also on the rise. Recent market research suggests that the expected market size of cryptocurrency payment processors may increase from $1.2 billion U.S. dollars (USD) to $4.4 billion USD from 2024 to 2032.[3 4]

This increase in market relevance deserves increased awareness by law enforcement agencies and financial regulatory agencies.

CRYPTOCURRENCY PAYMENT PROCESSORS (CONTINUED)

[1] bvnk.com: 9 Best Cryptocurrency Payment Gateways for International Business bvnk.com/blog/best-crypto-payment-gateway

[2] alwin.io: Why are Businesses Adopting Crypto Payment Solutions alwin.io/why-businesses-adopting-crypto-payment-solutions

[3] gminsights.com: Crypto Payment Gateways Market gminsights.com/industry-analysis/crypto-payment-gateways-market

[4] All dollar amounts in this report are USD.

Demystifying Cryptocurrency Payment Processors (continued)

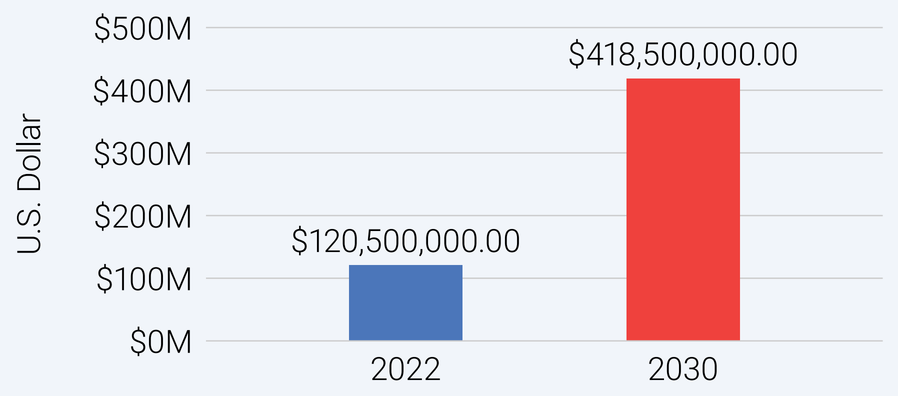
Desired Features: Off Ramps & Global Access

In recent years, luxury products have integrated cryptocurrency payment processors into their payment capabilities. Some of these include Rolls-Royce and Bentley dealers, Ferrari, Yacht brokerages, and luxury watches.[5 6 7 8] The ability to off-ramp cryptocurrency and purchase luxury goods can be an attractive concept for tax evaders and illicit actors who aim to use the proceeds of tax evasion, money laundering, and other financial crimes.

The ability to quickly transact across borders with lower costs than traditional payment options is a significant advantage for businesses, customers, and for global money laundering activity.

U.S. Cryptocurrency Payment Apps Market

Market Forecast to Grow at a Compound Annual Growth Rate (CAGR) of 17.0%



Source: https://www.researchandmarkets.com/report/united-states-cryptocurrency-wallet-market

Known Risks: Sanctions Evasion, Money Laundering

In 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) settled with Bitpay, a U.S.-based cryptocurrency payment processor, for violations of multiple sanctions programs. According to a U.S. Justice Department press release, in 2020, two brothers pleaded guilty to conspiring to launder money and operating an unlicensed money service business called Payza.com.[9] This payment processor was found to have processed over $250 million in illicit transactions. Payza served numerous merchants who facilitated Ponzi/pyramind schemes, tax evasion, money laundering and other financial crimes. Payza is a salient example of how cryptocurrency payment processors can be used as a vector for moving illicit funds.

Although they may be required by the Financial Crimes Enforcement Network (FinCEN) to file suspicious activity reports (SARs), some cryptocurrency payment processors may not be filing SARs.[10] At least one cryptocurrency payment processor has seen a significant increase in filings since 2021. This suggests that there may be gaps in visibility about potential tax evasion and money laundering activities occurring on these platforms.

CRYPTOCURRENCY PAYMENT PROCESSORS (PREVIOUS) | CRYPTOCURRENCY PAYMENT PROCESSORS (CONTINUED)

[5] inquisitr.com: Rolls-Royce, Bentley Car Dealer Accepts Bitcoin as Payment inquisitr.com/5062056/rolls-royce-bentley-car-dealer-now-accepts-bitcoin-as-payment

[6] eukapay.com: Yachting Entropia Integrates EukaPay's Cryptocurrency Payment Processing Solution for a Seamless Payment Experience eukapay.com/blog/yachting-entropia-integrates-eukapays-cryptocurrency-payment-processing-solution-for-a-seamless-payment-experience

[7] reuters.com: Ferrari to accept crypto as payment for its cars in the US reuters.com/business/autos-transportation/ferrari-accept-crypto-payment-its-cars-us-2023-10-14

[8] theblock.co: Luxury watchmaker TAG Heuer inks deal with BitPay to accept crypto online in the US theblock.co/post/147849/luxury-watchmaker-tag-heuer-inks-deal-with-bitpay-to-accept-crypto-online-in-the-us

[9] justice.gov: Two Canadian Brothers and their Company, Payza, Sentenced for Conspiring to Launder Money Service Business justice.gov/usao-dc/pr/two-canadian-brothers-and-their-company-payza-sentenced-conspiring-launder-money-service

[10] SARs are the U.S. and U.K. equivalents of Suspicious Transaction Reports (STRs) in Canada and the Netherlands and Suspicious Matter Reports (SMRs) in Australia.

Demystifying Cryptocurrency Payment Processors (continued)

Rising Trend: SARs

The number of SARs filed to FinCEN related to cryptocurrency payment processors has exhibited a significant and sustained increase over the past five years.

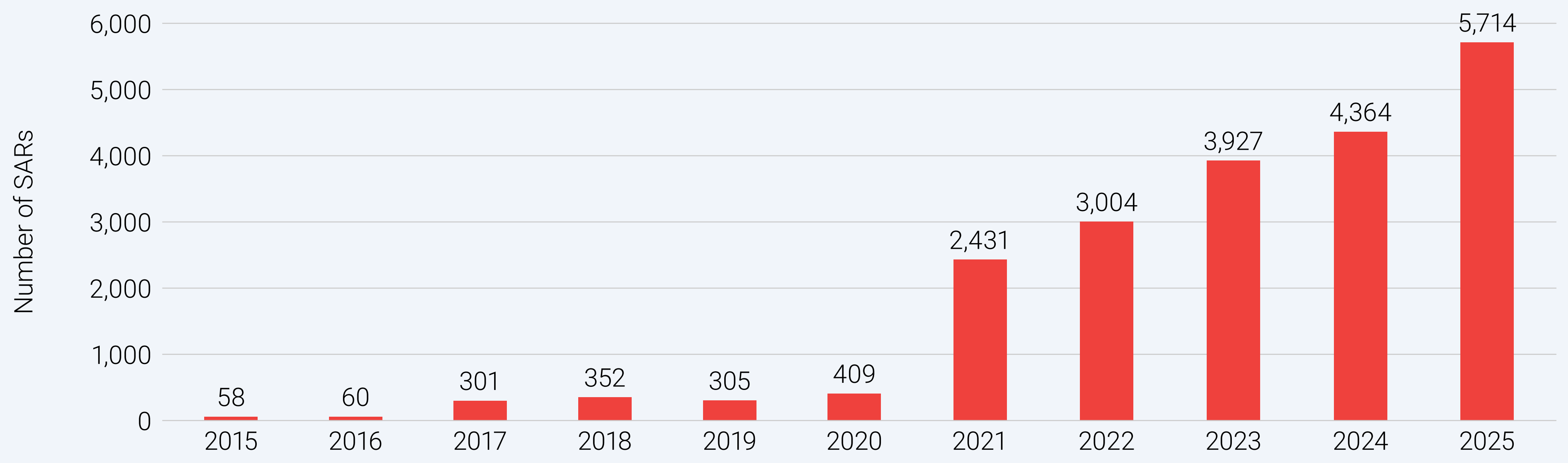
A sampling of cryptocurrency payment processors referenced in SARs demonstrates a growing trend in their use in potential tax evasion, money laundering, and other financial crimes. This trend combined with the lack of SAR filings by cryptocurrency payment processors suggests that these entities may be increasingly used to facilitate tax evasion, money laundering, and other financial crimes.

From 2020 to 2024, SARs related to cryptocurrency payment processors increased by over 1000%. To date, financial institutions and digital asset service providers have reported to FinCEN over $5 billion in suspicious activity related to cryptocurrency payment processors.

The trend of increasing SARs provides law enforcement with an opportunity to dive deeper into the reported data, enabling the identification and targeting of SARs that may be associated with tax evasion, money laundering, and other financial crimes.

CRYPTOCURRENCY PAYMENT PROCESSORS (PREVIOUS)

Number of SARs Filed to FinCEN Related to Cryptocurrency Payment Processors from 2015 through 2025



Source: FinCEN Data from 2015 through 2025

Enhancing Law Enforcement Strategies

The Joint Chiefs of Global Tax Enforcement (J5) emphasizes the importance of law enforcement agencies accessing financial intelligence unit (FIU) data with the focus of revealing cryptocurrency payment processors as a vector for the illicit movement of funds. These keyword searches can aid in identifying SARs that document alleged instances of tax evasion, money laundering, or other illicit transactions facilitated by cryptocurrency payment processors in their narratives.

Effective use of FIU data and targeted searches can aid law enforcement in identifying potential leads for investigation, disrupting illegal activities, developing intelligence of emerging threats and trends, and enhancing their understanding of the cryptocurrency landscape and its vulnerabilities.

Leveraging Targeted FIU Searches

Some of the best practices for targeting potential tax evasion, money laundering, and other financial crimes involving cryptocurrency payment processors include creating search terms using synonyms like "cryptocurrency," "virtual assets," and "digital currency" to capture different terminology used by financial institutions reporting the SARs. Combining these terms with terms related to payment processors like "payment gateway," "payment solution," "merchant payment," or "payment processing" can create targeted searches that can identify relevant SARs.

These searches can help identify suspicious transactions or patterns indicative of tax evasion or money laundering, individuals or entities using cryptocurrency payment processors to circumvent reporting requirements. Targeted searches can assist in the beginning stages of disrupting the illicit use of cryptocurrency payment processors.

Targeted Keyword Searches for Cryptocurrency Payment Processor SARs

1. Cryptocurrency Payment Processor
2. Crypto Payment Solution
3. Crypto Payment Gateway
4. Digital Asset Processing
5. Payment Processor
6. Merchant Services

Note: The recommendations are meant to be used in conjunction with other investigative techniques and tools and should be tailored to the specific needs of the agency.

Protecting the Financial System

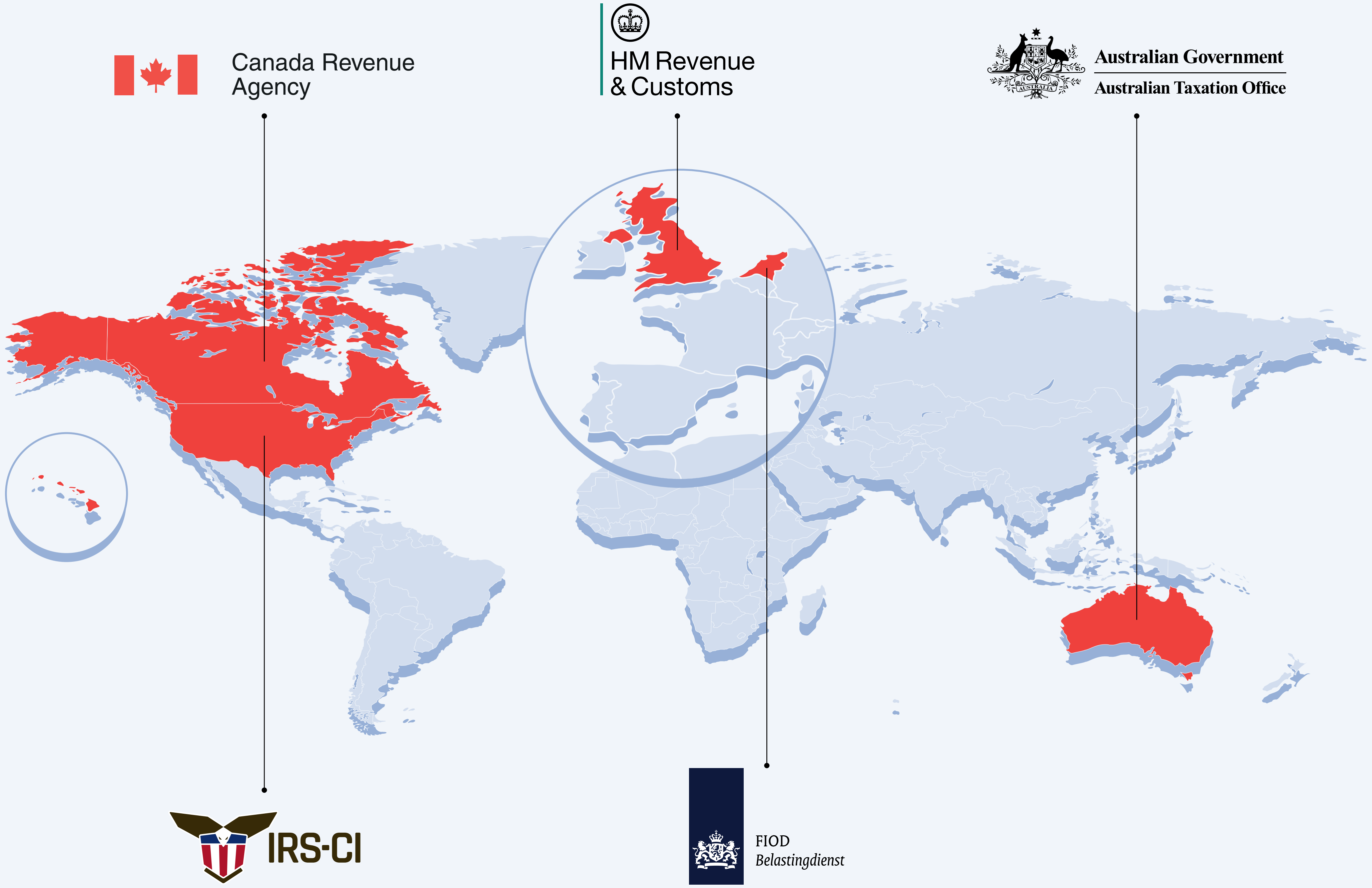
Cryptocurrency payment processors pose significant risks and unknown threats to the integrity of the global financial system. The use of cryptocurrency payment processors can allow bad actors to off-ramp illicit funds on a global scale and realize the benefits of their tax evasion, money laundering, and other financial crimes. Although anti-money laundering (AML)/know your customer (KYC) measures might be adopted by these entities, risks remain that merchants and customers are using these services to facilitate tax evasion, money laundering, and other financial crimes. While the United States' Bank Secrecy Act requires anti-money laundering compliance programs, examples have shown that these measures can be defeated, implemented improperly, or not implemented at all. This requires increased attention by law enforcement agencies to monitor these entities. This J5 report illuminates the utility of cryptocurrency payment processors and why illicit actors would use these services to facilitate and further obfuscate the flow of illicit funds. This J5 report also provides insights to enhance the detection of tax evasion and money laundering by understanding the risks associated with cryptocurrency payment processors and by the targeted SAR search words enabling law enforcement and FIUs to conduct more effective investigations. By working together and sharing intelligence, the J5 combats financial crime and promotes tax transparency in the evolving digital asset landscape.

About the J5

The J5 leads the fight against international tax crime and money laundering, including digital asset threats and those who undertake, enable, or facilitate global tax evasion. The J5 works together to gather information, share intelligence, and conduct coordinated operations against transnational financial crimes. The J5 includes the Australian Taxation Office, the Canada Revenue Agency, the Dutch Fiscal Intelligence and Investigation Service, His Majesty's Revenue and Customs from the U.K. and IRS Criminal Investigation from the U.S.

The J5 Cyber Group seeks to identify and work the largest, most impactful digital assets related cybercrime investigations in the world related to tax evasion, money laundering, and other related financial crime. Inquiries and tips can be sent to J5Cyber@ci.irs.gov.

For more information about the J5, please visit j5alliance.global.



JOINT CHIEFS OF GLOBAL TAX ENFORCEMENT