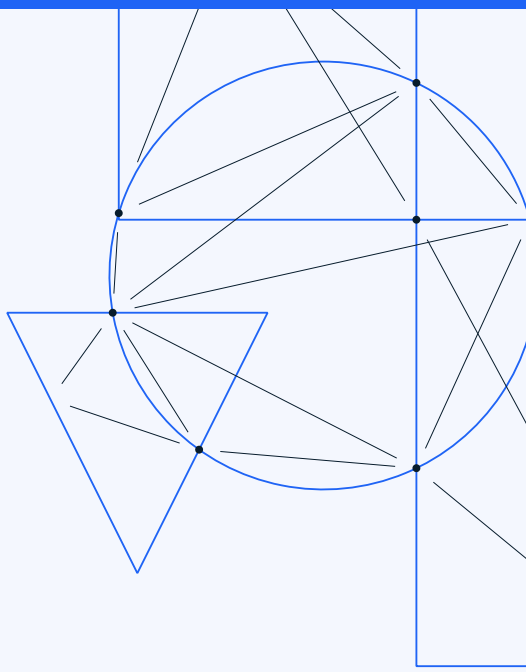
TRM

7 Pillars of Highly Effective Tax Agencies

Pillar 4: Case Selection Modeling



Many tax authorities around the globe struggle with limited resources. And they need to deploy those resources as efficiently as possible (particularly when it comes to enforcement) to best ensure compliance, maximize revenue collection, and deter tax evasion – especially in the rapidly evolving landscape of digital assets and decentralized finance.

Tax authorities should seek to modernize their examination and enforcement capabilities by identifying various risk levels of non-compliance, then use that information to allocate investigative resources. **The fourth pillar in scaling your crypto tax operations is through this process of case selection modeling.**

Case selection modeling optimizes efficiency and consistency for tax authorities

Using blockchain intelligence analytics, the objective of case selection modeling is to design a centralized **risk-based framework and methodology** to identify subsets of taxpayers exhibiting behaviors or signals that are indicative of tax noncompliance, aggressive avoidance, or tax fraud.

A case selection model based on both **data centralization** and **data-driven analytics** can enable tax authorities to create a process that optimizes both efficiency and consistency in the use of audit and examination resources. This model allows a tax authority to prioritize the highest risk cases and better understand the margin of error associated with each risk score.

Understanding the expected risk — as well as the variance on that expected risk — are key factors that tax authorities need to consider when determining whether a case should be put in a criminal or civil investigation workstream, as well as the type of workstream involved. The IRS, Canadian Revenue Authority, and others have been some of the first tax authorities to conceptualize this notion and put it into practice.

The role of blockchain intelligence in case selection modeling

Tax authorities across the globe possess varying degrees of technological capacity, which may create reservations with implementing measures like case selection monitoring. However, these frameworks don't need to be overly complicated, and may take many different forms based on the sophistication of the tax authority's existing capabilities and processes.

For example, a tax authority may have a relatively small number of wallet addresses obtained from an exchange, whistleblower, or investigation that originated in another law enforcement department. With relative ease, blockchain intelligence tools can perform bulk data analyses on those addresses to determine how much value sits in each one, what exchanges those addresses are connected to, and whether any of them have links to illicit finance categories such as darknet marketplaces, sanctioned entities, gambling establishments, or cybercriminal networks.

These enriched data points on crypto wallets and transactions enable tax authorities to quickly prioritize potential cases without exponentially increasing headcount. Ultimately, tax authorities can implement a framework that aligns with the level of data available and depth of detail needed. When coupled with additional data points tax authorities already possess, these frameworks can become even more dynamic, ingesting many complex inputs from a variety of sources and scaling the analysis across many thousands of addresses.

Using risk profiles to prioritize case work

In an ideal scenario, tax authorities can use the available data to design several high-risk behavioral profiles for noncompliance, depending on specific tax code parameters, available data, and targeted compliance needs.

One type of risk profile that may align with underreporting crypto asset income in the US may include a common set of factors or patterns, surfaced through multiple data sources. For instance:

- Taxpayer A reports gains and losses from a few crypto assets traded on one specific exchange through a Form 8949
- Taxpayer A's personal identifying information also matches the records received from a separate exchange via third-party reporting, and those records indicate undisclosed deposit and withdrawal activity to a separate unhosted wallet address
- That unhosted wallet address includes activity for the same tax year, involving a larger set of assets than what was disclosed in the Form 8949 filing, as well as information indicating activity at other undisclosed crypto exchanges, DeFi protocols, and mining pools

Using available data, a tax authority can flag this taxpayer for possible further examination — along with other similar taxpayers that exhibit the same structural pattern. Additional data elements relating to the value involved or whether the taxpayer engaged with high-risk wallets on-chain can then be incorporated to determine what type of compliance workstream taxpayer should be routed through: civil or criminal.

Importantly, due to the nature of blockchain data being open and public, blockchain intelligence tools provide a unique way to enable a kind of **on-chain fingerprinting** of transactional patterns that may be indicative of noncompliance. And the case selection modeling process is the fulcrum to identify these compliance cases, now ready to be assigned out. These patterns can also serve as a feedback loop for broadening taxpayer education and industry engagement in crypto, where patterns or trends of noncompliance begin to reveal themselves at scale.

> Ultimately, the output of any case selection design will ideally provide tax authorities with a manageable number of cases and a triage process ready for referral or further preparation for audits, notice letters, or other forms of civil or criminal proceedings.

Additionally, public awareness of the ability of the tax authority to pursue such matters provides a significant deterrent impact on many other similarly-situated taxpayers.