The J5 Sounds the Alarm: Fintech's Double-Edged Sword in Global Tax Enforcement

By Sandra R. Brown and Philipp Behrendt

In a coordinated move that should command the attention of financial institutions, fintech startups, crypto platforms, and tax professionals alike, on June 10, 2025, the Joint Chiefs of Global Tax Enforcement (J5) released a trilogy of threat assessments aimed at exposing how emerging technologies are facilitating global financial crimes, including tax evasion. These reports, developed through the J5's Global Financial Institutions Partnership (GFIP), provide a sobering view of how financial technology (fintech), identity-based fraud, and trade-based money laundering are increasingly undermining tax enforcement efforts. Of particular interest to taxpayers, financial professionals, and digital asset platforms is the report titled *Misuse of Fintech to Enable Tax Evasion and Money Laundering* (dated May 2025), which synthesizes both empirical observations and literature reviews to show how fintech is being exploited to move untaxed income across borders, anonymize financial flows, and bypass regulatory safeguards.

For those unfamiliar with the J5, the J5 is a coalition of tax enforcement agencies from the U.S., U.K., Australia, Canada, and the Netherlands. An overview of what the Joint Global Tax Force, known as J5, means for international criminal tax enforcement can be found at this linked article.

Their most recent reports, published under the J5's Global Financial Institutions Partnership (GFIP), detail typologies and red flags in the use of financial technology for illicit purposes. These aren't theoretical concerns—they're based on real-world investigations and emerging threat trends observed across jurisdictions.

Key Findings: Four Ways Fintech Is Being Misused

The J5's fintech report identifies four principal methods by which criminals are misusing technology to commit tax crimes:

1. **Nested and Pseudo-Banking Services.** Payment service providers (PSPs) and neobanks embedded within traditional banking infrastructure obscure ultimate account holders, reducing transaction visibility for regulators and auditors. The report mentions Virtual Bank Accounts (VBAs). VBAs are pseudo-account numbers that redirect incoming payments to a traditional bank account, allowing users to receive funds without disclosing their primary account details. Often used by fintech platforms and merchants, VBAs can obscure the identity of the true account holder, posing challenges for tax transparency and anti-money laundering enforcement.

2. **Virtual Assets and Pseudo-Anonymity.** Cryptocurrencies, mixers, privacy coins, unhosted wallets, and cross-chain bridges are facilitating pseudonymous storage and transfer of illicit funds. Peel chain layering and co-mingling are common techniques that are often abused to enhance anonymity in crypto-based tax evasion and money laundering schemes. Peel chain layering involves breaking a large cryptocurrency holding into smaller amounts through a series of rapid, automated transactions. With each "peel," a small portion is sent to a new address, making it harder for investigators to trace the origin of the funds and detect a taxable

event. The repeated layering mimics legitimate user behavior and frustrates blockchain analysis. Co-mingling refers to the deliberate mixing of illicit and legitimate funds—often within shared wallets, exchanges, or mixing services—to obscure the source and nature of transactions. This tactic helps conceal taxable income by making it difficult to distinguish between clean and dirty assets, especially when combined with privacy coins or unhosted wallets.

3. **Fiat On- and Off-Ramps.** Crypto ATMs, centralized exchanges, and sometimes even peer-to-peer exchanges allow transfer of funds to or from fiat currency without being traceable on the blockchain once they hit these services.

4. **Storing Undeclared Income.** NFTs and USD-pegged stablecoins serve as new-age safe havens for untaxed wealth.

These tools are not inherently illicit—many serve legitimate purposes. But their misuse is rapidly outpacing regulatory safeguards, particularly where AML and KYC frameworks remain underdeveloped or inconsistently applied.

Several services operate across the four typologies, blurring the lines between categories. For example, stablecoins, crypto prepaid cards, and debit cards linked to virtual assets can serve dual functions. These tools are misused to convert between digital assets and fiat currency, effectively bypassing tax authorities' ability to trace transactions. In addition to facilitating on- and off-ramping, they can also be used to store illicit or undeclared income, further complicating enforcement and compliance efforts.

Systemic Vulnerabilities: The "Perfect Storm"

The J5 partners also warn of six systemic vulnerabilities:

- **Speed and volume of transactions** via digital rails overwhelm traditional enforcement tools.
- **Borderless movement of funds** through decentralized systems undermines jurisdictional oversight.
- **Anonymity features**, such as mixers and privacy wallets, are abused to frustrate audit trails.
- **Underdeveloped AML compliance**, especially in emerging fintechs.
- **Regulatory fragmentation**, with inconsistent standards across borders.
- **Obfuscation via nested services**, where PSPs provide cover for illicit actors by operating under legitimate financial umbrellas.

A Legal Crossroads for Fintech and Tax Enforcement

The implications are vast. For criminal tax practitioners, these developments signal a renewed enforcement posture—and the likelihood of future indictments that combine digital asset tracing with tax fraud and money laundering charges.

For civil litigators, CPAs, and financial advisors, the growing expectation is that businesses implement fintech-specific compliance protocols and treat AML/KYC obligations as essential tax

controls. Clients under audit who have used services the J5 flagged should seek guidance from professionals well-versed in the tax and regulatory implications of these tools. These services can be easily misunderstood by auditors, especially when transaction patterns resemble known tax evasion typologies. For example, a client who transferred assets through multiple wallets using a peel chain pattern may have done so for operational or security reasons, not to conceal income. Without proper context, however, the IRS may interpret these transactions as deliberate layering to hide the source of funds. A knowledgeable advisor can help craft a communication strategy that clearly explains the legitimate use of such services and distinguishes it from illicit activity.

Closing Thoughts

The J5's reports are not merely regulatory white papers—they are enforcement roadmaps. The integration of technology into financial services is irreversible, but so too is the resolve of global tax agencies to keep pace.

For clients operating in this space, tax compliance can no longer be an afterthought. Since at least from mid-2023, the J5's Cyber Group has substantially escalated its campaign against crypto-enabled tax evasion—a theme made clear in the July 25, 2024 report from IRS-CI titled *The J5 Report*. That report emphasizes the group's annual "Crypto Challenge" events—collaborative Investigations that have yielded over 100 leads and launched more than 10 active operations directly tied to cryptocurrency tax schemes. Notably, IRS-CI and FIOD have already seized more than $25 million in crypto assets, resulting in over $333 million in asset forfeitures connected to various tax evasion and money laundering cases. This demonstrates that the J5 is no longer limited to advisory warnings—it is now aggressively dismantling real-world crypto networks, leveraging global partnerships to trace pseudonymous transactions and bring criminal enforcement home.