Crypto Scam Losses Are Heading to Court[1]

by Philipp Behrendt

On April 6, 2026, the FBI released its 2025 Internet Crime Report, which states that in 2025 the Internet Crime Complaint Center received 1,088,597 complaints of cyber-enabled crimes that cost Americans almost $21 billion. The largest number of complaints involved cryptocurrency, where there were 181,565 complaints involving more than $11 billion in losses.

People defrauded by crypto scammer who claim a theft loss of their tax returns can find their claims rejected by the IRS because they failed to prove that the loss was not a bad investment, a personal misfortune, or an unsubstantiated disappearance of funds, but a theft loss deductible under Internal Revenue Code section 165. Two recently filed cases—*Fry v. Commissioner*, No. 2838-26 (T.C. filed Apr. 16, 2026), and *Vaia v. United States*, No. 2:26-cv-00573 (S.D. Ohio filed May 12, 2026)—highlight the issues taxpayers and practitioners should expect to litigate on behalf of clients who are the victims of modern scams, such as "pig butchering" schemes: profit motive, state-law theft, timing, basis, reasonable prospect of recovery, Form 4684 reporting, and the limits of the Ponzi-loss safe harbor.

Both cases are in the pleading stage. The facts described below are allegations from the pleadings. But the cases are important because they allege facts similar to those addressed by IRS Chief Counsel Advice 202511015, which concluded that some scam victims may deduct theft losses when the loss arises from a transaction entered into for profit, while other victims—such as victims of romance or kidnapping scams—may be barred by the TCJA limitation on personal casualty and theft losses. I.R.S. C.C.A. 202511015 (Jan. 17, 2025, released Mar. 14, 2025).

What Is Pig Butchering?

"Pig butchering" is the term commonly used for a long-con investment scam in which fraudsters "fatten" the victim with trust, fake investment performance, and sometimes small early withdrawals before extracting larger deposits. The FBI describes cryptocurrency investment fraud, commonly called pig butchering, as one of today's most prevalent and

[1] *The information provided in this blog is for general informational and educational purposes only. It does not constitute professional tax, accounting, financial or legal advice and cannot be construed as legal representation. You should always consult with a qualified tax professional regarding your specific situation.*

damaging fraud schemes. Scammers convince victims to deposit increasing amounts into fake "investment" platforms; in reality, the money is controlled by criminal actors, often overseas, and victims typically lose all amounts transferred. The perpetrators of the fraud are often unknown, and the stolen funds are typically transferred to overseas accounts.

The mechanics are familiar. A victim may be approached through social media, text message, dating apps, WhatsApp, Telegram, fake investment groups, online advertisements, or even app stores. The relationship may be romantic, professional, or purely investment oriented. Once trust is established, the victim is directed to a platform that appears legitimate and shows account balances growing in real time. The victim may even be allowed to withdraw a small amount, reinforcing the appearance of legitimacy. Later, when the victim attempts to withdraw the larger "balance," the scammer demands additional deposits for taxes, margin, unlock fees, compliance fees, anti-money-laundering clearance, or similar fabricated charges. Those payments are not fees to release funds; they are usually the final stage of the theft.

Crypto matters because it makes the scam easier to execute and harder to unwind. Transfers can move quickly across exchanges, wallets, bridges, and offshore platforms. Victims often do not know whether they sent fiat, bitcoin, ether, stablecoins, or some combination. They may have transaction hashes but no meaningful counterparty information. The blockchain may preserve a trail, but that trail itself does not identify the scammer, compel an offshore exchange to cooperate, or create a realistic recovery. Chainalysis has reported that Southeast Asia-based scam operations caused at least $10 billion in losses to Americans in 2024, and that these schemes frequently rely on bitcoin, ether, and stablecoins deposited into fraudulent investment platforms.

The Tax Rule: Section 165 Still Matters, but TCJA Changed the Stakes.

Section 165(a) allows a deduction for losses sustained during the taxable year and not compensated for by insurance or otherwise. For individuals, however, section 165(c) limits deductible losses to three categories: losses incurred in a trade or business, losses incurred in a transaction entered into for profit, and certain casualty or theft losses. I.R.C. § 165(a), (c). A theft loss is treated as sustained in the year the taxpayer discovers the theft. I.R.C. § 165(e). But the loss is not deductible if, at year end, the taxpayer has a reasonable prospect of recovery. Treas. Reg. §§ 1.165-1(d)(2), 1.165-8(a)(2).

The TCJA made the distinction between investment scams and personal scams critical. For the years at issue in *Fry* and *Vaia*, personal casualty and theft losses generally are not

deductible unless attributable to a federally declared disaster or offset by personal casualty gains. But that limitation does not bar theft losses incurred in a transaction entered into for profit. IRS Publication 547 now expressly recognizes that victims of financial scams involving a transaction entered into for profit may be able to claim a theft loss deduction if the loss resulted from criminal conduct classified as theft under applicable state law, the taxpayer had no reasonable prospect of recovering the funds, and the loss arose from a transaction entered into for profit.

The theft element is not satisfied merely because the money disappeared. For section 165 purposes, theft is broadly defined to include criminal appropriation by swindling, false pretenses, or other guile. Rev. Rul. 2009-9, 2009-14 I.R.B. 735; Treas. Reg. § 1.165-8(d). But the taxpayer must establish that a theft occurred under applicable state law. *Vennes v. Commissioner*, T.C. Memo. 2021-93, at *28–29. "Theft" is broadly defined to include larceny, embezzlement, and robbery. Sec. 1.165-8(d) A conviction is not required, but the taxpayer must prove the theft.

The timing issue is equally important. A theft loss is generally sustained in the year of discovery, but is deductible only in the year in which there is no reasonable prospect of recovery. A reasonable prospect exists when the taxpayer has bona fide claims for recoupment and a substantial possibility of recovery. *Ramsey Scarlett & Co. v. Commissioner*, 61 T.C. 795, 811 (1974), aff'd, 521 F.2d 786 (4th Cir. 1975). The taxpayer need not be an "incorrigible optimist." *Id*.

The amount of the loss is another practical trap. The deduction is generally limited to the taxpayer's adjusted basis in the stolen property, not any account balance shown on the fake platform. I.R.C. § 165(b); Treas. Reg. § 1.165-1(c). If a platform shows a $900,000 deposit growing to $6 million, the taxpayer generally does not have a $6 million theft loss unless the phantom appreciation was previously included in income or otherwise gave rise to basis. The CCA 202511015 emphasizes that the allowable theft loss is the victim's basis in the stolen funds, not the fair market value of fictitious gains.

Chief Counsel Advice 202511015: The IRS's Roadmap

Chief Counsel Advice 202511015 is not precedent, but it is the most important current IRS discussion of scam losses under section 165. The CCA considered five scam scenarios and concluded that all five involved thefts under section 165, but only three produced deductible theft losses because only those three arose from a transaction entered into for profit. The pig-butchering example was one of the deductible scenarios.

The CCA's pig-butchering scenario involved a taxpayer who received an unsolicited email advertising a cryptocurrency investment opportunity promising large profits. The taxpayer made a small investment, saw the account balance increase, and successfully withdrew funds. That apparent success induced larger transfers from IRA and non-IRA accounts. When the taxpayer later attempted to withdraw, the platform failed, customer support disappeared, and the taxpayer discovered that others had been defrauded. Law enforcement and the financial institution advised that there was little to no prospect of recovery. On those facts, Chief Counsel concluded that the taxpayer's loss was incurred in a transaction entered into for profit under section 165(c)(2) and was deductible in the discovery year.

The CCA also claims that most pig-butchering victims cannot use the Ponzi-loss safe harbor of Rev. Proc. 2009-20, which provides a favorable safe harbor for certain "specified fraudulent arrangements" that generally requires a lead figure who has been charged by indictment or information, or is the subject of a qualifying criminal complaint. In many crypto scam cases, the perpetrators are unidentified, overseas, or operating through false names. That may not defeat the theft-loss claim itself, but it often defeats the safe harbor. Rev. Proc. 2009-20, 2009-14 I.R.B. 749; Rev. Proc. 2011-58, 2011-50 I.R.B. 849. A taxpayer may not qualify for the safe harbor but still prevail under the ordinary section 165 rules by proving theft, profit motive, basis, discovery year, and no reasonable prospect of recovery.

Although C.C.A. 202511015 is important as an expression of the Service's current view, it is not binding precedent, see I.R.C. § 6110(k)(3), and the pending cases are likely to test the pressure points in its analysis: whether the facts establish "theft" under applicable state law, whether the transfers were made in a transaction entered into for profit under § 165(c)(2) rather than as part of a nondeductible personal loss under § 165(c)(3) and (h)(5), whether the taxpayer discovered the loss in the claimed year and then had no reasonable prospect of recovery, and whether the claimed deduction is properly limited to basis rather than fictitious platform gains.

***Fry v. Commissioner*: A Tax Court Deficiency Case.**

In *Fry*, the taxpayers petitioned the Tax Court for redetermination of a 2022 deficiency. According to the petition, the IRS issued a notice of deficiency asserting $322,529 of income tax and a $64,505.80 accuracy-related penalty under section 6662(a). The deficiency allegedly arose from the IRS's disallowance of a $958,540 deduction claimed as "Other Miscellaneous Deductions" on the taxpayers' 2022 Form 1040. The taxpayers contend the deduction was proper under section 165 because the money was lost by theft.

The alleged facts read like a classic pig-butchering case. The taxpayers believed they were investing in cryptocurrency—identified as TASE—through a trading platform called SBIcoin. The petition alleges SBIcoin was not legitimate but instead solicited funds for purported income-producing investments. SBIcoin allegedly displayed investment growth in real time, represented that it was "legal and compliant," and promised that the taxpayers could withdraw funds after a one-to-three-month "protection period."

When the taxpayers later tried to cash out after seeing their purported TASE holdings grow to $6.4 million, SBIcoin allegedly demanded a $660,000 "margin fee" before allowing withdrawal. SBIcoin also allegedly threatened "court summons" or credit-score damage if payment was delayed. After several "margin fee" payments, the online storefront disappeared, and the taxpayers allegedly lost 100% of the $958,540 transferred to SBIcoin.

The petition pleads several facts designed to satisfy section 165. It alleges no reasonable prospect of recovery, filing of Form 4684 with the 2022 return, a later FBI report, and a violation of California Penal Code section 532, California's false-pretenses statute. It also alleges that the taxpayers "erroneously relied" on Rev. Proc. 2009-20 but nevertheless sustained a deductible theft loss under section 165.

The legal issues are predictable but important. First, was there a theft under California law? Second, was the transaction entered into for profit? Third, was 2022 the correct discovery year? Fourth, did the taxpayers have no reasonable prospect of recovery by the end of 2022? Fifth, what was the taxpayer's basis on the funds that were lost? Sixth, does the reporting as "Other Miscellaneous Deductions" create a technical problem, or is the substance preserved through Form 4684 and the section 165 claim? Finally, the section 6662 penalty raises the issues of whether victims who were deceived by a sophisticated fake platform act with reasonable cause and in good faith in claiming a theft loss deduction. See I.R.C. §§ 6662, 6664(c).

***Vaia v. United States*: A Refund Suit.**

Vaia comes to court in a different procedural posture. The taxpayer filed a refund complaint in the Southern District of Ohio seeking recovery of federal income tax for 2024. The complaint alleges jurisdiction under 28 U.S.C. § 1346 and I.R.C. § 7422.

According to the complaint, the taxpayer was the victim of a pig-butchering scam in 2023–2024. He allegedly transferred approximately $824,740 over about ten months to what was represented as a legitimate cryptocurrency investment platform. He made the transfers with the intent and expectation of earning a profit. In May 2024, when he attempted to withdraw

funds, access was denied, and the perpetrators ceased communication. The platform then became inaccessible.

The complaint further alleges that the taxpayer reported the fraud to law enforcement and regulatory authorities in June 2024 and was informed that there was little to no prospect of recovery. It alleges that he had no insurance or other reimbursement and recovered nothing. It also alleges that the perpetrators were never identified or apprehended and that no criminal charges were filed.

The taxpayer then filed a 2024 Form 1040-X on or about July 24, 2025, claiming a $136,846 refund based on the $824,740 theft loss. The complaint alleges that Form 4684 was attached, along with a written explanation and supporting documentation, including transaction records, communications with the perpetrator, and law-enforcement reports. The IRS allegedly denied the refund claim, leading to the refund suit.

Unlike *Fry*, *Vaia* appears to present a clean refund posture: no deficiency proceeding, no asserted accuracy-related penalty in the pleading, and a direct allegation that the taxpayer filed Form 4684 and provided documentation. The court will need to decide whether the taxpayer has sufficiently proven theft under applicable law, profit motive under section 165(c)(2), the correct discovery year, the absence of a reasonable prospect of recovery, and the amount of basis in the stolen funds.

The Obstacles Victims Face.

The central difficulty for victims is that the tax system does not simply ask whether the taxpayer was harmed. It asks whether the harm fits a statutory category. After the TCJA, that category matters enormously. A taxpayer who lost money in a fake investment may have a deductible section 165(c)(2) theft loss; a taxpayer who lost money in a non-investment romance scam may have a nondeductible personal theft loss. The economic devastation may be the same, but the tax result may differ.

Victims also face a proof problem. They often have screenshots, Telegram messages, WhatsApp chats, transaction hashes, bank wires, exchange confirmations, and fake account statements. But they may not have the scammer's true identity, a police arrest, a prosecutor's indictment, or a foreign exchange subpoena response. The law does not require a conviction, but it does require proof of a state-law theft. That means the administrative file should be built as if the case will be litigated: chronology, transfer trail, communications, platform screenshots, withdrawal-denial messages, law-enforcement reports, exchange records, wallet addresses, and a short legal analysis of the applicable theft statute.

While in the case of Fry and Vaia, it appears that the taxpayers wired US dollars, other schemes involve the exchange from cash into crypto and transferring the crypto to the perpetrator. Crypto also complicates the recovery analysis. On one hand, blockchain tracing may show where the funds went and sometimes support law enforcement action. On the other hand, the mere theoretical possibility of tracing does not necessarily create a reasonable prospect of recovery. The practical question is whether, as of the close of the tax year, the taxpayer had a bona fide claim with a substantial possibility of recovery. A report to IC3, an exchange freeze, or a blockchain analytics report may help document the taxpayer's efforts, but practitioners should be careful before concluding that every traceable transaction creates a meaningful recovery prospect.

Finally, the Ponzi safe harbor remains a trap. Many taxpayers and preparers hear "investment fraud" and assume Rev. Proc. 2009-20 applies. But the safe harbor is narrow. If the scammer is unknown and no lead figure has been charged, the taxpayer may need to proceed under the ordinary theft-loss rules. That is not fatal, but it requires more proof and less reliance on mechanical safe-harbor requirements.

Practitioner Takeaway.

Fry and *Vaia* show where crypto scam-loss litigation is going. Tax agencies require individualized, taxpayer specific proof, no matter how sympathetic the victim may be. Thus, Courts will be asked whether the taxpayer can prove a theft under state law, a primary profit motive, basis in the stolen property, the correct discovery year, and no reasonable prospect of recovery. The cases also illustrate that IRS guidance is helpful but not self-executing: even where C.C.A. 202511015 supports deductibility for investment-oriented pig-butchering losses, taxpayers still must build a factual record.

For practitioners, the lesson is straightforward. Treat the theft-loss claim like a controversy file from day one. Preserve the evidence, report the crime, document recovery efforts, trace the funds where feasible, identify the state-law theft theory, avoid claiming phantom platform gains, and use Form 4684 carefully. The tax law may provide relief for many crypto investment-fraud victims, but the deduction will turn on proof, not merely loss.

Philipp Behrendt *is a Principal at Hochman Salkin Toscher Perez P.C., licensed in California as well as in Germany and assists in advising clients in civil and criminal tax controversies as well as international money laundering investigations stemming from tax avoidance structures. He also focuses on the technical aspects involved in advising voluntary disclosures in connection with DeFis, NFTs, and other crypto assets. Philipp is a Liaison to the Young Lawyer Committee for the ABA Tax*

Section's Civil and Criminal Tax Penalties Committee and served on the Beverly Hills Bar Association's Barristers Board of Governors from 2022 to 2023. Philipp is the Chair of the Beverly Hills Bar Association's Tax Section and the Blockchain and Web3 Law Section.

For more information, please contact Philipp Behrendt at behrendt@taxlitigator.com