



Tax News and Industry Updates

2025
Volume 13, Issue 2

DHA

CPAs

LET'S START A CONVERSATION

We'd love to meet you, talk about your financial goals, and see if we're the right fit to help you get there.

952.448.4220 | cpa@dha-cpa.com

Inside This Issue

| | |
|--|---|
| Treasury Ordered to Cease Issuing and Accepting Paper Checks..... | 1 |
| Digital Asset Reporting..... | 2 |
| SSA Gets Rid of its No Phone Policy..... | 2 |
| IRS Can Share Taxpayer Information with Immigration Authorities..... | 2 |
| FinCEN Removes BOI Reporting for U.S. Companies..... | 3 |
| Business and Income-Producing Property Theft Losses..... | 4 |

Treasury Ordered to Cease Issuing and Accepting Paper Checks

Cross References

- <https://www.whitehouse.gov/fact-sheets/>

Phasing out paper checks. On March 25, 2025, President Donald J. Trump signed an Executive Order to modernize how the government handles money, switching from old-fashioned paper-based payments to fast, secure electronic payments.

- The Order mandates that, effective September 30, 2025, the federal government will cease issuing paper checks for all disbursements, including intragovernmental payments, benefits, vendor payments, and tax refunds.
- All executive departments and agencies must transition to modern, electronic funds transfer (EFT) methods like direct deposit, debit/credit card payments, digital wallets, and real-time transfers.

- Payments made to the federal government, such as fees, fines, loans, and taxes, must also be processed electronically where permissible under existing law.
- Treasury will phase out physical lockbox services and expedite electronic collection of federal receipts.
- A comprehensive public awareness campaign will be launched to inform federal payment recipients of the shift to electronic options and offer guidance on setting up digital payments.
- Exceptions will be made for people without banking or electronic payment access, certain emergency payments, certain law enforcement activities, and other special cases qualifying for an exception under the Order or other existing law.
- This Executive Order does not establish a Central Bank Digital Currency (CBDC).

Defending against financial fraud and improper payments. President Trump is cracking down on waste, fraud, and abuse in government by modernizing outdated paper-based payment systems that impose unnecessary costs, delays, and security risks.

- Paper-based payments, such as checks and money orders, impose unnecessary costs, delays, and risks of fraud, lost payments, theft, and inefficiencies.
- Mail theft complaints have increased substantially since 2020.
- Historically, Treasury checks are 16 times more likely to be reported lost or stolen, returned undeliverable, or altered than an electronic funds transfer.
- Maintaining the physical infrastructure and specialized technology for digitizing paper records cost the American taxpayer over \$657 million in fiscal year 2024 alone.

continued on next page

- Check fraud is becoming more common, with banks issuing about 680,000 reports of check fraud in 2022—nearly double the number from 2021.
- Digital payments are more efficient, less costly, and less vulnerable to fraud.



Digital Asset Reporting

Cross References

- Public Law 119-5, April 10, 2025

Signed into law on April 10, 2025, the law repeals the IRS regulation that would have required brokers to report gross proceeds from digital asset sales.

IRS regulations would have required brokers to file Form 1099-DA, *Digital Asset Proceeds From Broker Transactions*, with the IRS and issue a copy to taxpayers who engage in digital asset transactions. Critics of the IRS regulation claimed it would be burdensome for industry innovation. Industry experts, on the other hand, claim at least half of the country's digital asset transactions go unreported.

Note: According to the most recent IRS tax gap projection report, misreporting of income amounts subject to substantial information reporting and withholding is 1% of income. For amounts subject to substantial information reporting but not withholding, it is 6%. For income amounts subject to little or no information reporting, such as nonfarm sole proprietor income, it is 55%. Tax gap analyses have consistently shown each year that compliance is higher when amounts are subject to third-party information reporting. [IRS Publication 5869 (Rev. 10-2024)]



SSA Gets Rid of its No Phone Policy

Cross References

- ssa.gov/news/press/releases

After complaints from the public, Congress, advocates, and others, the Social Security Administration (SSA) has eliminated its no phone policy.

On March 18, 2025, the Social Security Administration (SSA) announced it would no longer allow identity verification over the phone. Applicants signing up for Social Security benefits would either have to set up and use their personal “my Social Security” account, which requires online identity proofing, or visit a local Social Security office to prove their identity in person.

On March 26, 2025, SSA updated its policy to allow individuals applying for Social Security Disability Insurance (SSDI), Medicare, or Supplemental Security Income (SSI) who cannot use a personal “my Social Security” account to complete their claim entirely over the telephone without the need to come into a local SSA office.

On April 12, 2025, SSA eliminated its no phone policy. Beginning April 14, 2025, SSA will allow individuals to complete all claim types via telephone.

The April 12, 2025 announcement states it is implementing enhanced fraud prevention tools for claims over the telephone. The enhanced technology enables SSA to identify suspicious activity in telephone claims by analyzing patterns and anomalies within a person's account. If irregularities are detected, the individual will be asked to complete in-person identity proofing to continue processing their claim. The announcement does not provide specifics or examples of what patterns or anomalies will require an applicant to prove his or her identity in person.



IRS Can Share Taxpayer Information with Immigration Authorities

Cross References

- *Centro De Trabajadores Unidos v. US Treasury*, DC District Court, April 7, 2025

The IRS issues Individual Taxpayer Identification Numbers (ITINs) to alien taxpayers for use in connection with filing requirements. A taxpayer must submit a Form W-7 to apply for an ITIN. The Form W-7 asks for information including an applicant's mailing and foreign address, country of citizen, type of United States visa, and date of entry into the United States. This information is considered to be tax return information under IRS regulations.

IRC section 6103 sets forth the general rule that tax return information shall be confidential. Tax return information includes a taxpayer's identity and any other data, received by, recorded by, prepared by, furnished to, or collected by the IRS with respect to a tax return or with respect to the determination of the existence, or possible existence, of liability under the Internal Revenue Code (IRC). The willful unauthorized disclosure and inspection of tax return information carries criminal penalties under IRC section 7213 and section 7213A.

IRC section 6103 contains numerous exceptions to the disclosure prohibition, including some that require disclosure of information. The exception relevant to this court case is IRC section 6103(i)(2) which states the IRS must provide requested tax return information to officers and employees of the requesting agency who are personally and directly engaged in preparation for a criminal proceeding, and investigation that may result in a proceeding, or a federal grand jury proceeding.

The agency must make a request that includes the following.

- 1) The taxpayer's name and address,
- 2) The relevant taxable periods,
- 3) The statutory authority for the criminal investigation, and
- 4) The reasons the tax return information is relevant to the investigation.

The disclosure must be solely for the use of the officers and employees personally and directly engaged in the criminal investigation or proceeding.

The agency receiving tax return information under IRC section 6103(i)(2) must follow stringent safeguards for protecting the information. Because the receiving agency is bound by the confidentiality mandate under IRC section 6103, redisclosures of tax return information must also be authorized under IRC section 6103. The receiving agency must establish and maintain a system of records that tracks its requests and the tax return information it receives. The records must be securely stored and access must be restricted to agency personnel whose duties require access and to whom disclosures may be made.

The plaintiffs in this case are four immigrant rights advocacy groups who filed suit to stop the IRS from providing tax return information to the Department of Homeland Security (DHS) and U.S. Immigration and Customs Enforcement (ICE).

A Memorandum of Understanding (MOU) signed by the Department of the Treasury and DHS reiterates the agencies' commitment to sharing information only in the way that IRC section 6103 permits. Some statutes impose criminal penalties for immigration-related offenses, such as up to 4 years imprisonment for willfully remaining in the United States for over 90 days after a final removal order is issued. An alien who illegally reenters the United States can be imprisoned for up to 2 years. As laid out in the MOU, DHS can legally request tax return information from the IRS relating to individuals under criminal investigation, and the IRS must provide it.

The court ruled in favor of the government because the conduct expressly contemplated in the MOU providing information to assist criminal investigations is lawful.



FinCEN Removes BOI Reporting for U.S. Companies

Cross References

- fincen.gov/news

Consistent with the U.S. Department of the Treasury's March 2, 2025 announcement, the Financial Crimes Enforcement Network (FinCEN) is issuing an interim final rule that removes the requirement for U.S. companies and U.S. persons to report beneficial ownership information (BOI) to FinCEN under the Corporate Transparency Act.

In that interim final rule, FinCEN revises the definition of "reporting company" in its implementing regulations to mean only those entities that are formed under the law of a foreign country and that have registered to do business in any U.S. state or tribal jurisdiction by the filing of a document with a secretary of state or similar office (formerly known as "foreign reporting companies"). FinCEN also exempts entities previously known as "domestic reporting companies" from BOI reporting requirements.

Thus, through this interim final rule, all entities created in the United States—including those previously known as "domestic reporting companies"—and their beneficial owners will be exempt from the requirement to report BOI to FinCEN. Foreign entities that meet the new definition of a "reporting company" and do not qualify for an exemption from the reporting requirements must report their BOI to FinCEN under new deadlines, detailed below. These foreign entities, however, will not be required to report any U.S. persons as beneficial owners, and U.S. persons will not be required to report BOI with respect to any such entity for which they are a beneficial owner.

Upon the publication of the interim final rule, the following deadlines apply for foreign entities that are reporting companies.

- Reporting companies registered to do business in the United States before the date of publication of the interim final rule must file BOI reports no later than 30 days from that date.
- Reporting companies registered to do business in the United States on or after the date of publication of the interim final rule have 30 calendar days to file an initial BOI report after receiving notice that their registration is effective.

FinCEN is accepting comments on this interim final rule and intends to finalize the rule this year.



Business and Income-Producing Property Theft Losses

Cross References

- IRC §165
- Form 4684, *Casualties and Thefts*
- ILM 202511015, January 17, 2025

For tax years 2018 through 2025, personal casualty and theft loss of personal-use property for an individual is deductible only if attributable to a federally-declared disaster. An exception applies if the taxpayer has personal casualty gains for the tax year. Deductible personal casualty and theft losses are also subject to a \$100 per event reduction, plus a 10% of adjusted gross income (AGI) reduction for combined casualty and theft losses for the year.

These limitations do not apply to business and income-producing property casualty and theft losses. Casualty and theft losses on business and income-producing property are reported in Part I, Section B of Form 4684, *Casualties and Thefts*. A business and income producing property casualty and theft loss is the lesser of:

- The taxpayer's adjusted basis in the property (cost or other basis minus depreciation allowed or allowable, including Section 179 and special depreciation), or
- The reduction in FMV due to the casualty or theft.
- Minus any insurance or reimbursement received or expected.

The loss is calculated separately for each item, including personal loss for mixed-use property. There is no \$100 per event reduction and no 10% of AGI reduction.

If business or income-producing property is stolen or completely destroyed, the decrease in FMV is not considered, and the loss is calculated as follows.

- Adjusted basis of property
- Minus salvage value of the property
- Minus any insurance or reimbursement received or expected.

Form 4684, Section C provides a special safe harbor for reporting for criminal fraud victims of Ponzi-Type investment schemes.

The IRS recently released a legal memorandum concluding that some victims of scams may be allowed to deduct theft losses of income-producing property. The legal memorandum included 5 examples illustrating when a scam is considered a personal casualty and theft loss vs. an income-producing property casualty and theft loss.

Example #1, compromised account scam. Taxpayer 1 was the victim of a compromised account scam involving an impersonator. Scammer A contacted Taxpayer 1 claiming to be a "fraud specialist" at Taxpayer 1's financial institution. Scammer A stated that Taxpayer 1's computer and bank accounts had been compromised and attempts were made to withdraw funds. Having gained Taxpayer 1's trust and created a sense of urgency, Scammer A fraudulently induced Taxpayer 1 to authorize distributions from IRA and non-IRA accounts and to transfer all the funds into new investment accounts created by Scammer A. Scammer A created and had access to the new investment accounts and immediately transferred the funds to an overseas account. At this point in 2024, Taxpayer 1 discovered that the accounts were empty, and Scammer A had stolen the funds. Taxpayer 1 contacted their financial institution and law enforcement and was informed that the distribution to an unknown person with an overseas account could not be undone and there was little to no prospect of recovery.

Taxpayer 1 authorized the distributions and transfers with the motive to safeguard and reinvest all of the funds in new accounts in the same manner as before the distributions. Therefore, the losses resulting from the scam were incurred in a transaction entered into for profit under IRC section 165(c)(2). Accordingly, Taxpayer 1 is entitled to deduct the loss in tax year 2024 because it qualifies as a theft loss and there is no reasonable prospect of recovery.

The amount of the loss allowable as a deduction is limited to the taxpayer's basis in the property. In this case, Taxpayer 1 is liable for federal income tax on the IRA account distribution and will recognize gain or loss from the disposition of assets in the non-IRA account, giving Taxpayer 1 basis in all of the stolen funds for purposes of calculating the amount of the deductible theft loss.

Example #2, pig butchering investment scam. Taxpayer 2 is an individual who in 2024 was the victim of a pig butchering investment scam. Taxpayer 2 received an unsolicited email from Scammer A advertising an investment opportunity in cryptocurrency and promising large profits. The email directed Taxpayer 2 to the website of a new platform that would ostensibly invest in cryptocurrencies using proprietary methods to generate large profits.

Taxpayer 2 visited the advertised website, which appeared to be legitimate, and deposited a small amount of cash to invest. Within a few days, the account balance increased in value, and Taxpayer 2 decided to withdraw the money from the website. Taxpayer 2 received the payout, reinforcing the belief that the website was legitimate, and then deposited a larger amount of cash to

invest. The investment increased in size and Taxpayer 2 once again successfully withdrew the funds.

After the success of these investments, Taxpayer 2 invested significantly more money in the scheme with funds taken from IRA and non-IRA accounts that were transferred to the website. After the account balance increased significantly in value, Taxpayer 2 decided to liquidate the investment and withdraw cash from the website. Taxpayer 2 attempted to withdraw the funds but received an error message, and customer support did not respond. Taxpayer 2 began searching online to see whether other investors had similar problems and discovered claims from several people saying they had been defrauded by the website and Scammer A.

At this point in 2024, Taxpayer 2 contacted law enforcement and the financial institution from which the original funds were withdrawn and was informed that the transfer to the website's overseas account could not be undone and there was little to no prospect of recovery. Scammer A was never identified or charged with any state or federal crime.

Taxpayer 2 transferred the funds from the IRA and non-IRA accounts to the website for investment purposes. Therefore, the losses from the scam were incurred in a transaction entered into for profit under IRC section 165(c)(2). Accordingly, Taxpayer 2 is entitled to deduct the loss in tax year 2024 because it qualifies as a theft loss and there is no reasonable prospect of recovery.

As was the case with Taxpayer 1, Taxpayer 2 will be liable for federal income tax on the IRA account distribution and will recognize gain or loss from the disposition of assets in the non-IRA account, giving Taxpayer 2 basis in all of the stolen funds for purposes of calculating the amount of the deductible theft loss.

Example #3, phishing scam. Taxpayer 3 is an individual who in 2024 was the victim of a phishing scam involving an impersonator. Taxpayer 3 received an unsolicited email from Scammer A claiming that Taxpayer 3's accounts had been compromised. The email contained official looking letterhead and was digitally signed by a "fraud protection analyst." The email contained a link, phone number, and directions to call the analyst to ensure Taxpayer 3's funds would be protected.

Taxpayer 3 immediately called the number in the email and communicated with Scammer A, who claimed to be the fraud analyst handling the case. Scammer A directed Taxpayer 3 to click on the link in the email, and then log into Taxpayer 3's tax-deferred retirement account so Scammer A could inspect the account for any issues. By clicking the link in the email, Taxpayer 3 gave Scammer A access to Taxpayer 3's computer. Scammer A was able to identify Taxpayer 3's account username and password

as it was entered into the login screen. Scammer A also convinced Taxpayer 3 to do the same with Taxpayer 3's non-IRA account. The next day, Taxpayer 3 logged into the retirement account and the investment account to find that all funds had been distributed to an overseas account. Taxpayer 3 did not authorize the distributions of the funds from the accounts. Taxpayer 3 contacted law enforcement and the financial institutions and was informed that the distribution to the overseas account could not be undone and there was little to no prospect of recovery.

Unlike Taxpayers 1 and 2, Taxpayer 3 did not authorize the transactions in which funds from the IRA and non-IRA accounts were distributed or transferred to Scammer A. These transactions would generally be looked to for purposes of determining the character of the loss. However, in this case, because the transactions were not authorized by the taxpayer, we look to the stolen property, i.e., securities held in investment accounts, and determine whether they were connected to the taxpayer's trade or business, were invested in for profit, or held as general personal property.

Taxpayer 3 contributed to the IRA and to the non-IRA accounts for the purpose of investing and growing the funds to provide income to Taxpayer 3 in retirement, thereby establishing a profit motive. The theft of property while invested establishes that Taxpayer 3's loss was incurred in a transaction entered into for profit for purposes of IRC section 165(c)(2). Accordingly, Taxpayer 3 is entitled to deduct the loss in tax year 2024 because it qualifies as a theft loss and there is no reasonable prospect of recovery.

The amount of the loss allowable as a deduction is limited to Taxpayer 3's basis in the property. In this case, basis will be established to the extent Taxpayer 3 is liable for federal income tax on the IRA account distribution and recognizes gain or loss from the disposition of assets in the non-IRA account.

Example #4, romance scam. Taxpayer 4 is an individual who in 2024 was the victim of a romance scam involving an impersonator. Taxpayer 4 received an unsolicited text message from Scammer A and proceeded to develop a virtual romantic relationship. Scammer A convinced Taxpayer 4 that a close relative was in dire need of medical assistance, but Scammer A could not afford the expensive medical bills. Taxpayer 4 authorized distributions from an IRA account and a non-IRA account to a personal bank account, and then transferred the money to Scammer A's overseas account to cover the purported medical expenses. After Taxpayer 4 transferred the money, Scammer A stopped responding to messages. At this time, in late 2024, Taxpayer 4 realized

that the romantic relationship with Scammer A was not real, and that Scammer A had stolen Taxpayer 4's funds. Taxpayer 4 contacted their financial institution and law enforcement and was informed that the distribution to the overseas account could not be undone and there was little to no prospect of recovery.

Taxpayer 4's motive was not to invest or reinvest any of the distributed funds from the IRA and non-IRA accounts but, rather, to voluntarily transfer the funds to Scammer A, albeit under false pretenses. Notwithstanding the fraudulent inducement, Taxpayer 4 did not have a profit motive when authorizing the distributions and transfers. Therefore, the losses were not incurred in a transaction entered into for profit and were instead personal casualty losses under IRC section 165(c)(3). Personal casualty losses sustained in 2018 through 2025 are disallowed under IRC section 165(h)(5), except to the extent of personal casualty gains or unless attributable to a federally declared disaster. Because Taxpayer 4 had no personal casualty gains and the loss was not attributable to a federally declared disaster, Taxpayer 4's theft loss is not deductible in 2024. Furthermore, the distribution from the IRA account is subject to federal income tax and Taxpayer 4 is required to recognize gain or loss from the disposition of assets in the non-IRA account.

Example #5, kidnapping scam. Taxpayer 5 is an individual who in 2024 was the victim of a kidnapping scam involving an impersonator. Scammer A contacted Taxpayer 5 by text and phone and claimed to have kidnapped Taxpayer 5's grandson for ransom. Taxpayer 5 demanded to speak to Taxpayer 5's grandson and heard his voice over the phone begging for help. Scammer A directed Taxpayer 5 to transfer money to an overseas account and not to contact law enforcement. Taxpayer 5 did not know that Scammer A had used artificial intelligence to clone the grandson's voice and that no kidnapping had taken place.

Under immense duress, Taxpayer 5 authorized distributions from an IRA account and a non-IRA account, then directed those funds to be deposited in the overseas account Scammer A provided, hoping to ensure the safety of Taxpayer 5's grandson. Later the next day, Taxpayer 5 was able to contact other family members and Taxpayer 5's grandson and learned that no kidnapping had taken place. Taxpayer 5 immediately contacted law enforcement and their financial institution but was informed that the distribution to the overseas account could not be undone and there was little to no prospect of recovery.

Taxpayer 5's motive was not to invest any of the funds distributed from the IRA and non-IRA accounts but, rather, to voluntarily transfer the funds to Scammer A, albeit under false pretenses and duress. Notwithstanding the fraudulent inducement and duress, Taxpayer 5 did not have a profit motive; therefore, the losses were not incurred in a transaction entered into for profit and were instead personal casualty losses under IRC section 165(c)(3). Personal casualty losses sustained in 2018 through 2025 are disallowed under IRC section 165(h)(5), except to the extent of personal casualty gains or unless attributable to a federally declared disaster. Because Taxpayer 5 had no personal casualty gains and the loss was not attributable to a federally declared disaster, Taxpayer 5's theft loss is not deductible in 2024. Furthermore, the distribution from the IRA account is subject to federal income tax and Taxpayer 5 is required to recognize gain or loss from the disposition of assets in the non-IRA account.

Note: AI (artificial intelligence) scams have been making the news and some of the advice to combat these type of scams is to talk with family members and create a secret code word, such as the name of grandpa's boat, the name of a family pet, or some other word that everyone in the family knows to verify whether the person on the phone is real or fake.

The IRS legal memorandum also concluded that none of the taxpayers in the examples above qualify for the Ponzi Safe Harbor in Rev. Proc. 2009-20 for various reasons.

