

# REGULATORY Update



## Proper Use of Forfeitures

Forfeitures are the non-vested portion of an employee's account balance in an employer-sponsored retirement plan. Plans that have a vesting schedule for employer contributions will generate forfeitures as employees terminate employment before fully vesting. If your plan has a vesting schedule for employer contributions, consider taking a fresh look at how those forfeitures are being directed.

Since the Employment Retirement Income Security Act (ERISA) of 1974 was written, plan sponsors have been permitted to use forfeitures to 1) pay reasonable administrative expenses, 2) fund employer contributions, or 3) use as additional allocations to participants. Forfeitures may not be returned to the employer.

It is permissible to use forfeitures in a combination of the stated purposes, though sponsors should verify with their plan document. Unless the plan document restricts the use, for example, a sponsor could use the accumulated forfeitures to pay a plan expense and reduce employer contributions in the same year.

Recently, litigation has sprung up targeting the use of forfeitures to fund employer contributions. Prosecutors charge that to not apply them solely for the benefit of participants is a prohibited transaction. Both the IRS and U.S. Department of Labor (DOL) have reaffirmed their position of the long-standing acceptable uses described above in recent years, but the outcomes of these cases are pending.

Plan sponsors can be diligent to ensure proper handling of these funds. In reviewing the plan document, pay close attention to forfeiture language and ensure that it meets participant needs. The document should:

- Grant the use of forfeitures for these three purposes, allowing for all three at the employer's discretion, or more explicitly state which of the options are allowable.
- State a deadline by which forfeitures must be applied. Plan documents most commonly require using them before end of the following plan year in which the forfeitures occurred, but some may indicate use during the same year.

Plan sponsors should check their plan document for applicable language and ensure that it's intended and being followed, giving the plan the desired flexibility. The DOL has expressed that a violation would occur if the action taken was expressly not allowed by the document, even if it was one of the three broadly available options.

Lastly, not applying all forfeitures by the applicable deadline will result in an operational failure and could lead to costly corrections and tedious census and compensation data verification.



### Charted Wealth

248 Main Street, Suite 101

Reading, MA 01867

888.801.1112 | [www.chartedwealth.com](http://www.chartedwealth.com)

Advisory services offered through Commonwealth Financial Network®, a Registered Investment Adviser.



## Developing a Plan-Specific Cybersecurity Policy

ERISA's prudent person standard of care stipulates fiduciaries must act in the best interests of participants and beneficiaries. Because plan records contain sensitive personally identifiable information (PII), cybersecurity risks are an ongoing part of plan administration. Recent high-profile breaches are a reminder of the high costs associated with cyberattacks as well as the importance of having a cybersecurity policy in place.

Due to the potential for cyberattacks on benefits plans, in April 2021 the DOL's Employee Benefits Security Administration issued "[new cybersecurity guidance for plan sponsors, plan fiduciaries, recordkeepers, \[and\] plan participants](#)" for plans governed by ERISA.\*

The notice provided guidance in three areas: hiring a service provider, protection best practices, and online security tips for participants and beneficiaries.

Please note that this guidance is not required by law; however, it can be a useful tool as a basis from which to build a cybersecurity plan. One thing plan sponsors can feel fairly certain about is that DOL audits will include a review of cyber policies in place and that they are being followed.

### Developing a Plan

Even if the employer already has a general cybersecurity policy in place, one should be created specific to the benefit plan. This is to ensure that the unique needs of the plan are covered, such as the longer record-retention requirements and the variable levels of data each service provider can access. Consider the following components to build a well-developed plan:

1. Develop a system to periodically review the cyber policies of current service providers and to evaluate potential new ones. A consistent process and documentation are critical. Review the [DOL's tips for evaluating a provider](#).
2. Add an IT professional to the plan committee.
3. Maintain cybersecurity insurance specific to the plan because fiduciaries may not be able to rely on an employer's general cyber liability insurance. The policy will require that specified cybersecurity controls are in place in order to maintain effective coverage.
4. Consistently educate participants on measures they can take to protect their accounts.

Plan fiduciaries have a responsibility to take procedural steps to lessen their cybersecurity risk as much as reasonably possible. It's important that they carefully review and incorporate the DOL's updated guidance into their policies.

Aside from passing an audit, keep in mind the damaging and costly reality of the threat. Cyber criminals are creative, persistent, and opportunistic. Having a plan in place can help protect participants and beneficiaries from the harm of a cyberattack and follow a standard of care.

\*In September 2024, the DOL updated its guidance that its original 2021 announcement generally applies to all employee benefit plans, including health and welfare plans, and not just retirement plans.



## Enhanced Catch-Up Contributions for 2025

Individuals ages 50 and older have long been able to contribute more to their retirement accounts than standard limits with an election called catch-up contributions. For employees of a certain age group who want to save more than these limits, regulatory changes are on the way but require close consideration.

SECURE 2.0 increased the catch-up contribution limit for individuals ages 60–63, effective January 1, 2025. The new “super” catch-up provision allows individuals in this age group to contribute \$10,000 or 150 percent of the regular catch-up contribution limit, whichever is greater, to their 401(k), 403(b), governmental 457(b), or SIMPLE plan on top of standard annual limits.

The limit will be adjusted for inflation after 2025 to keep pace with the rising cost of living.

### Notes About the Provision

This is an amendment to code 414(v). Because the current age 50 catch-up election is optional, so, too, is this one. Consistent with the existing rule, sponsors have the flexibility to set limits up to the maximums allowable by the IRS. In other words, sponsors can offer catch-up contributions but are not required to adopt the “super” limits for those in the age bracket.

If adopted, the allowance strictly applies to individuals ages 60–63. In the calendar year in which the individual turns 64, they will be back to the normal limits.

### What About the Pending Mandatory Roth Requirement?

SECURE 2.0 also introduced a mandatory Roth requirement for catch-up contributions when a participant’s FICA wages exceed \$145,000—meaning that individuals above this income threshold who contribute catch-up deferrals must do so in after-tax Roth dollars. The IRS has provided an administrative transition period, however, to implement the requirement. This means individuals can use the increased catch-up and not be subject to the mandatory Roth requirement in the new year.

For sponsors who want to offer the enhanced catch-up provision in their plan, a few steps must be followed:

1. Check with the plan’s recordkeeper and payroll providers to ensure that their systems can comply.
2. Update the plan document and applicable salary reduction agreements.
3. Notify participants.

Although the new election allows people of a certain age to save more for their retirement, we can see the administrative controls required to support these “super” catch-up contributions present new burdens for sponsors, administrators, and recordkeepers.

This material has been provided for general informational purposes only and does not constitute tax, legal, or investment advice. Although we go to great lengths to make sure our information is accurate and useful, we recommend you consult a qualified professional regarding your situation. Commonwealth Financial Network does not provide tax or legal advice.