Fall 2021

Save More for Retirement in 2022

On November 4, 2021, the IRS announced the Cost of Living Adjustments affecting the dollar limitations for retirement plans for 2022. In October, the Social Security Administration announced a benefit increase of 5.9%, the largest increase in nearly 40 years. Following suit, many retirement plan limits have increased as well over the 2021 levels. Contribution and benefit increases are intended to allow participant contributions and benefits to keep up with the "cost of living" from year to year. Here are the highlights from the 2022 limits:

- The calendar year elective deferral limit increased from $19,500 to $20,500.
- The elective deferral catch-up contribution remains unchanged at $6,500. This contribution is available to all participants age 50 or older in 2022.
- The maximum allowable dollar amount that can be contributed to a participant's retirement account in a defined contribution plan increased from $58,000 to $61,000. The limit includes both employee and employer contributions as well as any allocated forfeitures. For those over age 50, the annual addition limit increases by $6,500 to include catch-up contributions.
- The maximum amount of compensation that can be considered in retirement plan compliance has been raised from $290,000 to $305,000.
- Annual income subject to Social Security taxation has increased to $147,000 from $142,800.

If you have any questions on how these increases will affect your plan, please contact your First American Bank representative.

Annual Plan Limits	2022	2021	2020
Contribution and Benefit Limits			
Elective Deferral Limit	$20,500	$19,500	$19,500
Catch-Up Contributions	$6,500	$6,500	$6,500
Annual Contribution Limit	$61,000	$58,000	$57,000
Annual Contribution Limit including Catch-Up Contributions	$67,500	$64,500	$63,500
Annual Defined Benefit Limit	$245,000	$230,000	$230,000
Compensation Limits			
Maximum Plan Compensation	$305,000	$290,000	$285,000
Income Subject to Social Security	$147,000	$142,800	$137,700
Key EE Compensation Threshold	$200,000	$185,000	$185,000
Highly Compensated EE Threshold	$135,000	$130,000	$130,000
IRA Limits			
SIMPLE Plan Elective Deferrals	$14,000	$13,500	$13,500
SIMPLE Catch-Up Contributions	$3,000	$3,000	$3,000
Individual Retirement Account (IRA)	$6,000	$6,000	$6,000
IRA Catch-Up Contribution	$1,000	$1,000	$1,000

Form 5500 Filing Extension for FEMA Designated Disaster Areas

On August 31st, 2021, the IRS issued guidance extending tax filing deadlines for Form 5500 in areas designated by the Federal Emergency Management Agency (FEMA) as qualifying for assistance due to Hurricane Ida and other recent natural disasters. This extension applies not only to Form 5500 filings but also to Form 8955-SSA.

The list of FEMA-designated disaster areas due to Hurricane Ida and other natural disasters continues to grow. Plan Sponsors are eligible for this relief if their principal place of business is located in a covered disaster area. Plan Sponsors can check the updated Disaster Relief page (IRS.gov/newsroom/tax-relief-in-disaster-situations) or check with your service provider to see if your plan qualifies for the extension or for updates to the list of covered areas.

Hurricane Ida

This tax relief postpones filing deadlines for Form 5500s originally due, with valid extensions, starting on or after August 26. For a calendar year plan, subject to extension, with a due date of October 15, 2021, the 5500 is now due on January 3, 2022. Covered disaster areas due to Hurricane Ida include the states of Louisiana and Mississippi and several counties in New Jersey, New York and Pennsylvania.

Tropical Storm Fred

For businesses whose principal place of business is located in certain counties of North Carolina, Form 5500 filings that were originally due, with valid extensions, starting on or after August 16, are now due on December 15, 2021.

California wildfires

For businesses whose principal place of business is located in certain counties of California, Form 5500 filings that were originally due, with valid extensions, starting on or after July 14 and before November 15 are now due on November 15, 2021.

Tennessee severe storms and flooding

For businesses whose principal place of business is located in certain counties of Tennessee, Form 5500 filings that were originally due, with valid extensions, starting on or after August 21 and before January 3, 2022, are now due on January 3, 2022.

These disaster extensions are automatic if the plan qualifies for the extension. Both Form 5500 and Form 8955-SSA have a section to be completed by the Plan Administrator to designate the applicable disaster giving rise to the extension.

Upcoming Compliance Deadlines for Calendar-Year Plans

1st December 2021

Participant Notices – Annual notices due for Safe Harbor elections, Qualified Default Contributions (QDIA), and Automatic Contribution Arrangements (EACA or QACA).

31st

ADP/ACP Corrections - Deadline for a plan to make ADP/ACP corrective distributions and/or to deposit qualified nonelective contributions (QNEC) for the previous plan year.

Discretionary Amendments - Deadline to adopt discretionary amendments to the plan, subject to certain exceptions (e.g., anti-cutbacks).

31st January 2022

IRS Form 945 – Deadline to file IRS Form 945 to report income tax withheld from qualified plan distributions made during the prior plan year. The deadline may be extended to February 10th if taxes were deposited on time during the prior plan year.

IRS Form 1099-R – Deadline to distribute Form 1099-R to participants and beneficiaries who received a distribution or a deemed distribution during prior plan year.

IRS Form W-2 – Deadline to distribute Form W-2, which must reflect aggregate value of employer-provided employee benefits. The CARES Act gives the DOL the authority to delay retirement plan deadlines due to public health emergencies. The dates above are in effect as of the date of this publication.

Participant Distribution Fraud in the "New Normal"

The Coronavirus pandemic, without a doubt, has changed the way we do business. It has also created some unanticipated vulnerabilities. For instance, since the start of the "new normal," there has been an increase of cyberattacks on retirement plans and participant accounts through unauthorized distributions. How did this happen? In March of 2020, Congress passed the CARES Act legislation that increased access to retirement funds for those affected by the COVID-19 pandemic. At the same time, many employees started to work from home, many on personal devices and in unsecure environments. The heightened level of plan distributions together with the security risks associated with electronic communications and working remotely, may have created the perfect storm for exposure of participants' confidential and personal data to cybercriminals. Why would these sophisticated criminals target retirement plans? To quote the famous bank robber, Willie Sutton, when asked why he robbed banks, *"because that's where the money is."* With $6.7 trillion of total assets in 401(k) plans, it seems that Willie would agree that it's where the money is.

Participant distributions have become a particular focus for fraudsters. Retirement accounts typically have higher balances than checking or savings accounts and they also tend to be less monitored by the participant. Participants are typically encouraged NOT to change their investment selections too frequently, so many only view their statements on a quarterly basis. Though cases of distribution fraud were detected by the FBI as early as 2017, the instances of attacks against retirement accounts have skyrocketed during the pandemic. Additionally, retirement plans tend to have many service providers, like TPAs, recordkeepers, and financial advisors. Some even contract with an outside trustee or trust company to facilitate participant distributions. So, in the unfortunate case that a data breach or fraudulent distribution occurs, who is the responsible party? The answer is not as clear as one might think given that ERISA, the main body of law governing retirement plans, was passed into law in 1976, long before the use of the internet or electronic processing. So, with so many parties involved, the courts have many times indicated shared liability between the plan sponsor and other service providers.

How can the chance of cyberattacks be mitigated?

Monitor the Plan's service providers

Some plan sponsors believe that the hiring of external experts like trust companies and other fiduciaries will protect them in the case of fraud. Under ERISA, the employer/plan sponsor has the fiduciary duty to not only protect participant data but to also select and monitor plan service providers. Service providers, like recordkeepers and trust companies, say they are constantly upgrading their cybersecurity systems, but plan sponsors should be asking questions about their cyber policies as well as improvements to their systems. Mid Atlantic Trust Company, which provides trust and custody services to over 125,000 retirement plans, has taken steps to guard against distribution fraud in its paying agent services, a solution that can be used by recordkeepers, TPAs or even directly by the plan sponsor to process participant distributions. Michele Coletti, who serves as Mid Atlantic's Chief Operating Officer, states that when processing distributions, "Mid Atlantic includes several layers of review at pre-set release levels determined by the clients, as well as confirming distributions against an industry-leading fraud prevention service." Additionally, Mid Atlantic looks for distribution red flags in its processes, such as transfers to newly opened bank accounts or funds being transferred to accounts where the registrations don't match.

Transmit all plan data securely

Although it may take a few more clicks and the creation of another password protected account, plan sponsors and participants should always use a secure portal or encrypted email to send personally identifiable information (PII). That means not using company or personal email to send census information, distribution forms or other communications containing PII in an unsecure fashion.

Learn, learn, learn

Like most things involving cybersecurity, education is key. Educating staff members and participants about phishing emails and click bait schemes that are used to trick the recipient into revealing personal information is a highly effective way to stop fraud. Fraudsters use catchy subject lines like "Approve Changes to your 401(k) Account" or "Click here to update your information" to get participants to reveal information to them. This type of education isn't once and done but should be repeated on at least an annual basis and as part of employee orientation.

Establish online access

Though it may sound counter intuitive, encourage all participants to set up their online account access and check them regularly even if they prefer to receive paper statements. Unclaimed online accounts are easier for hackers

to access and take control. Participants should also choose strong passwords and set up multifactor authentication (MFA) which sends codes to multiple devices to verify the account holder's identity. Avoiding the use of public Wi-Fi to access retirement accounts greatly decreases the potential of being hacked.

Good policies and procedures go a long way

It's important to note that not all fraud will be electronic. There are reported cases where fraudsters have used fax, phone and even paper documents by mail to perpetrate distribution fraud. Plan sponsors should follow strict procedures, and ensure that their service providers do as well, to reduce the chance of a fraudulent withdrawal from a participant's account.

Will retirement accounts ever be 100% secure? Though we may wish so, account theft will continue to evolve as fraudsters find ways of mining personal information whether it be from social media sites, like LinkedIn and Facebook, or by hacking email accounts or passwords. Maintaining good administrative practices as a participant or plan sponsor and selecting service providers who remain vigilant in upgrading their cyber security systems will be key to protecting plan data and assets from cyberattacks.