

Content developed by LPL Financial. ♦ A MESSAGE FROM: **Sharonview Financial Services**

FINANCIAL VIEWPOINT



SHARONVIEW®

FINANCIAL SERVICES

Investing ♦ Retirement ♦ Insurance

How to Manage Your 401(k) When You Switch Jobs



In the past, boomers and generation Xers often held on to jobs for 10 or more years. Some professionals stayed with the same company for most of their working lives. The Great Recession changed this for many. Now, people have become more comfortable moving from job to job. Millennials are especially adept at this. They change jobs three times more often than other generations.

Changing jobs introduces a new dilemma for people, regardless of why or how often they do so: what to do with the 401(k) account they had with their former employer. Should they consider taking the cash distribution, or could there be a better choice?

Consider All Options

Here are some reasonable options to consider whether it's to cash out, or retain the tax-deferred benefits attached to your assets:

- 1. Take the Cash:** When people make financial decisions they may choose to do so based on interest rates and cash in hand. But another important factor to consider is taxes. When you take cash distributions from your 401(k) account, you may pay a lot of money in taxes and fees. This includes a 20% federal withholding tax and then another 10% penalty for people who are under the age of 59 and a half years old.
- 2. Directly Roll the Money Into an IRA:** An individual retirement account is much like a 401(k), but it can remain independent of any employer. You may want to consider this option if you change jobs often or if a new employer does not offer retirement plans.
- 3. Use the New Employer's Plan:** Some professionals prefer to keep rolling their 401(k) savings forward. You may want to consider this option if you mostly work corporate jobs with good 401(k) plans. Rolling the money over directly from one employer to the next may also help to eliminate any fees from the IRS. Note that even if you are not yet eligible to contribute to your new employer's retirement plan, you should be able to roll over your money.
- 4. Keep the Old Plan:** If you have at least \$5,000 in your old retirement account, your employer must allow you to retain your 401(k) account if you want to. You can no longer make contributions to the account, but you can

make decisions regarding the investment of your assets. You may want to consider this option if you leave your job to start a business, or want to add some diversity to your retirement holdings.

The Importance of Research

The right approach depends on a number of factors. Aside from those mentioned above, you should consider the rules at your company as well as longevity. Is the company in financial trouble? What happens to your retirement plan if it goes under? Some employers may also set lower thresholds to allow former employees to leave their retirement accounts behind. Speak directly with the human resources department to get some answers.

Another good source of reputable information is financial professionals. At LPL Financial, our team helps clients to navigate these and other important decisions that impact their economic future. Start working with one of our professionals today.

Disclosure: This material has been given an 'Approved As Is' status by Advertising Review. For advisors who want to sue and/or customize preapproved materials, they must first review the Communications with the Public chapter of the Advisor Compliance Manual. Specifically the sections on Commonly Used Disclosures and Pre-Approved Communications. There, they will find instructions on how to use the correct Broker-Dealer disclosure, use preapproved materials, and how to meet their Books and Records Requirements.

Required Attribution: Because of the possibility of human or mechanical error by DST Systems, Inc. or its sources, neither DST Systems, Inc. nor its sources guarantees the accuracy, adequacy, completeness or availability of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information. In no event shall DST Systems, Inc. be liable for any indirect, special or consequential damages in connection with subscriber's or others' use of the content.

© 2021 DST Systems, Inc. Reproduction in whole or in part prohibited, except by permission. All rights reserved. Not responsible for any errors or omissions.

LPL Tracking #1-972679 Exp. 08/22

Checkups are good for your financial health.

Call to schedule a free, no-obligation
consultation to discuss your options!



Dwayne Clendaniel, AWMA, CRPC®†

Senior Vice President, Sharonview Financial Services, LPL Financial Advisor

7422 Carmel Executive Park Drive, Suite 218 ♦ Charlotte, NC 28226

704.973.2625 or 800.462.4421 x2625

Serving Sharonview members in Charlotte, Salisbury, and surrounding areas. Visit sharonview.org/SFS for more information.



Chuck Coveney, AAMS, CRPC®†

Vice President, Sharonview Financial Services, LPL Financial Advisor

1855 E. Main Street, Suite 7 ♦ Spartanburg, SC 29307

864.967.8509 or 800.462.4421 x2006

Serving Sharonview members in the upstate of South Carolina and Shelby areas. Visit sharonview.org/SFS for more information.



Michael Ray Skibbe

LPL Financial Advisor

3212 Oleander Drive ♦ Wilmington, NC 28403

704.973.2629 or 800.462.4421 x2629

Serving Sharonview members in the Wilmington, NC area.
Visit sharonview.org/SFS for more information.

Securities and advisory services are offered through LPL Financial (LPL), a registered investment advisor and broker-dealer (member FINRA/SIPC). Insurance products are offered through LPL or its licensed affiliates. Sharonview Federal Credit Union and Sharonview Financial Services **are not** registered as a broker-dealer or investment advisor. Registered representatives of LPL offer products and services using Sharonview Financial Services, and may also be employees of Sharonview Federal Credit Union. These products and services are being offered through LPL or its affiliates, which are separate entities from, and not affiliates of, Sharonview Federal Credit Union or Sharonview Financial Services. Securities and insurance offered through LPL or its affiliates are:

Not Insured by NCUA or Any Other
Government Agency

Not Credit Union
Guaranteed

Not Credit Union Deposits or
Obligations

May Lose
Value

†CRPC is a registered service mark of the College for Financial Planning®

Recognizing & Avoiding Online Scams

According to the Identity Theft Resource Center, the annual number of records exposed rose 126% in 2018, even while the annual number of data breaches fell by 23%. The business sector experienced 46% of the data breaches in 2018, followed by the medical and health care sector at 29%.¹ This crime occurs when a thief obtains confidential information – including passwords, personal ID numbers, Social Security numbers, or an account number used with a financial institution – and uses it to commit fraud. Identity thieves use a victim's stolen information to open bank and brokerage accounts, run up bills for credit card purchases, obtain loans, and commit other forms of financial fraud. Criminals obtain a victim's personal information in a number of ways – both online and off. But as incidents of identity theft grows, so too does the arsenal of tools and sophistication level of techniques used to perpetrate the crimes.

Cybercrime: A Rapidly Shifting Model

Although online crime is a fast-moving target, currently, the primary methods in use by identity thieves are social engineering and phishing – or typically a combination of both. As the term implies, social engineering relies heavily on human interaction and often involves tricking unsuspecting victims into breaking normal security procedures. In short, it is a way for criminals to gain access to your computer or mobile device and the sensitive personal data it stores. For instance, a social engineer may use text messaging to contact a mobile device inviting the user to click on a link to a bogus website where the thieves collect user credentials and other personal information.

Similar results can be achieved through a phishing attack, in which the criminal uses email to lure victims to fake websites and then gain access to their passwords and usernames, credit card numbers, and other key data. Phishing emails often appear to be from a legitimate company that the victim recognizes. In yet another instance, attackers may inject infected “malicious” code onto your computer via email attachments, links contained in emails, infected search engine results, or through videos and documents on legitimate websites, particularly social networking sites. In the mobile device world, criminals can corrupt a legitimate smartphone app and upload it to a third-party site. If users innocently install the app, they expose their devices to assaults by hackers who collect personal user data, change device settings, and sometimes even control the device remotely.

Don't Be a Victim

In today's 24/7/365 world, it is nearly impossible to secure all sources of personal information that may be “out there” waiting to be intercepted by eager thieves. But you can help minimize your risk of loss by following a few simple hints offered by the Federal Bureau of Investigation (FBI):

- ◆ Never divulge your credit card number or other personally identifying information over the Internet or telephone unless you initiate the communication.
- ◆ Reconcile your bank account monthly, and notify your bank of discrepancies immediately.
- ◆ Actively monitor your online accounts to detect suspicious activity. Report unauthorized financial transactions to your bank, credit card company, and the police as soon as you detect them.
- ◆ Review a copy of your credit report at least once each year. Notify the credit bureau in writing of any questionable entries and follow through until they are explained or removed.
- ◆ If your identity has been assumed, ask the credit bureau to add a statement to that effect to your credit report.
- ◆ If you know of anyone who receives mail from credit card companies or banks in the names of others, report it to local or federal law enforcement authorities.

Finally, be very wary of any email or text message expressing an urgent need for you to update your personal information, activate an account, or verify your identity. Practice similar caution with email attachments and downloadable files and keep your computers protected with the latest security updates and virus protection software.

Disclosure: The attached has been given an ‘Approved As Is’ status by the Advertising Review Team. Advisors who are interested in using and/or customizing pre-approved materials should ensure an understanding of the Pre-Approved Communications section of the Advisor Compliance Manual posted on ClientWorks. This section of the compliance manual includes instructions on how to use pre-approved materials and meet the necessary Books and Records requirements.

Source/Disclaimer:

¹Identity Theft Resource Center, 2018 End-of-Year Data Breach Report, 2019.

Required Attribution:

Because of the possibility of human or mechanical error by DST Systems, Inc. or its sources, neither DST Systems, Inc. nor its sources guarantees the accuracy, adequacy, completeness or availability of any information and is not responsible for any errors or omissions or for the results obtained from the use of such information. In no event shall DST Systems, Inc. be liable for any indirect, special or consequential damages in connection with subscriber's or others' use of the content.

© 2020 DST Systems, Inc. Reproduction in whole or in part prohibited, except by permission. All rights reserved. Not responsible for any errors or omissions.

LPL Tracking # 1-983954