Employee Benefits Report

HEALEY & ASSOCIATES
progressive ingenuity. financial security.

10 Free Street, PO Box 599
Portland, Maine, 04112-0599
T: 207.775.6177 | F: 207.775.5688

232 Center St. Suite D, PO Box 3160
Auburn, Maine, 04212-3160
T: 207.784.1535 | F: 207.777.5208

www.healeyassociates.com

Benefits | August 2021 | Volume 19 • Number 8

How to Help Employees Set Up an Emergency Cash Reserve

The pandemic made it clear that many employees need a way to access funds in an emergency. Here's how to make it easier for them in the future.

Since the 1980s, employees have become accustomed to getting help from employers to save for retirement with 401(k) plans. But what about saving for more immediate needs? Now many employers are stepping up to help employees save for unexpected expenses.

Emergency Savings Accounts (ESAs) allow employees to make automatic deposits through payroll deductions — similar to how their 401(k) accounts are funded.

continued on next page

Cryptocurrency: A New 401(k) Option

Should Ethereum, Bitcoin, Dogecoin and other cryptocurrencies be a part of a sound retirement plan?

It's not as farfetched as you might think. This summer, one company started to allow some employers to offer cryptocurrency as a 401k investment option.

Investors exchange money for cryptocurrency, which can be used like a token to purchase goods or services. Cryptocurrencies generate no cash flow, so the value of cryptocurrency only increases if someone pays more than the investor before them. There currently are more than 10,000 different cryptocurrencies traded publicly.

ForUsAll, a retirement invest-

continued on next page

The need for emergency savings became apparent during the COVID-19 pandemic. As businesses were forced to reduce hours or shut down to encourage social distancing, many employees were confronted with the reality of reduced or no income for months on end.

Even before the pandemic, the Federal Reserve's Report on Economic Well-Being of U.S. Households in 2019 showed that 37 percent of U.S. households could not come up with $400 for an emergency expense if needed.

Experts believe that encouraging employees to contribute a portion of their pay to an emergency savings account can alleviate financial concerns and help employees focus better at work.

Perhaps even more importantly, an ESA can keep employees from seeking loans or early distributions from their existing retirement savings. This is particularly important now since the Coronavirus Aid, Relief, and Economic Security (CARES) Act has made retirement plan withdrawals possible for people who haven't yet reached retirement age.

The downside of an ESA is that it might cause an employee to put less money into their retirement account.

Employees already have the option to divert a portion of their paycheck into savings. But this is the first time the door is open for employers to auto-enroll employees into savings plans, in a way that's similar to how they set up a 401(k), with the employee having to opt out instead of opt in.

How to Set Up a Savings Account

There are two ways to set up an emergency savings account for employees:

- With an existing 401(k) plan used as a "sidecar account," where the ESA shares the same platform as a 401(k) plan. Once the after-tax cash builds up to a certain point, the employee can request further payroll deductions to be directed into their retirement savings using pretax dollars. One drawback is that it could take a few days for employees to withdraw money from their ESAs.
- With an account at an outside bank or financial institution

Regardless of the kind of account chosen, the employer must decide whether to manage the account. Many employers hire third-party administrators to handle the details. Employers must also decide whether employees need to sign up to participate or if they will be auto enrolled.

Remember that the difference between ESAs and 401(k)s is that the dollars deducted from employees' paychecks for an ESA are taxed as income and don't have to remain deposited long term. Plus, employers can make matching contributions to employees' accounts.

Federal Guidance

The federal Consumer Financial Protection Bureau (CFPB) addressed uncertainty about whether employers were authorized to set up ESAs. The bureau issued guidance in a Compliance Assistance Statement of Terms (CAST) template.

If you are interested in setting up an ESA that has automatic deposits, you can use the CAST template as the basis for an application to receive the CFPB's approval to create an ESA.

ment platform for small businesses, introduced the Alt 401(k). The 401(k) is offered through Coinbase Institutional, an arm of Coinbase Global Inc., a leading cryptocurrency exchange. Employees can invest up to 5 percent of their 401(k) contributions in bitcoin, Ether, Litecoin and others.

The advantages to having cryptocurrency as part of a 401(k) are:

- **Gains are tax-deferred — or tax free if invested in a Roth IRA**
- **Investments are diversified**
- **Potential for great returns**
- **They could entice employees who were hesitant to save.**

The downside is that it's risky. For instance, the value of all cryptocurrencies in May 2021 was more than $1.7 trillion — down from $2.2 trillion in April.

Best Practices for Administering Intermittent FMLA Leave

Handling FMLA leave can get complicated.

The Family Medical Leave Act (FMLA), enacted by Congress in 1993 to protect jobs, allows employees to take time off work for two reasons:

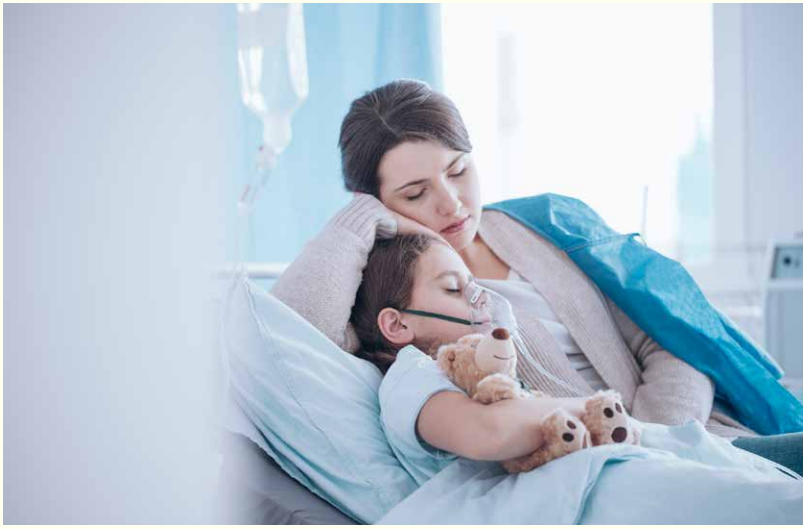
- Injury or illness
- To care for a family member who has been injured or is ill

While this sounds straightforward, administering FMLA leave can get complicated when employees want to take leave on an intermittent basis instead of all at once.

FMLA Basics

Public agencies, schools and private sector employers who employ 50 or more employees for at least 20 workweeks in the current or preceding calendar year must provide eligible employees up to 12 workweeks of unpaid family and medical leave in a 12-month period for:

- The birth of a child or to bond with a newborn child within one year of birth
- The adoption of a child or placement of a foster child and to bond with the newly placed child within one year of placement
- A serious health condition that makes the employee unable to perform his or her job functions
- To care for the employee's spouse, son, daughter or parent who has a serious health condition
- Any qualifying exigencies arising out of the fact that the employee's spouse, son, daughter, or parent is on covered active duty or is called to covered active-duty status as a member of the National Guard, Reserves or Regular Armed Forces.



To be eligible for FMLA, employees must have worked 1,250 hours during the 12 months prior to the start of leave. The 12 months of employment do not have to be consecutive.

Employees also must provide 30 days' notice when they know they will need the leave. If possible, employees should try to schedule medical treatments, so they don't disrupt the employer's operations. When the need is not foreseeable, employees should provide as much notice as possible.

FMLA requests may be verbal or written and the employee does not have to say the words "FMLA" or "intermittent leave." They do need to provide enough information for an HR person to ascertain whether the leave should be covered by the FMLA.

continued on next page

Intermittent Leave Best Practices

Employers cannot deny an employee the right to take FMLA leave, nor can they penalize or discourage them from taking leave.

Employees can take the leave all at once or take intermittent leave, which can be taken in separate blocks of time due to a single qualifying reason. Another type of intermittent leave is when an employee requests a "reduced leave schedule." The employee's schedule is either reduced per week or per workday. Examples of intermittent leave include time off for medical appointments, chemotherapy or morning sickness.

Employers must deduct an employee's leave by the actual amount of time they are off work. It's a little more complicated when calculating exempt employees — especially if they work more than 40 hours in a workweek. To make it clear that an employee's regular workweek is 40 hours, employers should include the information in their offer letters or employee policies.

It's important for employers to have clear written policies and practices. The policies should detail the employer's policy, including guidance on how to handle requests and tracking. Once the policies are in place, employees should receive regular communications about how FMLA works.

Managers must be trained to recognize FMLA leave requests and when to forward leave requests to HR.

An employer can fire an employee who is on FMLA leave, if they can prove the discipline or termination was not related to the employee taking leave. Employers also can move an employee from his or her current position, if necessary. The new position must be equivalent in pay and benefits to the old position and something that fits the employee's skills. These transfers should not go beyond the time of the FMLA leave.

Are You Responsible for Employee Identity Theft?

The answer is yes, which is why it's important to practice good cyber risk management.

Cyber thieves love employee personnel records. With the information they steal from Social Security numbers, birth dates, work history, bank account information and health information, they can do a lot of harm and "earn" a lot of money.

As an employer, it's your responsibility to protect this information. In fact, state and federal laws require employers to safeguard this data. If you don't, you could be held liable when the information is stolen.

Employers need this information for background and credit checks. It therefore often falls to human resource (HR) departments to determine risks and figure out the best lines of defense.

What Thieves Target

It's helpful to understand what types of information thieves are looking for. For instance, thieves can use stolen financial information to establish new accounts and use them to steal funds from the victim's existing accounts. Employee information also can be sold to undocumented workers to provide a false work history.

Thieves will sometimes use email to pose as a company executive to request a copy of an employee's W-2 form. If the employee receiving the request fails to verify the legitimacy of the request and forwards the W-2, the thief can use it to create and submit false tax returns or open lines of credit.

Internal Dangers

The Society for Human Resource Management (SHRM), a professional human resources membership association, reports that 30 to 50 percent of identity theft begins in the office. Numerous employees and management have access to HR records, making it more difficult to enforce proper security protocols. In addition, data stored in the cloud can be accessed if an employee uses an unsecure network or falls prey to a phishing scam. There is also the potential that a disgruntled employee might be enticed to sell password data

continued on next page

Federal Laws

The Fair and Accurate Credit Transactions Act and the Fair Credit Reporting Act hold employers liable if their acts or omissions lead to identity theft. In addition, failure to adequately safeguard health-related information or medical records makes employers liable under the Americans with Disabilities Act or the Health Insurance Portability and Accountability Act.

However, there is no one federal law that covers identity theft. The law that applies depends on the type of crime committed.

State Laws

States have taken the lead in establishing employer liability laws, but there is no uniformity or consistency from state to state. Some states have data privacy legislation, while almost all states have data breach notification laws. These laws often impose additional requirements and restrictions on how employers use, store and transmit employee information.

Best Practices

The first step is to develop a comprehensive cybersecurity plan. Working with your IT department and management, craft a document that outlines the best policies for handling, storing and accessing the personal data of employees. You will need to address:

- How the company will encrypt files that contain sensitive data
- Where hard-copies can be stored safely – preferably in a locked location

- How and when you'll conduct internal risk assessments
- What employee information should be stored on the network
- Who will be allowed to view or edit sensitive employee data
- Under what circumstances employee information can be shared
- How this data should be stored and encrypted
- Who will oversee training
- Whether to hire a consultant to assess your network vulnerabilities
- Who will be in charge of overseeing security and serve as the go to person for questions
- How the company will handle a breach if sensitive data is compromised.

Once you have a plan in place, train both your managers and your employees on the new procedures. It's also important for employees to understand the various ways thieves can get their or the company's information. For instance, a cybercriminal who gets control of a victim's social media account can defame and slander an employer and defraud an organization's customers, partners, vendors and clients.

Training should include the importance of:

- Understanding the tactics that cyber thieves use to attack employees and corporations, such as phishing emails
- Using stronger passwords and securing the information
- Alerting a manager, HR and IT immediately about potential data breaches
- Using more secure networks
- Not accessing company information from public Wi-Fi.

Finally, it's an excellent idea for your firm to carry cyber liability insurance. ■

more on next page

Why Do Health Care Premiums Increase?

Is there anything you can do about it?

A good step toward getting your group health care insurance costs under control is to understand why your premiums increase. While inflation plays a big part, there are other important factors:

- New technology and specialized medications save lives, but have a hefty price tag
- People are living longer, which increases the number of illnesses they have to treat
- Common chronic conditions often require long-term medical attention, including office visits, prescriptions, outpatient treatments or emergency care
- The number of covered lives
- The insurer's administrative costs.

How to Reduce Costs

Even before you get to your annual health insurance enrollment, there are things you can do to help lower health care costs:

- The more employees you hire, the lower your health care costs. Insurers are willing to offer lower premiums if there are a lot of employee premiums to cover the risk of a high medical bill.
- If you have fewer than 10 employees, you can increase your buying power by joining a health insurance group with other firms provided they are in the same state.

If the annual renewal period is imminent, consider these actions to lower costs:

- Offer preventative wellness plans. These plans often provide free medical services including low-cost flu shots, cancer screenings, non-smoking seminars, and mental health phone counselors — all can improve employees' health.
- Reduce your coverage costs by not offering dental or vision coverage
- Choose a high-deductible health plan (HDHP). These plans have low premiums, but employees must cover more of the costs. If you supplement it with a health savings account (HSA), employees can save for medical expenses with tax-exempt dollars.
- Choose a plan that has a high maximum out-of-pocket requirement and low premium. The employee will have to cover more of the medical costs.
- Compare insurance providers to find the best costs.

Please call us if you would like to explore some of these options further. ■