

NON-DISPARAGEMENT, CONFIDENTIALITY CLAUSES

NLRB Deals Blow to Severance Agreements

THE NATIONAL Labor Relations Board has issued a decision that non-disparagement and confidentiality clauses in employee severance agreements are illegal.

The board ruled that these provisions stifle employees' and ex-employees' rights under Title 7 of the National Labor Relations Act to discuss work and their employer with one another, among other things.

Since the NLRB's decision applies to both unionized and non-unionized workers, legal experts advise all employers to revisit their severance agreement templates. However, the decision only covers employees – and not severance agreements for supervisors or managers, who are not afforded rights under Title 7.

Decision is far-reaching

In the case before the NLRB, an employer decided to lay off a group of union workers and offered them a severance agreement that included them receiving additional months of pay and benefits depending on their tenure with the company.

It also included a standard confidentiality clause and non-disparagement clause that are found in many severance agreements:

Confidentiality Agreement. *“The Employee acknowledges that the terms of this Agreement are confidential and agrees not to disclose them to any third person, other than spouse, or as necessary to professional advisors for the purposes of obtaining legal counsel or tax advice, or unless legally compelled to do so by a court or administrative agency of competent jurisdiction.”*

Non-Disparagement Agreement. *“At all times hereafter, the Employee agrees not to make statements to Employer’s employees or to the general public which could disparage or harm the image of Employer, its parent and affiliated entities and their officers, directors, employees, agents and representatives.”*

The ruling

The board ruled that merely including non-disparagement and non-disclosure agreements in severance agreements constituted unfair labor practices under Title 7, which guarantees employees (in part):

“The right to self-organization ... and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection.”

Translation: Workers have the right to discuss their jobs and even complain about their employer and management to one another.

The takeaway

The ruling may be appealed, but for now it stands and is not on hold.

The decision will affect employers in virtually every industry and regardless of whether they have union workers or not.

If you plan to continue using severance agreements going forward, you should consult your legal counsel, particularly if your current agreements contain the clauses that offended the NLRB. ❖

CONTACT US

Pleasant Hill Office
363 Civic Drive, 100
Pleasant Hill, CA 94523
Phone: 925-686-2860

Morgan Hill Office
15005 Concord Circle
Morgan Hill CA 95037
Phone: 408-842-2131

Sacramento Office
2775 Cottage Way, Suite 21
Sacramento CA 95825
Phone: 916-970-2745

San Diego Office
5330 Carroll Canyon Rd., Suite 110
San Diego, CA 92121
Phone: 858-345-5787

License No. 0K07568

NEW GUIDANCE

FMLA Leave Can Be Taken in Hourly Increments

THE U.S. Department of Labor recently issued new guidance on the federal Family Medical Leave Act that has upended the notion of what qualifies as leave under the statute.

Its Wage and Hour Division in February issued a guidance letter noting that employees with a serious illness may use intermittent leave under the FMLA to work a reduced schedule for “an indefinite period.” That is a significant departure from the typical FMLA scenario where workers will take days, weeks or months off from work for a qualifying reason under the law.

The ruling paves the way for workers with serious health conditions that may limit how many hours they can work in a day to do reduced hours, which will count towards the law’s leave limit of 12 working weeks per 12-month period.

In other words, if an FMLA-eligible employee reduced their working hours by two every day, they would never exhaust their allowed leave (two hours a day for an entire year).

The FMLA entitles eligible employees to take unpaid job-protected leave for qualifying family and medical reasons with continuation of group health insurance coverage.

The case and opinion

The company that sought the opinion clarifying the law required its employees to regularly work 10-hour shifts to meet its 24-hour operational needs. Several of its workers asked the company under the FMLA to limit their shifts to eight hours.

It asked the Wage and Hour Division to render an opinion if that would be an appropriate use of the law.

Here is the ground-breaking interpretation of the law in the opinion that followed:

“In this case, if an employee would normally be required to work more than eight hours a day but is unable to do so because of an FMLA-qualifying reason, the employee may use FMLA leave for the remainder of each shift, and the hours which the employee would have otherwise been required to work are counted against the employee’s FMLA leave entitlement.”

The Wage and Hour Division added that employees can continue to use FMLA leave until they exhaust their leave, but if an employee only takes a few hours off every day from a workday that’s longer than eight hours, they could theoretically never exhaust their leave and be able to reduce their hours indefinitely.

The takeaway

This guidance changes the dynamic of family medical leave for both employers and employees.

In one sense, if employees are FMLA-eligible but still feel they can work a restricted amount of hours, it could be a benefit for an employer that needs the manpower they may lose with someone who takes weeks off work.

It would also allow the employee to earn a paycheck (albeit reduced by the hours they don’t work).

But for employers that need all hands on deck and working full shifts, this could be a burden.

If you are faced with a situation where an employee requests a restricted work schedule under the auspices of the FMLA, discuss your plans with legal counsel.❖



Smart Ways to Handle a Financial Windfall

A FINANCIAL WINDFALL is something many people dream of, and for quite a few people that dream actually comes true. When people imagine this happening to them, they often think of winning the lottery or sweepstakes and using that money to purchase expensive luxury items.

In fact, financial windfalls generally occur in more traditional ways such as the sale of a family business or a substantial property, an insurance or legal settlement, a large pay increase, or an inheritance.

Making your new wealth last

While a sudden surge in income or wealth can feel like the answer to financial concerns, if not handled properly (like overspending on unnecessary luxuries), it could cause more problems than it solves.

Thankfully, there are smart ways help ensure the benefits and security of a windfall last as long as possible. Start by taking these four steps:

1. Determine if the windfall is taxable or non-taxable. If it is taxable, then you want to address the tax impact first. It can be tempting to pay the tax at a later date but taking care of it right away can save you from owing a large sum during the next tax season.
2. Take a careful look at how much you are netting, not getting. Make sure your financial decisions are based on the actual amount you will receive, not the pre-tax amount listed on the paperwork. Then figure out how the new wealth fits into your current financial situation.
3. When considering your current financial situation, ask yourself “Do I have adequate retirement savings? Three to six months of emergency savings? Outstanding debt?” Your first priority should be to ensure you have enough money now and for the foreseeable future.
4. Finally, once all other financial considerations are taken care of, you may want to use any extra money to realize some dreams, help out family members, pursue an interest, take a nice vacation, or support a favorite charity, for instance.

Work with a professional

Although there are smart ways to handle a windfall on your own, there are times (i.e., if the dollar amount is very large, or the financial or tax implications are highly complex) when the best thing to do is to meet with a financial professional.

A financial advisor can work with you—along with your attorney, accountant, and/or insurance agent—to determine the best approach to take. For example, if you are not currently in debt or you are already up to date on your retirement savings, you may want to consider:

- Investing in stocks, mutual funds, real estate, or business opportunities
- Setting up trusts for your family
- Buying extra life insurance
- Adding more to a college savings fund
- Purchasing other financial products to protect your income and/or assets.

The point is, your windfall does not necessarily have to be earmarked for spending or paying bills. A financial professional can help you grow this money and work toward making your own or your family’s financial future even more secure.



Choose the right path for your unique situation

It may sound like a challenge we would all love to have, but handling a financial windfall intelligently is not as easy as it might seem.

If you experience an infusion of money, start by using the four steps mentioned above, and contact a financial professional to discuss strategies that can help you make the most of your newfound wealth. ❖

Edward C. Rusnak
Joseph Yang

Sagemark Consulting
3000 Executive Parkway, Suite 400
P.O. Box 5154
San Ramon, CA 94583

Phone: (925) 659-0372

Fax: (925) 804-2472

E-mail: Edward.Rusnak@LFG.com

Ed Rusnak and Joseph Yang are registered representatives of Lincoln Financial Advisors.

CA Insurance License # 0E78894 (Edward Rusnak)

CA Insurance License #0H84609 (Joseph Yang)

Securities and investment advisory services offered through Lincoln Financial Advisors Corp., a broker/dealer (member SIPC) and registered investment advisor. Insurance offered through Lincoln Marketing and Insurance Agency, LLC and Lincoln Associates Insurance Agency, Inc. and other fine companies. Lincoln Financial Advisors and its representatives do not offer tax or legal advice. Individuals should consult their tax or legal professionals regarding their specific circumstances. Pacific Diversified Insurance is not affiliated with Lincoln Financial Advisors Corp. CRN-5599092-033023

CYBER RISKS

Phishing Attacks on Business Smartphones Grow

PHISHING ATTACKS on enterprise and employees' smartphones continue plaguing businesses, with attacks increasing 10% in 2022 from 2021, according to a new report.

As more businesses have adopted bring-your-own-device (BYOD) policies, the risks grow for these attacks, which can be costly.

Last year, 11.8% of mobile enterprise users clicked on six or more malicious links, compared with just 1.6% in 2020, which "indicates users are having a tougher time recognizing phishing attempts," according to the report by cyber security firm Lookout Inc.

What is phishing?

Phishing attacks try to coax a target to reveal personal information like passwords or credentials in an e-mail that looks like it's been sent from a reputable source.

Messages are often enticing or convey a sense of urgency.

Typical Phishing Topics

- Prize notifications
- Tech support notifications
- Shipping notifications
- Contact-tracing messages that request personal information.

The dangers

Successful phishing attacks can have costly implications for a business, including:

Rerouting payments – Attackers gain access to your accounts so they can reroute legitimate vendor payments to their own accounts by modifying invoices. They may also gain access to an employee's e-mail and impersonate them, modify content of e-mails and request funds.

System outage – If the phishing attack is a ransomware attack, it can shut down your entire database and website. Depending on how much you rely on your systems, the damage could be a few hundred dollars or tens of thousands in lost revenue.

Data theft – A phishing attack can also result in sensitive company data being compromised or stolen. If personal data is exposed, it could have regulatory consequences, including fines.

What you can do

There are steps you can take to protect your organization, its company-owned and BYOD devices from phishing attacks. Cyber security firm TechTarget recommends:

Using mobile security tools – Security solutions called endpoint management tools may add a layer of protection to mobile devices. These include:

- Symantec Endpoint Protection Mobile
- Trend Micro Mobile Security
- Kaspersky Endpoint Security
- Microsoft Intune
- F-Secure Mobile Security.

Other solutions that can filter out spam text messages and block known sources of phishing attacks include:

- RoboKiller
- Apple iPhone built-in spam filters
- SpamHound SMS Spam Filter.

Creating mobile device policies – Establish smartphone policies for your employees to follow. If you have an IT person, they can set up these policies through mobile device management tools like Microsoft Intune or MobileIron.

These tools can keep employees from responding to messages from unknown sources or clicking on links send via text messages. They can also block messages from unknown sources.

Training your employees – Train your employees to not click on links in messages from unknown sources and to be wary if a co-worker is asking them to click on a link.

Provide examples of how to identify phishing attacks, what actions to take if they receive a request for information, and how to check that the mail is from a trusted source. ❖

