Insurance Buyers' News

Barker Phillips Jackson
Insurance and Other Financial Services

Springfield
PO Box 4207, Springfield, MO 65808
Phone: 800-422-5275
417-887-3550 • Fax: 417-887-3252

Rolla
PO Box 1258, Rolla, MO 65402-1258
Phone: 800-364-2212
573-364-8888 • Fax: 573-341-2257

West Plains
PO Box 964, West Plains, MO 65775
Phone: 800-400-3896
417-256-6162 • Fax: 417-256-6165

River City Insurance
PO Box 127, New Madrid, MO 63869
Phone: 800-899-7392
578-748-5215 • Fax: 573-748-5392

Employment Law July/August Volume 32 • Number 4

EEOC Issues COVID-19 Guidance for Employers

Latest EEOC guidance aims to help employers and employees understand how federal employment discrimination laws apply to mandatory vaccinations … and the rights and responsibilities of employers and employees at work during the pandemic.

The U.S. Equal Employment Opportunity Commission (EEOC) on May 28th posted updated and expanded guidance related to the COVID-19 pandemic. It also provided new information about how the Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA) apply when an employer offers incentives for

continued on next page

This Just In…

According to studies by Swiss Re AG, the effect of hundreds of "zombie companies" failing over the next few years and becoming a drag on the economy is playing a role in decision making by insurers to reduce risk and charge higher premiums — a trend likely to continue as failures increase.

Zombies — which lack the cash flow to cover the cost of their debt — are "a ticking time bomb" whose explosive effects will be felt as governments and central banks withdraw measures that have helped keep these companies alive during the pandemic, Jerome Haegeli, chief economist at the Swiss insurer, told Reuters.

These Zombie companies

continued on next page

employees to provide documentation or other confirmation of vaccination when employees get vaccinated in the community or by the employer or its agent. The EEOC stressed that its responses to COVID-19 questions are addressed only from the perspective of the EEO laws. Other federal, state, and local laws come into play regarding the COVID-19 pandemic for employers and employees.

"The updated technical assistance released today addresses frequently asked questions concerning vaccinations in the employment context," said EEOC Chair Charlotte A. Burrows. "The EEOC will continue to clarify and update our COVID-19 technical assistance to ensure that we are providing the public with clear, easy to understand, and helpful information. We will continue to address the issues that were raised at the Commission's recent hearing on the civil rights impact of COVID-19."

The key updates to the "technical assistance" under the guidance are:

- **Vaccinations may be compulsory.** Federal EEO laws do not prevent an employer from requiring all employees physically entering the workplace to be vaccinated for COVID-19, so long as employers comply with the reasonable accommodation provisions of the ADA and Title VII of the Civil Rights Act of 1964 and other EEO considerations. Other laws, not in EEOC's jurisdiction, may place additional restrictions on employers. From an EEO perspective, employers should keep in mind that because some individuals or demographic groups may face greater barriers to receiving a COVID-19 vaccination than others, some employees may be more likely to be negatively impacted by a vaccination requirement.
- **Incentives are allowed.** Federal EEO laws do not prevent or limit employers from offering incentives to employees to voluntarily provide documentation or other confirmation of vaccination obtained from a third party (not the employer) in the community, such as a pharmacy, personal health care provider, or public clinic. If employers choose to obtain vaccination information from their employees, employers must keep vaccination information confidential pursuant to the ADA.
- **Incentives may not be coercive.** Employers that are administering vaccines to their employees may offer incentives for employees to be vaccinated, provided the incentives are not coercive. Because vaccinations require employees to answer pre-vaccination disability-related screening questions, a very large incentive could make employees feel pressured to disclose protected medical information.
- **Raising awareness of the benefits of vaccinations is permitted.** Employers may provide employees and their family members with information to educate them about COVID-19 vaccines and raise awareness about the benefits of vaccination. The technical assistance highlights federal government resources available to those seeking more information about how to get vaccinated.

This Just In

are a potential burden for the financial sector, especially when it comes to increased credit default rates. Low interest rates incentivize companies to take up bank credit, creating a risk of large-scale defaults on these loans once government support dries up and the zombie companies become insolvent. The Institute of International Finance reported that bank loans to small-and-medium enterprises in the US rose by 6% in 2020.

To avoid a potential surge of defaults and bankruptcies, governments will need to carefully decide how and when to withdraw stimulus packages. According to the Swiss Re study, to assure a sustainable economic recovery, government policy should support businesses that are viable in the long run and facilitate the orderly restructuring of non-viable firms.

The updates are further discussed in two new resources available online:

- **What You Should Know about COVID-19 and the ADA Rehabilitation Act and other EEO Laws** *https://tinyurl.com/4hvn369j*.
- **Federal Laws Protect You Against Employment Discrimination During the COVID-19 Pandemic**, *https://tinyurl.com/2azxf4nx*, which is intended for job applicants and employees, explains how federal employment discrimination laws protect workers during the pandemic.

Surety Bonds: The Other Risk Management Tool

Surety premiums are only a fraction of property/casualty premiums ($8.6 billion versus $633 billion in 2019), but sureties play a critical role in our economy.

According to the Surety & Fidelity Association of America (SFAA), surety contracts protect over $9 trillion in assets.

Surety bonds and insurance policies both provide financial security, but in very different ways. When you buy insurance, the insurer guarantees to reimburse you for a covered loss. When you buy a surety bond, it guarantees that you (the principal) will fulfill the terms of your contract or other obligation with a third party. If you fail to meet these obligations, the surety company will pay the other party (called the "obligee"). When a surety company issues a bond, it's saying that it believes you will make good on your obligations.

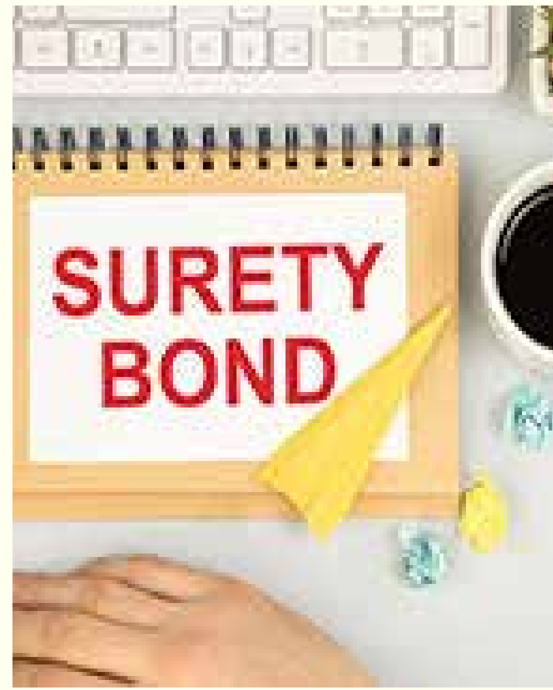
When Do You Need Surety Bonds?

If your profession requires a license, the state will likely require you to have a license bond to protect your clients if you don't uphold the regulations that govern your license. Project owners often use construction or performance bonds to guarantee that a project or job will be completed according to the contract; contractors many also be reiored to buy bonds to guarantee they will pay workers' compensation claims. Crime bonds guarantee that a covered employee won't embezzle your funds.

Insurance vs. Surety Bonds

Although insurance and surety bonds both transfer risk, they have important differences.

- In traditional insurance, the risk is transferred to the insurance company. In suretyship, the risk remains with the principal. The protection of the bond is for the obligee.
- In traditional insurance, the insurance company takes into consideration that a certain amount of the premium for the policy will be paid out in losses.
- In true suretyship, the premiums paid are 'service fees' charged for the use of the surety company's financial backing and guarantee.
- In underwriting traditional insurance products, the goal is "spread of risk." In suretyship, surety professionals view underwriting as a form of credit, so the emphasis is on prequalification and selection.



When you apply for a surety bond, the surety company will make a thorough investigation of your company, including its finances, qualifications and experience. The premium you pay depends on how the surety

continued on next page

underwriter assesses your default risk. The greater your perceived risk of default, the higher your premiums will be.

If a surety company has to make a payment to an obligee on your behalf, you must reimburse the surety. Each bond specifies a maximum amount of money the surety will pay, called the penal sum, in the event of your default.

Guaranteeing a financial obligation such as a loan requires a different set of underwriting tools — and a different type of bond. Financial guarantees require the analysis of complex contractual terms and conditions and an evaluation of how they will affect your ability to pay the loan or financial obligation you want to guarantee.

Because underwriting financial guarantees is so complex, insurance regulations permit only companies licensed expressly for that line of business to write it. Surety bonds can play an important role in your risk management program. For more information, please call us. ■

The Rising Threat of Cyber Risk and How to Control It

When insurance companies started offering cyber insurance a few years ago, it was to take advantage of what seemed like mostly just a marketing opportunity.

In exchange for taking on a minor risk, the principal aim was to capture premium dollars. That was then.

A new report from insurance credit rating agency A.M. Best calls the cyber insurance market "grim," warning insurers they need to urgently "reassess all aspects of their cyber risk, including their appetite, risk controls, modeling, stress testing and pricing, to remain a viable long-term partner dealing with cyber risk."

The report, Best's Market Segment Report, "Ransomware and Aggregation Issues Call for New Approaches to Cyber Risk," names the main challenges facing insurance companies who offer cyber insurance:

- As Exposure to cyber losses rapidly increases insurers are not applying enough underwriting controls.
- Cyber criminals are quickly becoming more sophisticated in their ability to exploit malware and cyber vulnerabilities — much faster than companies have been able to protect themselves.
- Cyber losses are prone to create cascading losses, unlimited by geography or commercial relationships, impacting a wide array of vulnerable targets.

The report notes that although more cyber coverage is now included in package policies, the number of standalone cyber policies has grown 28% in the last year, representing the escalating concerns of companies that want to buy more specialized and comprehensive cyber insurance. These are also the policies that have experienced more frequent and larger losses the past few years.

continued on next page

The kinds of cyber losses have also changed. The report notes that hackers' motives appear to be migrating from stealing identities (third-party claims) to shutting down systems for ransom (first-party claims).

Total claims rose 18% in 2020 owing strictly to first-party ransomware claims, which were up 35% in 2020 and now account for 75% of cyber claims. "The recent Colonial Pipeline hack — for a multi-million-dollar ransom — is an example of first-party claims that have become so prevalent," said Christopher Graham, senior industry analyst, AM Best.

Obviously as a business, your takeaway should be to increase control over your cyber vulnerabilities.

The following cybersecurity best practices from the Small Business Administration offer a good start. But we also highly recommend that you include carrying cyber insurance in your risk management plan. Please call us if you'd like to review your cyber liability preparedness.

Cybersecurity best practices

Train your employees!

Employees and emails are a leading cause of data breaches for small businesses because they are a direct path into your systems. Training employees on basic internet best practices can go a long way in preventing cyber-attacks. The Department of Homeland Security's "Stop.Think.Connect" campaign offers training and other materials.

Training topics to cover include:

- Spotting a phishing email
- Using good browsing practices
- Avoiding suspicious downloads
- Creating strong passwords
- Protecting sensitive customer and vendor information

Maintain good cyber hygiene.

Use antivirus software and keep it updated

Make sure each of your business's computers is equipped with antivirus software and antispyware and updated regularly. Antivirus software vendors regularly provide patches and updates to their products to correct security problems and improve functionality. Configure all software to install updates automatically.

Secure your networks

Safeguard your Internet connection by using a firewall and encrypting information. If you have a Wi-Fi network, make sure it is secure and hidden. To hide your Wi-Fi network, set up your wireless access point or router so it does not broadcast the network name, known as the Service Set Identifier (SSID). Password-protect access to the router.

Use strong passwords

Using strong passwords is an easy way to improve your cybersecurity. Use different passwords for different accounts. A strong password includes:

- 10 characters or more
- At least one uppercase letter
- At least one lowercase letter
- At least one number
- At least one special character

Multifactor authentication

Multifactor authentication requires additional information (e.g., a security code sent to your phone) to log in. Check with your vendors that handle sensitive data, especially financial institutions, to see if they offer multifactor authentication for your account.

Protect sensitive data and back up the rest

Back up your data

Regularly back up the data on all computers. Critical data includes word processing documents, electronic spreadsheets, databases, financial files, human resources files, and accounts receivable/payable files. Back up data automatically if possible, or at least weekly, and store the copies either offsite or in the cloud.

Secure payment processing

Work with your banks or card processors to ensure the most trusted and validated tools and anti-fraud services are being used. You may also have additional security obligations related to agreements with your bank or processor. Isolate payment systems from other, less secure programs and do not use the same computer to process payments and surf the Internet.

Control physical access

Prevent access or use of business computers by unauthorized individuals. Laptops can be particularly easy targets for theft or can be lost, so lock them up when unattended. Make sure a separate user account is created for each employee and require strong passwords. Administrative privileges should only be given to trusted IT staff and key personnel.

5 Types of Surety Bonds You Might Need

Types of Surety Bonds You Might Need

Commercial surety bonds can generally be divided into five types of bonds:

1 License and Permit Bonds: Required by federal, state, or local governments as a condition for obtaining a license or permit for various occupations and professions. License and permit bonds include auto dealer bonds, mortgage broker bonds, contractor license bonds, and surplus lines broker bonds.

2 Court Bonds (also called judicial bonds): Required of a plaintiff or defendant in judicial proceedings to reserve the rights of the opposing litigant or other interested parties. Court bonds include appeal bonds, supersedeas bonds, attachment bonds, and injunction bonds.

3 Fiduciary Bond (also called probate bonds): Required of those who administer a trust under court supervision. Typically such bonds are executor and administrator bonds, trustee bonds, guardian bonds, and conservator bonds.

4 Public Official Bonds: Required by statute for certain holders of public office, to protect the public from malfeasance by an official or from an official's failure to faithfully perform duties. Public official bonds include county clerk bonds, tax collector bonds, notary bonds, and treasurer bonds.

5 Miscellaneous Bonds: These are commercial surety bonds that do not fit into any of the types above. Included are a wide variety of bonds, such as warehouse bonds, title bonds, utility bonds, and fuel tax bonds. ■

The National Association of Surety Bond Producers

Insurance Buyers' News