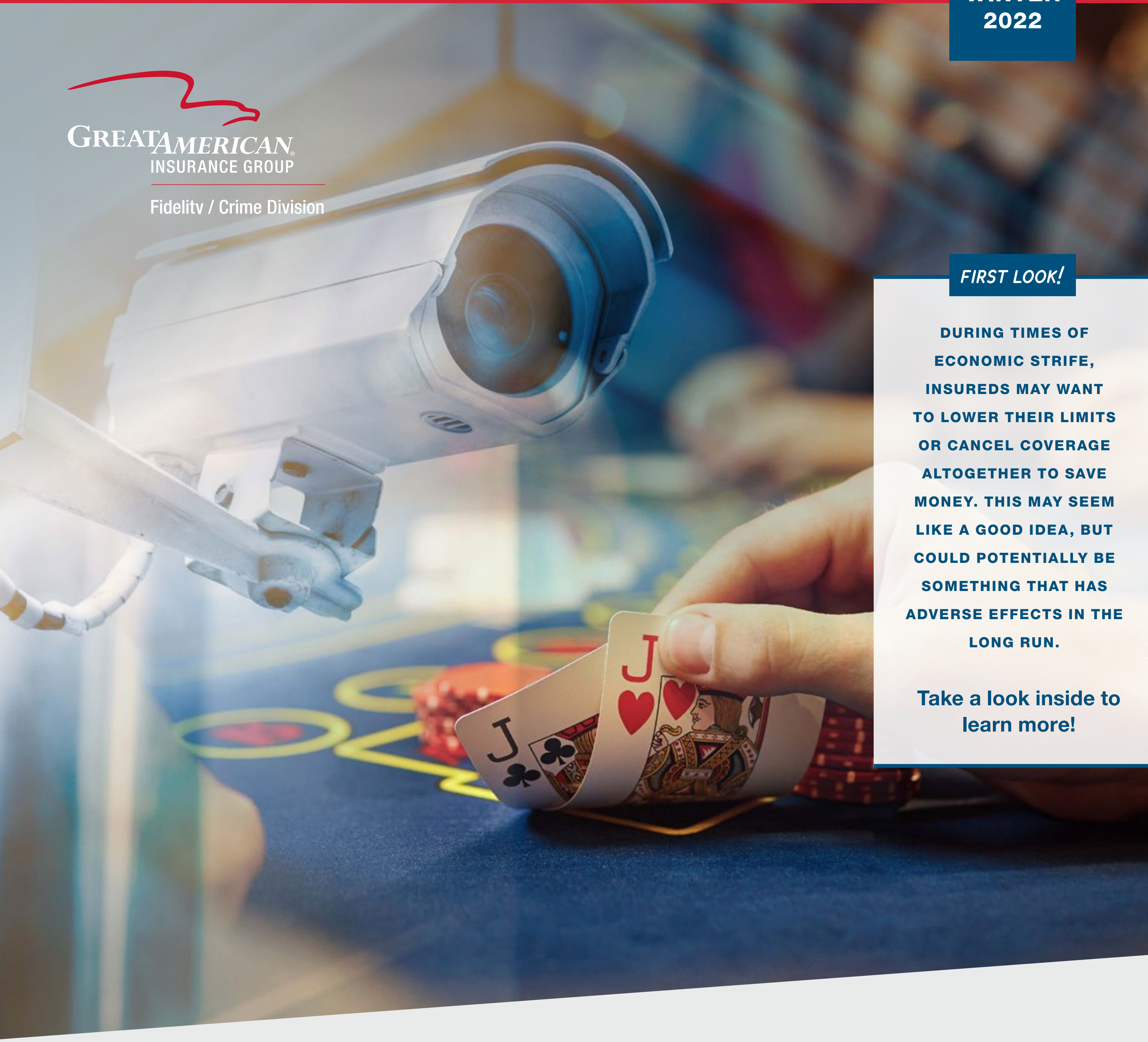
WINTER
2022

GREAT AMERICAN INSURANCE GROUP
Fidelity / Crime Division



FIRST LOOK!

DURING TIMES OF ECONOMIC STRIFE, INSUREDS MAY WANT TO LOWER THEIR LIMITS OR CANCEL COVERAGE ALTOGETHER TO SAVE MONEY. THIS MAY SEEM LIKE A GOOD IDEA, BUT COULD POTENTIALLY BE SOMETHING THAT HAS ADVERSE EFFECTS IN THE LONG RUN.

Take a look inside to learn more!

The Casino Times

INSIDE THE ISSUE

Could Have Known? Should Have Known. The Perils of Negligence in the New Era of Monitoring.

Jon Groussman, J.D., President
Lowers & Associates Consulting

Some of us have been around long enough to remember when pre-employment screening was not a widely-utilized part of the hiring process. Companies trusted their instincts and the positive word of others when making hiring choices. And that seemed to work out fine. Until it didn't.

The crux of negligence is what an employer could have (and therefore, should have) known about an employee.

So today, it is well known that if you're not screening new employees at a level commensurate with the risk of the position they will hold, you're leaving people, brands, and profits at risk. And because employment screening is so widely available and relatively inexpensive to implement, there can be no excuse for failing to catch something in a background check that would deem an employee unsuitable or unsafe for their role.

> *If you could have known, you should have known.*

What about negligent retention? Would the person you hired a year ago have the same results on their background check today?

Many of us have learned this lesson the hard way. Either through a negligent retention case or having experienced a loss caused by an employee whose background had changed in ways that (had you known) might have changed the nature of their employment.

While negligent retention cases have been around as long as negligent hiring cases, what has changed today is what an employer "could" know. Recent advances in monitoring technology can offer employers easy and cost-effective ways to essentially look at the same types of court records they would investigate in a pre-employment background check, except instead of looking at past activity, they can look at near real-time activity. What this means is that, for many employers, there's no longer a reason not to know.

In the casino industry, we encourage employers to look at the riskiest positions – people who have unsupervised access to guest rooms, those who handle cash and other finances… a casino is full of vulnerabilities with many assets to protect. Having an objective way to monitor those you deem necessary to monitor could be of great benefit.

We advise employers to select the types of crimes that are relevant to the safety of a given role and monitor the individuals in those roles accordingly. Monitoring can and should become part of the safety culture, similar to drug screening. Because it's not about spying on employees, it's a mutual understanding between employer and employee that there are simply certain types of crimes, based on an individual's position, that the employer could and should know about.

Casino Riskopolis - See below for lurking crime exposures.

1. **Cashier Stations -** A patron jumped over the cashier counter with a gun and demanded all of the cash and chips be put into a duffel bag. Proper physical controls would have prevented the patron from ever being able to jump over the counter or pose a physical threat to the cashier.

2. **Counting Room / Vault -** An annual audit discovered $400,000 was stolen from the vault and counting room by an employee over the course of the previous year. The casino didn't require employees to wear special clothing when inside, allowing the employee to easily stash up to $10,000 per shift into their pocket, positioning themselves where they knew there was a camera blind spot.

3. **Fine Art -** A janitor knocked over an $800,000 piece of art on display while vacuuming, causing $70,000 in restoration expenses. The artwork was not hung by a trained art handler and the cleaning staff was not trained on special care of fine art.

4. **HR Office -** An employee misused the company credit card to fund personal vacation stays, designer clothing, car payments and more. This was not the first time the employee had stolen from an employer; a previous background check would have shown dishonest acts committed in the past.

5. **HR Office -** An HR manager creates a phony employee in the payroll system and has checks directly deposited into a personal account for 2 years.

6. **Restaurant -** A bartender frequently sold drinks to patrons and voided the point-of-sale transactions, pocketing the cash.

7. **Slot Machines -** A patron tipped off a dealer that a slot machine was functioning improperly. The dealer colluded with the patron to continuously play this faulty machine, causing the casino to pay out "winnings" that were not legitimate.

8. **Accounting Office -** An executive creates a fictitious vendor in the Accounts Payable system and creates phony invoices to be paid to a personal bank account. Invoices are paid to this fictitious vendor for 3 years for a total of $1,300,000.

9. **Shipping / Loading Dock -** A maintenance manager is able to authorize purchases and receive items with no oversight. The manager purchases additional maintenance supplies to be shipped to the loading dock and sells them online for a personal profit. The scheme goes on for 8 months for a $250,000 loss.

The Importance of Crime Coverage and Adequate Limits During Tough Economic Times

Steve Arduini
Senior Account Executive
Great American Insurance Group

During times of economic strife, Insureds may want to lower their Crime limits or cancel coverage altogether to save some money. Although this may seem like a good idea short-term for cost savings, it is something that can have adverse effects in the long run:

- If a loss is discovered, the Insured could be subject to the new lower limit even though they have been paying for the higher limit for many years - even if the actual loss happened when their limits were higher.
- During economic hardship, employee theft tends to be higher. Fired & laid off employees are more likely to steal because they are angry, believe they are owed or become desperate for money to feed their families.
- There is higher likelihood of burglary and robbery and increased hazard of a computer/email related loss with all the people working from home.
- When companies operate with a reduced staff there tends to be fewer people in oversight roles, a lack of checks and balances, and a lessening of internal controls. With fewer employees, existing internal controls can get overridden. Employees take on additional duties. It's not just the employees who will take advantage of this unprecedented time, so will the cyber criminals. According to the FBI, in 2020 their Internet Crime Complaint Center (IC3) received 791,790 complaints with losses of $4.2 billion. It is expected cyber-criminals are ramping up their activity to take advantage of these chaotic times. The losses in 2021 and beyond can easily surpass $4.2 billion annually.[1]
- Companies are more susceptible to cybercrimes with employees working from home using the household Wi-Fi. System log in credentials and passwords to bank accounts are exposed. There are fewer employees to verify requests for wire transfers or changes in bank information.
- Other risks increase as well. Cutbacks in security exposes a business to burglary, and robberies increase during hard economic times. Bank and armored car attacks also increase in frequency.

CrimeInsurance.com

1 "IC3 Releases 2020 Internet Crime Report." FBI, FBI, 17 Mar. 2021, https://www.fbi.gov/news/pressrel/press-releases/fbi-releases-the-internet-crime-complaint-center-2020-internet-crime-report-including-covid-19-scam-statistics.