

Insurance Buyers' News



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



Crime

September / October 2023

Volume 34 • Number 5

Car Thefts Rise by 33.5 Percent in First Half of 2023

Homicide and most other violent crimes declined in American cities in the first half of 2023, but they remain above levels seen before the onset of the coronavirus pandemic and nationwide protests that followed the killing of George Floyd, according to a new study of crime trends in 37 cities released last month by the Council on Criminal Justice.

Examining homicides in 30 cities that make homicide data readily available, the analysis found that the number of murders in the first half of 2023 fell by 9.4% compared to the first half of 2022 (a decrease of 202 homicides in those cities). Twenty of the study cities recorded a decrease in homicides during the first six months of the year, ranging from a 59% drop in Raleigh, NC, to a 2% drop in Nashville, TN. Ten cities experienced an increase in homicide, ranging

from about 5% in Seattle to 133% in Lincoln, NE.

Motor vehicle thefts, which began to rise at the onset of the pandemic, continued an upward trend. Considered a “keystone crime” that facilitates the commission of homicide and other offenses, motor vehicle theft rose by 33.5% in the first half of the year, representing 23,974 more stolen vehicles in the 32 cities that reported data. Seven of those cities experienced an increase of 100% or more, led by Rochester, NY, (+355%) and Cincinnati (+162%). Over-

EEOC Defines ADA for Visually Impaired Employees

WASHINGTON – In July, the U.S. Equal Employment Opportunity Commission (EEOC) released an updated technical assistance document, “Visual Disabilities in the Workplace and the Americans with Disabilities Act,” explaining how the Americans with Disabilities Act (ADA) applies to job applicants and employees with visual disabilities.

The document outlines when an employer may ask an applicant or employee questions about their vision, how an employer should treat voluntary disclosures about visual disabilities, and what types of reasonable accommodations those with visual disabilities may need in the workplace. The updated document highlights new technologies for reasonable accommodation, many of which are free or low-cost, and describes how using artificial intelligence (AI) and algorithms to make employment decisions can impact individuals with visual disabilities.

The document addresses how an employer should manage safety concerns about applicants and employees with vi-

continued on next page

continued on next page



all, the number of vehicle thefts from January to June 2023 was 104.3% higher than during the same period in 2019. While it's likely that much of the increase is the result of thefts of Kia and Hyundai models, the authors said, rates were rising before the cars became popular targets.

In other findings, gun assaults (-5.6%), robberies (-3.6%), nonresidential burglaries (-5%), larcenies (-4.1%), residential burglaries (-3.8%), and aggravated assaults (-2.5%) all fell in the first six months of this year compared to the same timeframe last year. Drug offenses rose by 1% and domestic violence by 0.3%.

"The decline we see across the major crime categories is encouraging, but our country should not be comfortable with rates of violence that continue to claim thousands of lives each year," said University of Missouri – St. Louis Professor Emeritus Richard Rosenfeld, co-author of the study and chair of CCJ's recently formed Crime Trends Working Group. "We now have a solid array of research-backed crime prevention tools at our disposal. Law enforcement, policymakers, and communities should

redouble efforts to deploy them."

Expanding on the analysis of mid-year 2023 trends, the study provides comparisons with offense levels recorded in 2019, before the coronavirus, the killing of Floyd, and the ensuing mass protests over police violence. Violent crimes remained higher during the first half of 2023 compared to the first half of 2019. While homicide has receded from its peak in 2021, levels remained 24% higher than in the first half of 2019. Even if homicide rates were to fall back to pre-pandemic levels, the 2019 homicide rate was still 15% higher than in 2014, the lowest level recorded since World War II. Gun assaults (+39%), aggravated assaults (+8%), and robberies (+2%) also remained higher in the first half of 2023 compared to the first half of 2019.

Property crime trends were more mixed as motor vehicle thefts (+104.3%) and nonresidential burglaries (+5.1%) were higher in the first half of 2023 compared to the same period in 2019, while drug offenses (-38.7%), residential burglaries (-26%), and larcenies (-7%) were lower.

This Just In

sual disabilities and how an employer can ensure that no employee is harassed because of a visual disability.

"The ADA became law 33 years ago today and continues to provide vital protections for workers, including those with visual disabilities," said EEOC Chair Charlotte A. Burrows. "Providing reasonable accommodations is an employer's responsibility. Those who have vision impairments, including limited or low vision, should be provided with the resources needed to succeed. This document will be able to provide employers the guidance to do so."

Many individuals who are blind, visually impaired, or have other vision-related conditions can perform successfully on the job and should not be denied opportunities because of stereotypical and generalized negative assumptions. The document also discusses harassment and retaliation.

More information about disability discrimination is available on EEOC's disability discrimination landing page: <https://www.eeoc.gov/eeoc-disability-related-resources>. For a resource on workplace accommodations, visit <https://askjan.org/>.

"The downward trends in violent crime we're seeing as the pandemic recedes should not dim the intensity of our commitment to reduce violence across the country," said CCJ Research Specialist Ernesto Lopez, the study's co-author. "Although the levels of homicide and other violent crime are well below historical peaks, they remain intolerably high, especially in poorer communities of color."

The authors noted that CCJ's Task Force on Policing and Violent Crime Working Group highlight numerous reforms to improve policing and strengthen the overall effectiveness of violence reduction efforts in the U.S. In addition, the Crime Trends Working Group is currently investigating trends for multiple offenses and exploring ways to improve the nation's crime data infrastructure. ■

How to Read Fine Print

While it's a good idea to read your insurance policy, let's be honest, hardly anybody does. The important thing is to understand what's in it and how it works.

Here are a couple of concepts you want to understand if you have a loss.



What is subrogation and how does it apply to insurance?

Subrogation in the context of insurance is the right of an insurance company to “step into the shoes” of the insured after the company has paid the loss. Subrogation entitles the insurance

company to assert any rights on its own behalf that the insured may have had to recover payment from the parties that caused the loss.

The topic of subrogation is loaded with nuance and there are too many fine points to cover here. But these short explanations of how subro-

gation works in various types of insurance policies should be helpful.

- * In auto insurance, for example, if you have collision coverage, your insurer will pay to repair your car regardless of whether you were at fault. If you were not at fault, though, your insurer would subrogate against the party who hit your car for the damages it paid for.
- * In workers' compensation, if a worker is injured operating a piece of machinery that malfunctions, the worker would be compensated for his injuries according to the workers compensation laws of the state. But the insurance company that paid out the workers compensation would be subrogated to the worker's right to sue the manufacturer of the malfunctioning equipment and recover its payments.
- * One of the most common appearances of subrogation is in property leases, which typically include mutual waivers of subrogation. In these clauses the landlord and tenant each agree to waive any rights of subrogation they may have against each other in the event of a loss. Most insurance policies permit waivers of subrogation if the waiver

has been agreed to before any loss occurs.

Proximate Cause vs. Immediate Cause

Many coverage disputes between insurer and insured arise from different interpretation of the word “cause.” Even when you have an “all-risk” property policy, it is not enough that the cause and its result (the loss) be covered. There must be a sufficiently close connection between the cause and the loss. This is known as the requirement of “proximate cause.”

Black’s Law Dictionary defines proximate cause as “that which, in a natural and continuous sequence, unbroken by any efficient intervening cause, produces the injury, and without which the result would not have occurred.” This is not to be confused with the “immediate cause,” or cause closest to the injury’s occurrence.

How do you distinguish between “proximate” and “immediate” cause?

All basic property insurance policies cover fire damage, but only “special form” policies cover water damage. Nevertheless, if you had a basic policy and your house burned, the policy would cover water damage from fire hoses, because the fire is the “proximate cause” that led to the damage. That is, the water damage would not have occurred without the fire.

Many cases aren’t this clear-cut, however, and disputes often end up in court. Fortunately, whenever a dispute involves ambiguity in a policy’s wording, the court usually rules in favor of the insured. ■

Court Says Employers Responsible for Employee Identity Theft —Regardless of Monetary Damages

Employers go to great lengths to protect their data from breaches from intruders. But what about any employee data that may exist on company servers? Now employers are responsible for the security of that data as well.

In a recent federal case, *Clemens v. ExecuPharm Inc.*, 48 F.4th 146, 157–58 (3d Cir. 2022), the Third Circuit Court of Appeals held that an employee had standing to bring negligence and breach of contract claims against her employer after her personal information was published on the dark web due to a data breach, according to a post by the law firm Porzio, Brombert and Newman.

“The employer, a global pharmaceutical subsidiary known as ExecuPharm, required the plaintiff to provide sensitive personal and financial information, including information regarding her financial accounts and her social security number, and promised to take ‘appropriate measures’ to protect this information after it was stored on its servers.”

After the employee’s job ended, a group of hackers accessed the plaintiff’s personal information and posted it to websites on the dark web. ExecuPharm notified its current and

former employees of the breach and advised them to take action. The plaintiff did so, and her personal information was never used in an unauthorized way. However, despite suffering no monetary damages, the plaintiff sued for negligence and breach of contract. Though the case was dismissed in the Federal District Court, the plaintiff won her case on appeal. The court said that the “disclosure of private information” alone constituted a cognizable harm, along with emotional and other distress:

“In an increasingly digitalized world, an employer’s duty to protect its employees’ sensitive information has significantly broadened. Information security is no longer a matter of keeping a small universe of sensitive, hard-copy paperwork under lock and key. Now, employers maintain massive datasets on digital networks. In order to protect the data, they must implement appropriate security measures and ensure that those mea-



sures continue to comply with ever-changing industry standards.”

According to the law firm’s post, “The Court’s holding presents a clear warning to employers, who may be liable to their employees for security and data breaches even if the employees suffer no actual financial harm. The decision creates a new layer of complexity for employers dealing with cybersecurity threats, who now face potential liability to their current and

former employees in addition to the other numerous negative consequences that may flow from a data breach.

“Going forward, employers must ensure that they maintain appropriate and up-to-date security measures to provide strong and broad protection for the sensitive information stored on their servers and understand that a data breach may expose them to employee lawsuits.” ■

Cybersecurity Basics

To develop a comprehensive cybersecurity plan, work with your IT department and management to craft a document that includes the best practices 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 oversee security and serve as the go to person for questions
- * How the company will manage a breach if sensitive data is compromised.

Once you have a plan in place, train both your managers and your employees in the new procedures. It's also important for employees to understand the many 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. ■

Insurance Buyers' News

