JANUARY 2025

CLEARSTAR®

SCREENING COMPLIANCE UPDATE

CLEARSTAR OFFERS EEOC GUIDELINES COMPLIANCE ON CRIMINAL BACKGROUND CHECKS, GDPR & SOC TYPE 2 SECURITY CONTROL COMPLIANCE AND STAFFING COMPLIANCE.

Compliance is one of the most important parts of background screening, it involves following the rules and regulations set forth by the Fair Credit Reporting Act and local ordinances.

CLICK FOR PAST UPDATES

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | JANUARY 2025

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

This monthly publication is intended to bring to your attention screening industry related articles written by subject matter experts and published online to assist you with establishing and keeping a compliant background screening program.

PLEASE NOTE: Spellings of words in International articles such as those written in the British English format are native to the original author and differ from the spellings of words in the American English format.

EXECUTIVE SUMMARY

January 2025 Screening Compliance Update Executive Summary

The screening compliance landscape witnessed some major changes that have been documented in this month's SCREENING COMPLIANCE UPDATE. Below is an EXECUTIVE SUMMARY of some of the new developments at the FEDERAL, STATE, and INTERNATIONAL levels.

- FEDERAL DEVELOPMENTS: On December 27, 2024, the Department of Justice issued the final rules "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the "Final Rules"), which will be effective three months after issuance.
- STATE DEVELOPMENTS: Five states have joined the growing number of states with pay transparency laws requiring employers to include compensation information in job postings. An Illinois law and a Minnesota law took effect on January 1, 2025, and New Jersey, Vermont, and Massachusetts laws will take effect later this year.
- INTERNATIONAL DEVELOPMENTS: A Federal Court of Appeal in Canada recently issued a decision signaling that employees working in safety-critical roles have a "diminished expectation of privacy" in regard to random alcohol and drug testing.

I hope you find this month's SCREENING COMPLIANCE UPDATE both informative and helpful in keeping up with establishing and maintaining a compliant background screening program.

Nicolas S. Dufour

ClearStar Executive Vice President, General Counsel & Corporate Secretary

Nicolas Dufour serves as EVP, General Counsel, corporate secretary, data privacy officer, and is a member of the executive management team for ClearStar. He is proficient in the FCRA, GLBA, Data Privacy Framework, and GDPR compliance, as well as other data privacy regimes. He is responsible for managing all legal functions to support the evolving needs of a fast-paced and rapidly changing industry. His position includes providing legal guidance and legal management best practices and operating standards related to the background screening industry, federal, state, and local laws and regulations, legal strategic matters, product development, and managing outside counsels. He represents the company in a broad range of corporate and commercial matters, including commercial transactions, M&A, licensing, regulatory compliance, litigation management, and corporate and board governance. He researches and evaluates all aspects of legal risks associated with growth into different markets. He assists the management team in setting goals and objectives in the development, implementation, and marketing of new products and services. He also advises and supports management, Board of Directors, and operating personnel on corporate governance, company policies, and regulatory compliance.

PLEASE NOTE: ClearStar does not provide or offer legal services or legal advice of any kind or nature. Any information contained in this Screening Compliance Update or available on the ClearStar website is for educational purposes only.

FEDERAL DEVELOPMENTS

U.S. Issues Final Rules Regulating the Cross-Border Flow of Data for the First Time

On February 28, 2024, President Biden issued the "Executive Order on Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern". Concurrently, the Department of Justice issued an "Advanced Notice of Proposed Rulemaking, the Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern". On October 21, 2024, it issued a "Notice of Proposed Rulemaking" with proposed rules. On December 27, 2024, it issued the final rules "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" (the "Final Rules"), which will be effective three months after issuance.

The Final Rules create a framework that regulates for the first time the cross-border flow of data from the United States to "countries of concern". The Final Rules largely build on the concepts introduced in the proposed rules and contain more detailed implementation guidelines and helpful working examples. These working examples reveal that in practice, the Final Rules will regulate the cross-border flow of data from U.S. subsidiaries to parent entities headquartered in "countries of concern". Furthermore, the Final Rules create what could be interpreted as a "backdoor CFIUS" mechanism that restricts investment transactions in U.S. businesses by investors in "countries of concern", even if these transactions are cleared by CFIUS.

Jurisdictional Reach - Countries of Concern and Covered Persons Only
Unlike other global cross-border data transfer regulatory regimes such as Europe's GDPR and the PRC's cybersecurity regime, the Final Rules do not regulate the cross-border flow of data from the U.S. to all jurisdictions, only "countries of concern", namely China (including Hong Kong and Macau), Cuba, Iran, North Korea, Russia, and Venezuela.

A "covered person" consists of a government or legal entity in a "country of concern" and includes businesses whose principal place of business is in a "country of concern", 50% or more owned subsidiaries (modelled after the 50 percent rule from the U.S. sanctions regime), and the employees and contractors of each of them. Applied in practice, this means that Chinese companies with offshore Cayman structures would nevertheless be covered as their principal place of business is in China. Furthermore, the reach of the Final Rules extends to their employees and their U.S. subsidiaries to the extent they own 50% or more of them directly or indirectly.

Prohibitions, Restrictions, Exemptions, Licensing, and Penalties
Prohibitions: The Final Rules prohibit "covered data transactions" involving "data brokerage" or human genomic data access with a "country of concern" or a "covered person".

A "covered data transaction" involves government related data or "bulk U.S. sensitive personal data", which meets the following thresholds:

Type of Data	U.S. Person Threshold
Human 'omic data	1,000
Human genomic data	100
Biometric identifiers	1,000
Precise geolocation data	10,000
Personal financial data	10,000
Covered personal identifiers	100,000

A "covered personal identifier" means any identifier in combination with another identifier, but excluding demographic or contact data that is only linked to other demographic or contact data. The contours of these concepts are explained in more detail in working examples. A standalone listed identifier, such as an account username, would not be a covered personal identifier. A demographic or contact data linked to any other demographic or contact data, such as a name linked to a residential address, would not be covered personal identifiers. However, a listed identifier linked with another listed identifier, or a listed identifier linked with demographic or contact data, would be covered personal identifiers. These include a name linked to an e-mail or IP address, and a username linked to a password.

"Data brokerage" means the sale or license of data that is not collected directly by the recipient. The working examples provide clarity on whether inter-company data transfers count as "data brokage". Except in the cases of personal communications subject the Bremer amendment (which would save TikTok from these rules), they are. In one example, a U.S. subsidiary of a parent headquartered in a "country of concern" operates an autonomous driving platform in the U.S. that collects precise geolocation data of its cars. The license of such data from the U.S. subsidiary to the parent is a prohibited transaction. In another example, the U.S. subsidiary of a parent headquartered in a "country of concern" develops an AI chatbot with covered data sourced from the U.S. To the extent its parent can access the raw data underlying the AI chatbot, such access would be considered a prohibited transaction.

Restrictions: Vendor agreements, employment agreements, and non-passive investment agreements are restricted, meaning they require the U.S. business to adhere to a set of security standards that have the effect of data anonymization. The term "vendor agreement" includes the provision of cloud computing services.

With respect to non-passive investments, the Final Rules effectively contain a "backdoor CFIUS" mechanism. Non-passive investments in U.S. companies, defined as 10% or more investments or investments involving operational control including board representation, by investors in "countries of concern", are now restricted and subject to the security standards in the Final Rules. This is true even if the underlying transaction was cleared by CFIUS without conditions.

Exemptions: Exemptions relate to personal communications (e.g. text messaging that does not include anything of value), informational materials, financial transaction such as banking, capital markets, and financial insurance, payments processing, and inter-company sharing of ancillary business data such as human resources and payroll data.

Licensing Regime and Penalties: The Final Rules include a licensing regime for transactions that would otherwise be prohibited or restricted, as well as an advisory opinion regime very similar to the one that already exists for U.S. export controls.

Penalties: Liability is tied to the IEEPA as it is for U.S. export controls and sanctions, meaning violations may result in a fine of not more than US$368,136 (adjusted for inflation) or 2x the amount of the transaction, whichever is higher, or in the case of willful violations, US$1,000,000 and/or imprisonment of not more than 20 years.

Potential Impact

There are two potential overarching themes in the Final Rules, one of which is general and the other of which involves the new compliance burdens of the Final Rules in practice.

The general theme is that the Final Rules represent what is likely to be the opening salvo in the national regulation of the cross-border flow of data from the U.S. to outside of the U.S., making the U.S. as a third rail in data privacy schemes alongside the European Union and China.

The compliance burdens of the Final Rules do not just impact the U.S. businesses of companies headquartered in "countries of concern", but also all multinationals who are involved in the sale or licensing of data they collect in the U.S. The "backdoor CFIUS" mechanism also adds a new layer of complexity that may be expanded to the U.S. businesses of companies that have significant operations in "countries of concern", as evidenced by CFIUS' recent focus on the Chinese operations of Japanese acquirers of U.S. *businesses.*

Source: Lexology - Clyde & Co LLP-Charles Wu

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

New law eliminates redundant background checks for truckers applying for TSA credentials, including TWIC and HME

Lawmakers passed a bill that will cut down on red tape for truckers applying for Transportation Security Administration (TSA) credentials including Transportation Worker Identification Credential (TWIC) and Hazardous Materials Endorsements (HME).

On December 23, 2024, the Transportation Security Screening Modernization Act of 2024 was signed into law by President Biden. It will allow truckers to use existing valid background checks for multiple TSA credentials without paying a duplicative cost.

The new law seeks to modernize current TSA policies which often require essential transportation workers, including truckers, to submit and pay for separate applications for required credentials like the TWIC and HME.

Specifically, the new Transportation Security Screening Modernization Act of 2024 will require the TSA to take the following actions:

- Permit an individual to enroll at a TSA-authorized enrollment center once and use the application, as well as information generated by TSA's vetting, to enroll in any other programs
- Permit an individual to enroll in more than one security threat assessment (STA) program at the same time for a single fee that is less than the combined fee for applying to the same programs separately
- Provide for a streamlined and expeditious renewal process
- Provide states the expiration dates for each individual's STA to ensure commercial driver's licenses include an individual's current HME status
- The new law was endorsed by multiple trade groups including the Owner-Operator Independent Drivers Association, the American Trucking Associations (ATA), National Propane Gas Association, Transportation Trades Department, Border Trade Alliance, National Tank Truck Carriers, Mississippi Trucking Association, Association of the American Railroads, American Short Line and Regional Railroad Association, and National Energy and Fuels Institute.
- "For far too long, the truck drivers who keep our country running have been subjected to an outdated, inefficient credentialing system that does not respect their time and money. That begins to change today. By taking the final step needed to eliminate unnecessary bureaucratic hurdles, Congress will provide essential supply chain workers with overdue relief from redundant background checks and fees," said ATA President & CEO Chris Spear.

Source: Newsbrake - CDLLife

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

City of Madison, Wisconsin Amends its Equal Opportunities Ordinance Regulating Arrest and Conviction Record Discrimination

The Wisconsin Fair Employment Act (WFEA) prohibits employers from discriminating against applicants and employees on the basis of their arrest and conviction records. Generally, an employer cannot make decisions based on an arrest or conviction record unless the crimes "substantially relate" to the circumstances of the job at issue. The City of Madison has its own equal opportunities ordinance that applies to employers within Madison.[1] Included within the Madison ordinance is a similar prohibition on discrimination against applicants and employees based on their arrest and conviction records.[2] Historically, there have been key differences between state law and the Madison ordinance that have created legal potholes for unwitting employers with Madison employees.

One such difference was that under the Madison ordinance, employers arguing for a substantial relationship could only do so when the employee or applicant "has been within the past three (3) years placed on probation, paroled, released from incarceration, or paid a fine, for a felony, misdemeanor, or other offense . . .." Conversely, under state law, there is no such time limitation. Thus, it was a possible that an employment decision could be lawful under state law because an older conviction was substantially related to the job at issue, while at the same time be unlawful under the Madison ordinance because the criminal record is too old.

On December 5, 2024, the Madison Common Council amended the ordinance, removing the three-year lookback provision, effective immediately.[3] Under both state law and the Madison ordinance, however, the age of the conviction is still a relevant factor in the substantial relationship analysis. For example, if there has been a long passage of time between a conviction and the adverse employment action and the individual has no significant history of recidivism, it is more likely that the state agency and the Madison Equal Opportunities Commission (MEOC) will find that there is no substantial relationship.

The harmonization of the Madison ordinance with state law is good news for Wisconsin employers. However, the Madison Common Council may have unintentionally created a new headache for employers. Beyond eliminating the three-year lookback, the amendment provides some guidelines regarding the application of the substantial relationship test, adding the following language to the ordinance:

Whether the circumstances of any such offense substantially relate to the circumstances of the particular job or licensed activity shall be based on the facts of the particular offense, including but not limited to the seriousness of the offense, the passage of time since the employee or applicant was placed on probation, paroled, released from incarceration, or paid a fine, for a felony, misdemeanor, or other offense, the age of the employee or applicant at the time the offense occurred, and the character of the employee or applicant.

This majority of this statement is consistent with how the state agency and the MEOC have applied the substantial relationship test, with the notable exception of the portion declaring that the "character of the employee or applicant" must be considered. How the MEOC will apply this in practice remains to be seen, but in the meantime, employers are left wondering what it will mean to litigate about an employee's or applicant's "character" at an administrative hearing. At the very least, employers should consider mitigating evidence submitted by candidates in response to a pre-adverse action letter, such as letters of reference, documents confirming community service, proof of training (*e.g.*, anger management), etc.

Employers also should be mindful that various jurisdictions continue to prohibit consideration of older criminal records, including California, Hawaii, Massachusetts, and Washington. Before taking adverse action based on criminal records, employers should take steps to become familiar with the laws, if any, in the specific jurisdiction. Employers also should be aware that the EEOC disfavors reliance on older criminal records and remains active in this area of employment law.

Source: Lexology - Littler Mendelson PC - Casey Kaiser

New Pay Transparency Laws Effective in 2025

Five states have joined the growing number of states with pay transparency laws requiring employers to include compensation information in job postings. An Illinois law and a Minnesota law took effect on January 1, 2025, and New

Jersey, Vermont, and Massachusetts laws will take effect later this year. While the new laws differ in their specific requirements, they generally mirror pay transparency statutes passed in recent years in other states, including California, Colorado, and New York, that require employers to disclose pay ranges, and sometimes benefits information and other compensation, in job postings.

The new laws are summarized below:

- The Pay Transparency Amendment to the Illinois Equal Pay Act of 2003 (effective January 1, 2025) requires employers with 15 or more employees to include in job postings a wage or salary range and a general description of the benefits and other compensation (including bonuses, stock options, etc.) for the position. The law applies to positions that will be physically performed, at least in part, in Illinois, or will be performed outside Illinois but the employee reports to a supervisor, office, or other work site in Illinois. Also, when an employer posts a job externally, the employer also must, within 14 days, announce, post, or otherwise make known to all current employees such posting to the extent it would represent an opportunity for promotion for existing employees. Employers must preserve records of job postings for at least five years.
- The Minnesota Omnibus Labor and Industry Policy Bill (effective January 1, 2025) requires employers with 30 or more employees in Minnesota to disclose in job postings the starting pay range and a general description of all benefits (including health and retirement benefits) and other compensation offered for the position. The law is silent as to whether it applies to jobs performed outside Minnesota.
- New Jersey Senate Bill No. 2310 (effective June 1, 2025) will apply to employers with ten or more employees over 20 calendar weeks in a given year that do business, employ workers, or take applications for employment in New Jersey; the law does not specify whether all ten employees must be located in New Jersey. These employers will be required to include in job postings the hourly wage or salary range and a general description of benefits and other compensation programs for which the employee would be eligible. The law also will require employers to make "reasonable efforts" to announce, post, or otherwise make known to current employees opportunities for promotion that are advertised internally or externally prior to making a promotion decision. The law is silent on whether it will apply to jobs performed outside New Jersey.
- Vermont H.704 (effective July 2025) will apply to employers with five or more employees but does not specify whether all five employees must be located in Vermont. Covered employers must include in job advertisements the compensation or range of compensation for the job opening. For roles that will be paid on a commission basis, employers must only note in the job advertisement that the role will be paid on commission and need not disclose the compensation or range of compensation. The law will apply to job advertisements for positions that will be physically located in Vermont and to remote positions that will predominantly perform work for an office or work location physically located in Vermont.
- The Massachusetts Frances Perkins Workplace Equity Act (effective October 29, 2025) will require employers with 25 or more employees in Massachusetts to disclose pay ranges in job postings. Employers also must disclose pay ranges to employees offered promotions, transfers, or new positions with different responsibilities. The law is silent as to whether it applies to jobs performed outside Massachusetts. The law separately will require employers that have 100 or more employees and are subject to federal EEO-1 reporting obligations to file the EEO-1 wage data report with the state.

With regard to how pay or compensation range is defined in these new laws, the Illinois, Massachusetts, Minnesota, and Vermont laws generally provide that the pay range means the minimum and maximum compensation the employer reasonably expects to pay for the position, based on the employer's good-faith estimate, and the New Jersey law does not define pay range. The Minnesota law expressly prohibits employers from posting open-ended pay ranges, and guidance from the Illinois Department of Labor states that employers should avoid open-ended phrases like "$40,000 and up" or "up to $60,000." Under each of the new pay transparency laws, employers that fail to comply may be subject to fines or civil penalties.

In light of the growing number of states enacting pay transparency laws, employers should review their job postings and advertisements and revise to include pay ranges and other information as required by applicable laws. Employers should also ensure that all job postings provided to third parties to advertise on the employer's behalf contain the necessary information to comply with applicable pay transparency laws.

Source: Covington & Burling LLP - Lindsay Burke, Evan Parness, Carolyn Rashby and Amanda Michalski

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

New Massachusetts Workforce Data Reporting: Covered MA Employers Must Submit Most Recent EEO Reports by February 3, 2025

Real World Impact: A recently enacted Massachusetts law requires employers with 100 or more employees in the state to submit a copy of their most recently filed EEO reports to the state by February 1 annually (or the next business day following February 1, which is February 3 for 2025).

Introduction: The Massachusetts pay transparency and reporting law entitled *An Act Relative to Salary Range Transparency* was passed in July 2024 as an effort to increase equity and transparency in pay. As part of its workforce data reporting requirement, employers with 100 or more employees in Massachusetts are required to submit a copy of their most recently filed EEO reports to the state by February 1 annually. The law also has a separate pay transparency provision effective October 19, 2025, requiring employers to disclose pay ranges in job postings, which will be covered in a separate legal alert.

Who is Considered a Covered Employer?
Employers with 100 or more employees in the Commonwealth at any time during the prior calendar year are considered covered employers. Importantly, although the Equal Employment Opportunity Commission (EEOC) requires federal contractors with 50 or more employees to file an EEO-1 report, the Massachusetts law only applies to employers with 100 or more employees.

What Do Employers Need to File?
As background, the EEOC requires certain employers to submit annual EEO-1 reports. Other types of employers are required to submit similar reports, such as the Local Union Reports (EEO-3), State and Local Government Reports, (EEO-4); and Elementary-Secondary Staff Information Reports (EEO-5).

Under the new Massachusetts law, covered employers are required to submit "wage data reports," which are defined by statute as the EEO-1, EEO-3, EEO-4, or EEO-5 reports submitted annually to the EEOC. Importantly, although the statute defines "wage data" as the data collected annually by the EEOC, the EEO-1, EEO-3, EEO-4, and EEO-5 reports no longer collect wage data. Indeed, the "Component 2" wage data was only collected by EEOC for the 2017 and 2018 calendar years and has not since been required. Although the annual reports presently do not include pay data, the Executive Office of Labor and Workforce Development has made clear that (a) EEO-1 reports (despite including no wage data) must still be filed to meet the new law's requirements; and (b) if the EEOC re-implements Component 2 in the future, it will also become part of the annual Massachusetts filing requirement.

Thus, covered employers must simply submit a copy of their most recent EEO report – no new or modified report is required.

When is the Filing Deadline?
Employers filing EEO-1 reports must complete their submission by February 1 annually, and if February 1 falls on a weekend or holiday, by the next business day. This year, this means reports will be due by Monday, February 3, 2025. The other EEO reports are due by the same February 1 deadline, but on a biennial basis: EEO-3 and EEO-5 reports are due this year, and EEO-4 reports will be due next year.

How Do Employers Submit a Report?
Covered employers should submit their most recently filed EEO-1, EEO-3, EEO-4, or EEO-5 report to the Secretary of State's web portal.

Will Aggregate Data be Published?
The Executive Office of Labor and Workforce Development will compile the data and publish an aggregated report broken down by industry sector (NAICS code). Individual company data will not be published. The inaugural wage and workforce data report is expected to be published by June 1, 2025.

What Resources Have Been Provided for Employers?
The Secretary of State's website now includes an EEO Wage and Workforce Data Reports page with helpful deadlines and filing procedures, including file name requirements for reports being uploaded. The Executive Office of Labor and

Workforce Development has also prepared Workforce Data Reporting FAQs regarding the Commonwealth's new EEO reporting requirements.

Source: Lexology- FordHarrisson LLP- Nancy Van der Holt and Erica Johnson

New York Enacts Immediate Updates to Breach Notification Law

Governor Kathy Hochul signed several bills last month designed to strengthen protections for the personal data of consumers. One of those bills (S2659B) makes important changes to the notification timing requirements under the Empire State's breach notification law, Section 899-aa of the New York General Business Law. The bill was effective immediately when signed, or December 21, 2024.

All fifty states have enacted at least one data breach notification law. Some states, such as California, have more than one statute – a generally applicable statute and one applying to certain health care entities. Over the years, many of these states have updated their laws in different respects. For example, some have expanded the definition of personal information, resulting in broader categories of personal information triggering a potential notification requirement if breached. Others have added requirements to notify one or more state agency. While some states have modified the specific notification requirements, such as the timing of notification. That is one of the changes New York made to its law.

Prior to the change, a business subject to the New York statute that experienced a covered breach would be required to provide notification to affected individuals: *in the most expedient time possible and without unreasonable delay*.

There was no outside time frame by which the notice must be provided. The bill added a 30-day deadline. So, now, the law requires the breached entity to provide notification *in the most expedient time possible and without unreasonable delay, provided that such notification shall be made within thirty days after the breach has been discovered*

Notably, prior to the change, the law excluded from this timing requirement the legitimate needs of law enforcement and "any measures necessary to determine the scope of the breach and restore the integrity of the systems." The legitimate needs of law enforcement exception remain in the law, determining the scope of the breach and restoring system integrity do not. S2659B also made a change to the state agencies that must be notified in the event of a breach under the statute. Under the prior law, if any New York residents were to be notified under the State's breach notification law, the state attorney general, the department of state and, the division of state police all needed to be notified. The new law adds the Department of Financial Services to the list.

With breach notification requirements under federal law, the laws in all states and several localities, and increasingly embedded in contract obligations, it can be difficult stay up to date, particularly if the company is in the middle of handling the breach. In addition to it being required in some scenarios, this is one more reason why we recommend maintaining an incident response plan. Such a plan is a good place to track these kinds of developments for the company's incident response team.

Source: Lexology - Jackson Lewis PC- Joseph J. Lazzarotti

School volunteer background screenings in FL will intensify

A more intense background screening will go into effect March 1, 2025 in Florida for those who volunteer in public schools increasing the cost of the screening.

School Board of Highlands County Coordinator of Communications John Varady said the School Board has already been following the updated screening requirements for employees and will begin utilizing the new screening procedures for volunteers in 2025, prior to the March 1st date.

"While this may have a potential impact on the cost of volunteer screening, I do not have any concrete numbers at this time," he said.

The Polk County School District will increase the rate it charges potential volunteers from $25 to nearly $100 to cover the

cost of more intensive background screenings, the Lakeland Ledger reports. The district seems to anticipate a decline in volunteers.

The Florida Legislature passed a law in 2023 requiring enhanced screening procedures for volunteers at public schools. The bill passed unanimously in both the House and Senate.

The measure, sponsored by Sen. Erin Grall, R-Vero Beach, elevates the screening from Level 1 to Level 2, which entails fingerprinting for all volunteers.

Also, Senate 676 (2023) amends Florida Statues to revise background screening requirements for athletic coaches to require these individuals, including managers, to increase the level of background screening from a Level 1 to a Level 2 background screening.

The bill also removes the 20-hour minimum work requirement. These changes mean that all youth athletic coaches, assistant coaches, managers, and referees must undergo a Level 2 background screening, regardless of hours worked.

The Pasco County School District decided to get more serious about background checks for its volunteers announcing in June it would require all volunteers to get a Level 2 screening, according to the Tampa Bay Times.

The $41.25 fee has some worried the charge would deter families that can't afford it from volunteering, but officials also have made District funds available to cover the costs for individuals who can't afford the $41.25 fingerprinting, which includes crime database screenings every five years.

Level 2 screening is a comprehensive criminal background check that includes fingerprint-based checks for statewide criminal history records through the Florida Department of Law Enforcement and national criminal history records through the Federal Bureau of Investigation.

This type of check is typically performed on hires in the following cases:

- Positions of trust or responsibility.
- Working in sensitive locations.
- Working in or volunteering with a youth camp or activity outside of the summer period.

Source: Highlands News Sun- Marc Valero

New Jersey Attorney General: NJ's Law Against Discrimination (LAD) Applies to Automated Decision-Making Tools

This month, the New Jersey Attorney General's office (NJAG) added to nationwide efforts to regulate, or at least clarify the application of existing law, in this case the NJ Law Against Discrimination, N.J.S.A. § 10:5-1 et seq. (LAD), to artificial intelligence technologies. In short, the NJAG's guidance states: *the LAD applies to algorithmic discrimination in the same way it has long applied to other discriminatory conduct.*

If you are not familiar with it, the LAD generally applies to employers, housing providers, places of public accommodation, and certain other entities. The law prohibits discrimination on the basis of actual or perceived race, religion, color, national origin, sexual orientation, pregnancy, breastfeeding, sex, gender identity, gender expression, disability, and other protected characteristics. According to the NJAG's guidance, the LAD protections extend to algorithmic discrimination (discrimination that results from the use of automated decision-making tools) in employment, housing, places of public accommodation, credit, and contracting.

Citing a recent Rutgers survey, the NJAG pointed to high levels of adoption of AI tools by NJ employers. According to the survey, 63% of NJ employers use one or more tools to recruit job applicants and/or make hiring decisions. These AI tools are broadly defined in the guidance to include: *any technological tool, including but not limited to, a software tool, system, or process that is used to automate all or part of the human decision-making process…such as generative AI, machine-learning models, traditional statistical tools, and decision trees*.

The NJAG guidance examines some ways that AI tools may contribute to discriminatory outcomes.

- **Design**. Here, the choices a developer makes in designing an AI tool could, purposefully or inadvertently, result in unlawful discrimination. The results can be influenced by the output the tool provides, the model or algorithms the tool uses, and what inputs the tool assesses which can introduce bias into the automated decision-making tool.
- **Training**. As AI tools need to be trained to learn the intended correlations or rules relating to their objectives, the datasets used for such training may contain biases or institutional and systemic inequities that can affect the outcome. Thus, the datasets used in training can drive unlawful discrimination.
- **Deployment**. The NJAG also observed that AI tools could be used to purposely discriminate, or to make decisions for which the tool was not designed. These and other deployment issues could lead to bias and unlawful discrimination.

The NJAG notes that its guidance does not impose any new or additional requirements that are not included in the LAD, nor does it establish any rights or obligations for any person beyond what exists under the LAD. However, the guidance makes clear that covered entities can violate the LAD even if they have no intent to discriminate (or do not understand the inner workings of the tool) and, just as noted by the EEOC in guidance the federal agency issued under Title VII, even if a third-party was responsible for developing the AI tool. Importantly, under NJ law, this includes disparate treatment/impact which may result from the design or usage of AI tools.

As we have noted, it is critical for organizations to assess, test, and regularly evaluate the AI tools they seek to deploy in their organizations for many reasons, including to avoid unlawful discrimination. The measures should include working closely with the developers to vet the design and testing of their automated decision-making tools before they are deployed. In fact, the NJAG specifically noted many of these steps as ways organizations may decrease the risk of liability under the LAD. Maintaining a well thought out governance strategy for managing this technology can go a long way to minimizing legal risk, particularly as the law develops in this area.

Source: Lexology - Jackson Lewis PC - Joseph J. Lazzarotti and Jason C. Gavejian

Illinois Issues New E-Verify Guidance

On August 9, 2024, Illinois Governor JB Pritzker signed Public Act 103-0879 into law, amending the Illinois Right to Privacy in the Workplace Act (RPWA). The amendments, which took effect on January 1, 2025, impose new requirements on employers related to verification of employee work authorization. While the law references E-Verify, many of the provisions apply to all Illinois employers, including those employers who do not use E-Verify or other employment verification systems.

Section 12(a) of the RPWA includes language that one could interpret as barring employers from using E-Verify if they are not required by federal law to use that system to determine work authorization status. The Illinois Department of Labor (IDOL) recently issued Frequently Asked Questions (FAQs) clarifying that "**Illinois Law does not prohibit any employer from using E-Verify.** However, employers who use E-Verify must follow the requirements of the Right to Privacy in the Workplace Act." Illinois employers must ensure that their use of the federal E-Verify system or similar employment eligibility verification tool complies with both federal and state law.

The amendments also include the following:

- A prohibition against employers taking adverse employment actions based solely on the initial results of E-Verify or similar system before receiving final confirmation.
- A new requirement for employers to notify employees of their rights under E-Verify and similar systems. Similar to federal rules for E-Verify users, employers must provide written notice to employees, as well as the employee's authorized representative (if allowed under E-Verify's Memorandum of Understanding), regarding the use of these systems and notice of specific deficiencies in the employee's documentation.
- Additional employee rights and protections when an employer receives notification from any federal or state agency of a discrepancy in relation to work authorization, for example a "mismatch" letter from the Social Security Administration.
- New requirements related to I-9 Employment Eligibility Verification government audits and investigations conducted by U.S. Immigration and Customs Enforcement (ICE).
- Employers must provide notice to each current employee of any inspections of I-9 forms or other employment records conducted by the inspecting entity within 72 hours after receiving notice of the inspection.

- If during an inspection of the employer's I-9 forms, the inspecting entity determines that the employee's work authorization documents do not establish that the employee is authorized to work in the United States and provides the employer with notice of that determination, the employer must provide a written notice of that determination to the employee within five (5) business days, unless a shorter timeline is provided for under federal law or a collective bargaining agreement.

It is important for employers to be aware of these new provisions, as a violation allows an employee or applicant for employment to commence action to enforce these provisions. If the employee or applicant prevails in court, they may be awarded actual damages plus costs along with additional monetary penalties.

Compliance Steps for Employers We recommend employers take the following steps to ensure compliance with the new requirements.

- Evaluate how your Company currently uses E-Verify and similar systems to ensure compliance with both state and federal law.
- Ensure that all personnel involved in hiring and employment verification receive training on the new requirements and understand the proper procedures for handling discrepancies or challenges to verification results.
- Implement or update internal policies to ensure that the required records are maintained and readily accessible in case of an audit or dispute.
- Contact legal counsel immediately in the event of a government I-9 audit or other ICE inspection to ensure proper notices are provided to employees.

Source: Lexology - Michael Best & Friedrick LLP - Kelly M. Fortier and Kelly R. Rourke

Oregon courts clear 47K residential eviction records

The state begins clearing eviction records to improve housing access, with 47,000 cases sealed and 50,000 more under review.

Oregon's state courts have cleared about 47,000 residential eviction records from people's backgrounds, a significant step toward reducing barriers to housing access under a new state law.

The law, ORS 105.164 (House Bill 2001, 2023), requires courts to "set aside" and "seal" past residential evictions that meet specific criteria. These sealed evictions will no longer appear in background checks, legally treated as if they never occurred. Judicial department staff manually reviewed approximately 160,000 eviction cases dating back to 2014 to determine eligibility. The December clearance represents the first phase of a broader effort to address housing challenges.

"An eviction can affect a renter's ability to qualify for another rental and can have downstream effects on homelessness and transitory housing arrangements, health, and/or employment," according to a 2023 bill summary from the House Committee on Housing and Homelessness.

The law applies to eviction cases where a court entered a judgment after Jan. 1, 2014, with additional specific eligibility requirements detailed on the judicial department's website.

Court officials emphasized that the 47,000 records sealed in December are just the beginning. An additional backlog of approximately 50,000 cases remains under review, with a goal of completing those by the end of 2025.
Moving forward, state courts will automatically set aside eligible cases annually, creating a more streamlined process for record clearance.

Individuals can check whether their past eviction was set aside and request a copy of their set-aside order through the judicial department's eviction set-asides webpage, available in multiple languages.

Source: KGW

Florida HR Considerations: Marijuana in the Workplace

Florida employers should take note of new developments regarding marijuana use.

First, a recent circuit court decision (which is now on appeal) held that the Florida Civil Rights Act (FCRA) requires employers to consider reasonable accommodations for off-duty medical marijuana use. In *Giambrone v. Hillsborough County* (Fla. 13th Cir. Ct. Dec. 10, 2024), the employee who worked for Hillsborough County as an Emergency Medical Technician (EMT) tested positive for marijuana following a random drug test. In accordance with an applicable collective bargaining agreement and the County's Drug Free Workplace policy, the employee presented his employer and the testing doctor with a valid medical marijuana card. The County nevertheless placed the employee on administrative leave without pay. It admitted in court proceedings, however, that there had been no allegations that the employee used marijuana during work hours or that his job performance was impacted by his off-duty marijuana use.

The employee sued the County, alleging a failure to accommodate in violation of the FCRA as well as wrongful termination and breach of contract for failure to accept his state-issued medical marijuana card. Analyzing the relevant provisions of the Florida Constitution and Florida statutes legalizing medical marijuana, the court found that while the plain language of the law does not require accommodation for on-site use, it does require employers to accommodate the qualified patient's off-site use of medical marijuana. Here, there was no factual dispute as to whether the employee met the definition of a qualified patient, as he suffers from anxiety, PTSD, and insomnia which "substantially limits one or more of his major life activities on a daily basis when he is not properly medicated". Therefore, the court concluded that the employee was protected under the FCRA and the County violated the law by failing to make a reasonable accommodation. The court was unpersuaded by the County's argument that marijuana remains illegal under federal law, specifically finding it significant that the employee's EMT license was supervised by Florida *state law* and that, under the collective bargaining agreement, the employee was entitled to report the use of prescription medications authorized under federal *or state law* to explain positive drug test results.

As noted above, the County has appealed this decision to Florida's Second District Court of Appeal; however, employers should proceed with caution in assessing adverse action against a medical marijuana user.

Second, on the heels of this decision, a bill was introduced in the Florida Legislature that would require public employers to consider reasonable accommodations for medical marijuana users, and there is a renewed effort to approve a 2026 voter initiative to legalize recreational marijuana for adults. While a similar measure failed to garner sufficient support in the November 2024 general election, the new initiative includes several updates to address prior criticisms, including making clear that smoking and vaping in any public place would be prohibited.

In light of these marijuana related developments, including employee marijuana use protections, Florida employers should consider reviewing their drug-free workplace policies and procedures.

Source: Lexology – Proskaurer Rose – Jurate Schwarts, Guy Brenner, Arielle E. Kobets and Jake Lee

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

COURT CASES

FL Court Limits Employer Actions for Off-Site Marijuana Use

A Florida court recently held that an employer violated the Florida Civil Rights Act (FCRA) when it suspended an employee for using medical marijuana outside of work. The decision in *Giambrone v. Hillsborough County* raises questions about Florida employers' workplace drug testing policies.

The employee worked for Hillsborough County as an emergency medical technician (EMT). After testing positive for marijuana during a random drug screening, he explained to the county that he was lawfully prescribed medical marijuana for anxiety and severe insomnia. Significantly, the employee had never possessed marijuana at work, never been under the influence at work, and never had any problems with his work performance. Despite this, the county suspended him for the failed drug test.

The employee sued the county, arguing that it failed to accommodate his disabilities. The county maintained that the suspension was justified because marijuana remains federally illegal, and the employee failed a drug test. The county also argued that employee failed to seek accommodations because he did not disclose his prescription until after the drug test.
The court rejected the county's arguments and ruled in favor of the employee. The court acknowledged that marijuana remains illegal under federal law and agreed that employers may forbid marijuana use in the workplace. But by suspending the employee for *off-site* use of marijuana to treat his disabilities—treatment which complied with state law and did not intrude into the workplace—the court ruled the county violated the employee's rights.

Notably, it did not matter that the employee failed to seek accommodations in advance. As the court explained, he had no reason to ask. He was not attempting to use marijuana at work, and it was not affecting his job performance.

The court also distinguished another case, *Ortiz v. Department of Corrections*, where a correctional officer was lawfully terminated for using medical marijuana. In *Ortiz*, the officer was required to carry a firearm—a felony for marijuana users. Florida correctional officers cannot remain certified if they commit a state *or* federal felony, even if they are never charged with a crime. But there is no such requirement for EMTs. Indeed, the Florida Department of Health determined that the employee fully complied with the conditions of his EMT license. Accordingly, the court held the county violated the FCRA when it refused to accept the employee's medical marijuana card as justification for the positive drug test.

It is unclear whether the county will appeal the ruling. Although this is a trial court decision that does not create binding precedent, it may suggest how other judges will evaluate the issue when presented with cases involving marijuana use outside of work. Even though medical marijuana remains federally illegal, Florida employers should carefully review their accommodation policies and consider whether they account for rights granted by state law.

Source: Lexology - Phelps Dunbar LLP - Jason A. Pill and Wesley D. Thorp

INTERNATIONAL DEVELOPMENTS

PLEASE NOTE: Spellings of words in International articles such as those written in the British English format are native to the original author and differ from the spellings of words in the American English format.

Safety-critical workers: Diminished expectation of privacy in alcohol and drug testing

The Federal Court of Appeal recently issued a decision signaling that employees working in safety-critical roles have a "diminished expectation of privacy" in regard to random alcohol and drug testing. Given the unique environment of a safety-critical worker's job, including the highly regulated nature of their work and the public interest in ensuring safety, the diminished expectation of privacy may be justified in certain circumstances.

Background information – "pre-placement" and random alcohol and drug testing

In *Power Workers' Union v Canada (Attorney General)*, 2024 FCA 182 the Court of Appeal reviewed the validity of "pre-placement" and random alcohol and drug testing, which the Canadian Nuclear Safety Commission (the "Commission") wanted to impose as a licence condition for those licensed to operate high security nuclear facilities. Safety-critical workers include employees who make decisions or take actions that have a direct and immediate impact on nuclear safety.

Six affected workers and their union claimed that pre-placement and random alcohol and drug testing breached their rights under the *Canadian Charter of Rights and Freedoms*, including: section 7 which is the right to life, liberty and security of the person; section 8 which includes the right to be secure against unreasonable search and seizure; and the right to equality under section 15.

Alternatively, they claimed the licence requirement was unreasonable on administrative law grounds. The workers brought applications for judicial review, which the application judge dismissed on all grounds.

The Federal Court of Appeal's comments

Section 8

The Federal Court of Appeal began by focusing on section 8 of the *Charter* and the right to be secure against unreasonable search and seizure. The court did not deny alcohol and drug tests involved the collection of personal information and therefore amounted to a search and seizure. However, the court noted this was a relatively non-invasive process.

A section 8 challenge to a search and seizure requires a two-step analysis: 1) does the impugned search or seizure interfere with an individual's reasonable expectation of privacy? 2) if so, is the action reasonable?

Having acknowledged there was a search and seizure and that section 8 of the *Charter* was engaged, the court stated that the reasonable expectation of privacy requires an analysis of the unique context of the case – particularly here, where the highly regulated nuclear industry considers safety the most important priority given the potential for devastating and long lasting impacts in the event of a nuclear incident.

The court decided it was not necessary to find evidence of a substance abuse problem in the workplace before implementing testing requirements. Ultimately, a pre-emptive and proactive approach to safety measures was favoured over a "wait and see" approach, given the severe consequences that could follow.

Turning to whether the testing was reasonable, the court considered the highly regulated nature of the nuclear industry, stating the main purpose of the regulatory framework was to limit the risks to national security, the health and safety of people, and the environment. As a result, an employee's fitness for duty plays a key role in reducing the risks of impairment-related safety events. The court emphasized that the nuclear industry is unlike other inherently dangerous industries given the magnitude and dangers a nuclear incident can cause.

Considering the context of this case, the court concluded there was a diminished expectation of privacy for safety-critical workers. Although the testing requirements engage section 8, they do not infringe the rights conferred under that section. The testing requirements were considered authorized by law and reasonable considering the regulatory context, the public

interest in nuclear safety, the need to bolster fitness for duty programs, the reliability of the testing methodology and the availability of judicial oversight.

Sections 7 and 15
The court considered, and rejected, the alleged violation of section 7 of the *Charter*, noting there is no danger to the security of the person because the tests included the non-invasive taking of saliva, urine or breath samples.

Finally, the court considered, and also rejected, the alleged violation of section 15 of the *Charter* based on the union's failure to establish that the testing requirements created a distinction or had a disproportionate impact based on an enumerated or analogous ground of discrimination. There was no evidence the testing requirements would result in an arbitrary disadvantage for safety-critical workers with drug or alcohol dependencies and no evidence to establish the testing requirements are discriminatory by being arbitrary or prejudicial.

The Federal Court of Appeal agreed with the application judge and dismissed the appeal, noting there is no breach of the Charter given the safety-critical nature of the work.

Takeaways for employers

This decision from the Federal Court of Appeal provides some important points to consider for employers in determining whether it is appropriate to implement random alcohol and drug testing in the workplace:

1. First, the appropriateness of these measures will be based on the specific job and nature of the industry involved. In this case, the safety-critical nature of the work in the nuclear industry led the court to finding that employees in this industry have a diminished expectation of privacy when it comes to random alcohol and drug testing. This analysis is likely to apply in other safety-sensitive contexts.
2. Second, random alcohol and drug testing imposed on all employees in a dangerous workplace is generally rejected for being unreasonable, however, when it applies to a subset of only safety-critical workers, it is less likely to be scrutinized. In this particular case, the safety-critical workers represented less than 10% of the nuclear industry's entire workforce and was not imposed on workers outside safety-critical roles.
3. Third, if alcohol and drug testing is implemented, it is important that the method used is reliable, consistent and accurate at detecting drug and alcohol impairment. In confirming the testing was reasonable, the court noted the reliability and accuracy of the system used to help support the testing being implemented as a license condition.
4. Finally, any program, such as alcohol and drug testing, that involves the collection, use and disclosure of personal information (almost anything about an identifiable individual) should be reviewed from a privacy perspective to enable the program to be developed and implemented in accordance with privacy laws and minimize privacy related risks.

Source: Lexology - MLT Aikins - Riley Cockwill, Stephanie Yang Morris and Kristel Kriel

Background checks on employees / candidates in light of Polish law

Employers, especially those that are part of foreign groups, sometimes wish to carry out background checks, to analyse information concerning the circumstances or status of job candidates or employees beyond the extent of their legal right to do so. As this involves the processing of candidates' or employees' personal data, employers should make sure that what they do complies with the legislation before undertaking any activities in this respect.

This article focuses on issues relating to background checks carried out by employers in relation to candidates and employees. We do not refer to situations that are similar but materially different in terms of regulatory implications, such as:

- Background checks carried out in respect of persons providing services on a basis other than an employment contract
- An employer's processing of publicly available information (such as that published on social media)
- Situations where an employer carries out background checks on its employees not on its own behalf, but on behalf of a client with whom the employee in question would be engaged to carry out a specific assignment.

Can employers carry out background checks on employees?

Conducting most types of background checks can be problematic from the point of view of Polish regulations, especially if the information was not to be collected directly from the job candidate or employee. However, even where information is collected directly from them, Polish employment and data protection laws significantly limit the scope of personal data and documents that employers may request, effectively limiting their ability to carry out background checks.

Whether a particular type of background check will be permissible under Polish law depends on the type of activities to be performed as part of that check. In practice, background checks may have very different forms. Some may take this term to mean verification of references from previous employers, verification of a university diploma or checking a person's identity, while others may mean verification of a criminal record, family situation or credit history. Different restrictions will apply to each of these background checks.

Background checks and the Labour Code

As regards information collected directly from the job candidate/employee, the Labour Code contains **a closed catalogue of personal data** that an employer can request. This list **does not include credit history, financial condition or family situation**. Therefore, an employer's request for this type of information from a candidate or employee may be considered a breach of the law and, in principle, may only be allowed in exceptional cases. Importantly, even obtaining the candidate or employee's consent to carry out a verification that involves the processing of personal data that goes beyond the catalogue under the Labour Code does not eliminate legal risks for the employer, as this type of consent can easily be considered as having been given involuntarily, therefore making it invalid under data-protection legislation.

Personal data, **to the extent that the Labour Code allows it to be obtained**, shall be made available to the employer in the form of candidate/employee statement. The employer may request documents necessary to corroborate the statement in question (in principle, this is the only permissible check on the veracity of the information provided).

According to the President of the Personal Data Protection Office (PUODO), an employer cannot independently contact a previous employer to obtain information about a candidate (references). This would only be permissible if the candidate has voluntarily consented to this (and the employer should be able to prove that consent was voluntarily given). Even if the candidate provides the reference on their own initiative, the employer is not entitled to contact the previous employer for additional information. According to PUODO, the employer is also not entitled to contact educational institutions to confirm the authenticity of the education data provided.

Indeed, this limits the ability of employers to carry out background checks on their own, without the candidate's involvement**, even with regard to personal data that the employer may obtain under the Labour Code**. Even if the candidate agrees to certain background checks (such as contacting the university or former employer), unless the employee independently and on their initiative provides certain information, the carrying out of background checks by the employer is not without risks from a regulatory perspective, as there is a risk that the candidate's consent to the processing of personal data in connection with the background check may be deemed involuntary and, therefore, invalid under data protection legislation.

Background checks on criminal records

One of the most popular background checks that employers would like to carry out is the verification of a person's criminal record. Importantly, due to data protection legislation, **an employer cannot process personal data of candidates/employees regarding their criminal records unless there is separate legislation that permits such processing** (in the absence of such legislation, the prohibition of processing such personal data even on the basis of consent derives from the Labour Code), **and only to the extent that such legislation permits such processing**. Few provisions allow for criminal record verification.

An important exception is the Act of 12 April 2018 on the principles of obtaining information on the criminal record of job applicants and persons employed by entities operating in the financial sector**.** Under this law, it is possible, under certain conditions, to request criminal record information from candidates/employees. However, the employer should make a prior analysis to determine whether the provisions of this Act will apply to a particular employer at all (given the wording of the Act, this analysis may be relatively complex). Even if the provisions do apply in a particular case, they contain a number of restrictions on the criminal record verification process. An employer that is an entity operating in the financial sector may check the criminal record of candidates or employees if those persons are to work or are already employed in managing the entity's or a third parties' property, access to legally protected information, making decisions with a high risk of losing the

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

entity's or third parties' property or causing other significant damage to the entity or third parties. In addition, employers may only verify criminal records for the offences specified in the Act.

***

As can be seen, the possibility for employers in Poland to legally carry out background checks is very limited. Before starting such checks, it is advisable to analyse whether and to what extent doing so will be legally permissible. In some cases, specific regulations may apply, such as work with children or work in the financial sector – which may result in some background checks being allowed (and in some cases even required), but only to the extent permitted by these regulations.

Source: Lexology - MLT Aikins - Riley Cockwill, Stephanie Yang Morris and Kristel Kriel

© ClearStar, Inc., All Rights Reserved | 888.982.4648 | clearstar.net

MISCELLANEOUS DEVELOPMENTS

EEOC Guidance Provides Valuable Advice for Employers Facing Complaints of Harassment

The Equal Employment Opportunity Commission's (EEOC) updated Enforcement Guidance on Harassment in the Workplace, while not the law, represents the EEOC's interpretation of federal law and provides important, risk-minimizing insight for employers who have received complaints of harassment. Indeed, instituting a prompt and thorough investigation upon receipt of a complaint is usually the first step to help avoid costly litigation, preserve a positive workplace culture and ensure a safe work environment for employees going forward.

The EEOC guidance makes clear that an employer is liable for a hostile work environment due to harassment if it (1) unreasonably failed to prevent the harassment or (2) failed to take reasonable corrective action in response to harassment about which it knew or should have known.

Failing to Prevent Harassment
In determining whether an employer took reasonable steps to prevent harassment, the EEOC looks at numerous factors including:

- The adequacy of the employer's anti-harassment policy, complaint procedures and training;
- The degree of authority that the alleged harasser exercised over the complaining employee;
- The adequacy of the employer's training and reporting mechanisms; and
- The employer's efforts to minimize obvious risks (for example, lacking diversity in the workforce, creating workspaces that are isolated and not sufficiently monitored, or failure to protect employees who are vulnerable, etc.).

Investigating a Complaint of Harassment
When an employer has notice of unlawful harassment by both employees and nonemployees, it must act "reasonably" to correct the harassment. This includes conducting a "prompt and adequate investigation." According to the EEOC, an investigation is "prompt" if it is conducted "reasonably soon" after the employer receives the complaint of harassment. This is fact-specific, but, according to the EEOC, waiting two months or more to open an investigation is not prompt unless specific circumstances warranted such a delay. An investigation is "adequate" if it is sufficiently thorough to obtain a "reasonably fair estimate of the truth." This means that, at minimum, the investigation must be conducted by a neutral party and must seek information about the conduct from all parties involved. The alleged harasser should not be a supervisor of the individual conducting the investigation and should not have direct or indirect control over the investigation. Where there are conflicting versions of events, as is typically the case, the investigator will have to make credibility determinations. For this reason, the person conducting the investigation should be well-trained in interviewing witnesses and evaluating credibility.

Employers should consider whether intermediate measures are needed during the pendency of the investigation, for example adjusting schedules to avoid contact between the parties, temporarily transferring the alleged harasser or placing the alleged harasser on paid leave and suspending any terminations or adverse job decisions. The complaining employee should not be subjected to any negative consequences both during and after the investigation.

When the investigation is concluded, the employer should inform the complainant and the alleged harasser of its determination and any corrective action that it will be taking, subject to any applicable privacy laws. Employers must retain records of harassment complaints and investigations. Upon a finding of harassment, an employer must take corrective action that is "reasonably calculated to prevent further harassment."

Employers are thus encouraged to act swiftly in dealing with harassment complaints and can help shield themselves from liability if an investigation is properly implemented.

Best Practices for Employers

Be Proactive

Review your anti-harassment policy and distribution practices to ensure that all employees are aware of and can easily access the policy. You should send your anti-harassment policy to all employees annually and have each employee sign an acknowledgment that it has been received and reviewed. Make sure the policy includes a clear process for how complaints should be reported and how the company will investigate the complaint.

Training Is Key
In addition to anti-harassment training for all employees, make sure supervisory employees are aware of reporting requirements and receive specialized supervisor training.

Act Quickly
Delays in taking action can not only increase the risk that an employer will be held liable for harassment but can cast doubt on the employer's entire procedure for responding to harassment. Acting quickly also sends a strong message to employees that complaints are taken seriously.

Select the Right Investigator
Choosing the right person to investigate a complaint is crucial. Investigations can be completed in-house if the human resources department is experienced in conducting harassment investigations and no conflicts of interest exist. If the alleged harasser is a supervisory employee, members of the human resources team are involved in the conduct under investigation (either as witnesses, complaining employees, or as alleged harassers), or other circumstances warrant impartiality, engaging outside counsel to conduct the investigation is recommended. Also, if conducted by counsel for the purpose of providing legal assistance, the investigation will likely be protected by attorney-client privilege.

Assess Any Litigation Risk
Consider whether a litigation hold is necessary during the investigation to preserve documents and evidence.

Source: Lexology - Duan Morris LLP – Bronwyn L. Robers and Charlotte Drew