APRIL 2024

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

CLEARSTAR®

TABLE OF CONTENTS

SCREENING COMPLIANCE UPDATE | APRIL 2024

ClearStar is happy to share the below industry related articles written by subject matter experts and published on the internet in order to assist you in establishing and keeping a compliant background screening program.

FEDERAL DEVELOPMENTS

General Counsel of the CFPB Delivers Remarks Focusing on Medical Collections and Tenant Screening

In a recent speech at the National Consumer Law Center/National Association of Consumer Advocates Spring Training, Seth Frotman, General Counsel of the Consumer Financial Protection Bureau (CFPB or Bureau), focused on medical billing and collections and tenant screening and debt, emphasizing the CFPB's enforcement of the Fair Debt Collection Practices Act (FDCPA) and Fair Credit Reporting Act (FCRA) in these areas.

Medical Collections and Consumer Reporting

According to Frotman, as healthcare costs rise families are being burdened with medical bills that they should not or do not owe. The CFPB has purportedly received over 15,000 complaints about debt collectors pursuing unpaid medical bills in the past two years. Frotman emphasized that debt collectors are strictly liable under the FDCPA for any misrepresentations they make about whether and how much a consumer owes. Additionally, a debt collector violates the FDCPA if they collect an amount that is no longer correct, such as when an insurance company or patient has made a payment on the bill.

The CFPB is also focused on the issue of medical bills appearing on credit reports. The Bureau has initiated a rulemaking process, discussed here, to remove medical bills from credit reports used by creditors as a matter of federal law.

Rental Collections and Consumer Reporting

Frotman also discussed the collection and reporting of unpaid rent. According to Frotman, as corporate landlords have increased their rental holdings, demand has substantially increased for "tenant screening" products that perform digital, algorithmic scoring of prospective tenants. The CFPB has purportedly received complaints from renters about inaccuracies and errors on tenant screening reports that have a long impact on their housing opportunities.

As discussed here, the CFPB recently issued an advisory opinion on background screening emphasizing that consumer reporting agencies, including those offering tenant screening products, must under the FCRA maintain reasonable procedures to avoid producing reports with false or misleading information.

The CFPB has also seen debt collection activity related to rental debt increase substantially over the last several years. The CFPB is monitoring debt collection and consumer reporting complaints involving rental-related activity. The CFPB has emphasized that the FDCPA applies to the collection of residential rental debt by debt collectors, including by attorneys. Thus, law firms can be held liable under the FDCPA if they approve eviction actions without performing a meaningful review of each case. Additionally, according to Frotman, debt collectors acting on behalf of landlords may violate the FDCPA by collecting amounts that are inflated by fees that are not owed as a matter of state law. He gave the example that landlords may improperly charge tenants for basic repairs and routine upkeep that should be the landlord's financial responsibility under the warranty of habitability in most states. These amounts may then improperly end up in debt collection actions subject to the FDCPA or on credit reports.

Frotman concluded his remarks by encouraging the attendees to tell the Bureau about their cases in this area. "The CFPB has an active amicus brief program. And we rely on monitoring of active litigation to bring to our attention emerging issues and areas of concern."

CLICK HERE.

Enforcement Guidance on Harassment in the Workplace

On April 29, 2024, the EEOC issued a new Enforcement Guidance on Harassment in the Workplace under EEOC-enforced laws. The guidance became effective on the same day. The Enforcement Guidance supersedes Compliance Manual Section 615: Harassment *(1987);* Policy Guidance on Current Issues of Sexual Harassment *(1990);* Policy Guidance on Employer

Liability under Title VII for Sexual Favoritism *(1990);* Enforcement Guidance on Harris v. Forklift Sys., Inc. (1994); and *Enforcement Guidance on Vicarious Employer Liability for Unlawful Harassment by Supervisors* (1999).
For more information on the Enforcement Guidance, you can review it at:
https://www.eeoc.gov/laws/guidance/enforcement-guidance-harassment-workplace#_Toc164807993

CLICK HERE.

STATE, CITY, COUNTY AND MUNICIPAL DEVELOPMENTS

LA County Passes Fair Chance Ordinance on Employer Consideration of Criminal History

The County of Los Angeles has announced a new Fair Chance Ordinance, taking effect on September 3, 2024, that will regulate the consideration of criminal history information by employers with five or more employees in unincorporated areas of the county. While some of the new requirements align with similar requirements under California's existing fair chance laws, many of the ordinance's provisions impose entirely new requirements. Employers that fail to update their background check processes to comply with the amendments could face a private civil action or significant civil penalties. The new ordinance (the Ordinance) is one of several fair chance laws with which California employers must comply. For example, the California Fair Chance Act (Fair Chance Act) requires employers considering criminal history information to follow strict rules, which were expanded by amended regulations that went into effect last year. In addition, the City of Los Angeles previously enacted the Fair Chance Initiative for Hiring Ordinance (FCIHO), imposing additional limitations and procedural requirements on employers that consider an applicant's criminal history when making employment decisions.

Below we highlight notable aspects of the new Ordinance, including similarities and differences between the Ordinance and the existing Fair Chance Act and FCIHO. However, this LawFlash does not cover all aspects of the Ordinance. The full text of the Ordinance can be found here.

REQUIREMENTS FOR JOB POSTINGS AND CONDITIONAL OFFER LETTERS

Similar to the FCIHO, the new Ordinance requires employers to state in job postings that qualified applicants with criminal histories will be considered for employment. However, the Ordinance uniquely requires "regulated employers" that are "required by local, State or federal law or regulation to restrict or prohibit the hiring of individuals with certain specified Criminal History for the job position" to identify such laws or regulations in all job postings.

Moreover, if an employer intends to review an applicant's criminal history in connection with a conditional offer of employment, the job posting must include a list of "all material job duties of the specific job position which the Employer reasonably believes that Criminal History may have a direct, adverse and negative relationship potentially resulting in the withdrawal of the Conditional Offer."

The Ordinance identifies several statements that must be incorporated into conditional offer letters, including a statement that the conditional offer is contingent upon the review of the individual's criminal history and a statement that the employer has "good cause" to conduct a review of criminal history for the specific job, with supporting justification provided in writing.

"Good cause" exists where

- the employer faces a significant risk to its business operations or business reputation unless a review of criminal history is conducted for the specific job position; or
- a review of criminal history is necessary for the specific job position due to articulable concerns regarding the safety of, or risk of harm or harassment to, the employer's staff, employees, contractors, vendors, associates, clients, customers, or the general public.

Finally, if the employer is reviewing additional information, background, or history in addition to criminal history in connection with a conditional offer of employment, the conditional offer letter must include a "complete list of all types of information, background or history that will be reviewed by the employer," including education, social media history, employment history, motor vehicle or driving history, reference checks, credit history, license or credential verification, drug testing, or medical examinations.

NOTIFYING APPLICANTS OF PRELIMINARY ADVERSE ACTION DECISION BASED ON CRIMINAL HISTORY

Prior to taking adverse action against an applicant based on criminal history, employers in California must conduct an individualized assessment of the applicant's criminal history and provide the applicant with written notice of the preliminary decision to take adverse action (a pre-adverse action notice).

Unlike the statewide Fair Chance Act, the new Ordinance and FCIHO require Los Angeles employers to provide a written copy of the individualized assessment to the applicant along with the pre-adverse action notice.[1] However, whereas the Fair Chance Act and FCIHO allow employers to send pre-adverse action documents to applicants by either email or regular mail, the new Ordinance requires employers to send pre-adverse action documents by both email **and** regular mail whenever email is available.

PROHIBITION ON CONSIDERING CONVICTIONS MORE THAN SEVEN YEARS OLD

The Ordinance also prohibits employers from considering a conviction that is more than seven years old unless certain exceptions apply, including when the applicant or employee will be providing care to a minor or dependent adult. The seven-year lookback period is measured from the date of disposition of the conviction.

ORDINANCE REQUIREMENTS THAT TRACK REQUIREMENTS OF FAIR CHANCE ACT

As with last year's amended regulations for the Fair Chance Act, the new Ordinance clarifies when a pre-adverse action notice is considered "received" by an applicant. Specifically, if sent by email, the pre-adverse action notice is considered "received" two business days after it was sent. However, if the notice was sent by US mail without tracking to an applicant in California, it is considered "received" five calendar days following the employer's placement of the notice in the mail. If the applicant's residential address is located outside of the state, the notice is considered "received" 10 calendar days after the notice is placed in the mail by the employer.

However, the Ordinance gives applicants more time to respond to the pre-adverse action notice than they are afforded under the existing Fair Chance Act and FCIHO. Under those frameworks, an applicant has five business days from the date they "receive" a pre-adverse action notice to respond to the notice with rehabilitation information and mitigating evidence that an employer must consider before a final adverse decision is made.

While the Ordinance also uses a five-business-day response window, the response deadline must conform to the date on which the pre-adverse action notice is considered "received" in the mail. Specifically, the Ordinance provides that, even when the pre-adverse action notice is sent via email, the "timelines to respond to the notice will be calculated based on the date the notice was mailed." In effect, this means that the Ordinance requires an employer to provide an applicant with a minimum of five calendar days from the date on which a pre-adverse action notice is **mailed** to the applicant and an additional five business days before the employer may finalize any adverse decision.

Similarly, if an applicant informs the employer in writing that the applicant disputes the accuracy of the criminal history information and is taking specific steps to obtain evidence supporting that assertion and/or the applicant needs additional time to obtain written evidence of rehabilitation or mitigating circumstances, the employer must provide the applicant with 10 additional business days to provide this information. In contrast, the Fair Chance Act only provides such applicants with five additional business days.

For applicants covered by the new Ordinance, employers must include this new timeline, as well as an explanation of when the pre-adverse action notice will be deemed "received," in the pre-adverse action notice in bold or underlined font or in all capital letters.

PROVIDING EVIDENCE OF REHABILITATION OR MITIGATING CIRCUMSTANCES OVER THE PHONE OR IN PERSON

The new Ordinance provides applicants with ample methods for providing evidence of rehabilitation or mitigating circumstances to employers. Specifically, in lieu of submitting written materials to an employer, an applicant may request an opportunity to present evidence of rehabilitation or mitigating circumstances in person, virtually, or via telephone contact with the employer.

If the applicant requests this opportunity within five business days of receiving the pre-adverse action notice, the employer must give the applicant the opportunity to provide this information within 10 business days of the request.

PROCESS FOR NOTIFYING APPLICANTS OF A FINAL ADVERSE ACTION DECISION

Under the existing Fair Chance Act and FCIHO, an employer must perform a written reassessment of an applicant's criminal history if the applicant provides information in response to the pre-adverse action notice. However, the new Ordinance requires employers to conduct a "second individualized assessment" regardless of whether the applicant responded to the pre-adverse action notice and provide a written copy of that individualized assessment to the applicant.

Unlike the City of Los Angeles with the FCIHO, the county has not provided a sample notice that employers should use when providing applicants with a copy of individualized assessments under the new Ordinance.

Similar to the statewide Fair Chance Act, which requires a final adverse action notice to inform applicants of their right to file a charge with the California Civil Rights Division, the new Ordinance additionally requires the final adverse action notice to notify applicants of their right to file a charge with the Los Angeles County Department of Consumer and Business Affairs (DCBA) for a violation of the Ordinance.

Uniquely, if an employer provides the final adverse action notice to an applicant more than 30 calendar days after the applicant provided a timely response to the employer's pre-adverse action notice, the Ordinance presumes that the employer's delay was untimely and thus a violation of the Ordinance. To rebut this presumption, the employer must provide a written explanation in the final adverse action notice that justifies why the final decision was not made within 30 days. The Ordinance states that this explanation may include a description of circumstances involving a business or personal emergency or delays outside of the employer's control.

WORKPLACE POSTING REQUIREMENTS

Employers with a workplace, job site, or other location in the unincorporated areas of Los Angeles County that is under the employer's control and frequently visited by their employees or applicants must post a notice informing applicants and employees of the provisions of the Ordinance in a conspicuous place. Employers must also post the notice on webpages frequented by their employees or applicants and send a copy of the notice to each labor union or representative of workers with which they have a collective bargaining agreement or other agreement or understanding that is applicable to employees in the unincorporated areas of Los Angeles County.

CIVIL PENALTIES AND PRIVATE RIGHT OF ACTION

Violations of the Ordinance expose an employer to a penalty of up to $5,000 for a first violation, $10,000 for a second violation, and $20,000 for the third and subsequent violations. These penalties are higher than those under the FCIHO, where employers face a $500 penalty for a first violation, $1,000 for a second violation, and $2,000 for a third violation. Penalties under the new Ordinance are calculated on a per-violation basis, under which an employer may be liable for multiple penalties if a single violation impacts multiple individuals.

The Ordinance allows the DCBA to investigate violations of the new Ordinance and impose civil penalties. However, the Ordinance also provides applicants or employees the option to bring a civil action in court upon timely submission of an intent-to-sue notice to the DCBA, which will allow a civil action to be brought against the employer within one year from the date of the notice.

CLICK HERE.

Kentucky Passes a Comprehensive Privacy Law Becoming the Next State to Join the Privacy Race

On April 4, 2024, Governor Andy Beshear signed into law Kentucky's comprehensive privacy legislation, H.B. 15 (the Act), officially placing Kentucky as the nation's sixteenth state to join the privacy legislation race. The Act, which mirrors Virginia's comprehensive privacy law, is set to take effect January 1, 2026.

The Act applies to entities that conduct business in Kentucky or produce products/services targeted to Kentucky residents and that annually (1) control or process personal data of 100,000 consumers or, (2) control or process personal data of 25,000 consumers, if over 50% of gross revenue is derived from the sale of personal data. Notably, exemptions exist for government entities, certain financial institutions, HIPAA covered entities, and nonprofit organizations, institutions of higher education to name a few.

Following the steps of other states, the Act grants consumers the rights of access, deletion, portability, correction, and opt-out of targeted advertising, sale of data, and profiling. It also required processors to obtain consent for the processing of sensitive personal data. Like Virginia, Kentucky requires Data Protection Impact Assessments (DPIAs) for processing activities that involve targeted advertising, the sale of personal data, profiling under specific circumstances, processing of sensitive data, or would present a heightened risk to consumers. The Kentucky Attorney General has been tasked with enforcement and controllers and processors have a 30-day cure period.

Kentucky's new law adds to the growing complexity of compliance with U.S. privacy laws.

CLICK HERE.

Nebraska Enacts Comprehensive Data Privacy Law

On 17 April 2024, Nebraska Governor Jim Pillen signed into law omnibus Legislative Bill 1074, which includes the Nebraska Data Privacy Act, making Nebraska the seventeenth state to adopt comprehensive data privacy legislation. This signing continues the unprecedented momentum as Nebraska is the fourth state to enact a data privacy law in 2024 alone. The Nebraska Data Privacy Act will take effect on 1 January, 2025. The Nebraska Office of the Attorney General will have exclusive enforcement authority, and there is no private right of action available under this act. In this latest in our series of articles on US State Data Privacy Laws, we have summarised below the key components of Nebraska Data Privacy Act.

To whom does Nebraska's Data Privacy Act apply?

Nebraska's Data Privacy Act imposes obligations to a person that:

- conducts business in Nebraska or produces a product or service consumed by residents of Nebraska;
- processes or engages in the sale of personal data; and
- is not a small business as determined under the federal Small Business Act, except if such person engages in the sale of sensitive data without receiving prior consent from the consumer.

Notably, similar to the Texas Data Privacy and Security Act, the Nebraska Data Privacy Act does not contain a revenue threshold nor a minimum number of consumers whose personal data is processed or sold for the law to apply. As such, the Act will sweep up a broader array of businesses under its jurisdiction. The Nebraska Data Privacy Act exempts several categories of entities, including state and city government agencies; financial institutions and data regulated by the Gramm-Leach-Bliley Act; nonprofit organizations; and covered entities and business associates as defined by the Health Insurance Portability and Accountability Act (HIPAA). Certain types of information and data are also exempted, including health records, consumer credit-reporting data, data covered by the Drivers' Privacy Protection Act, Family Educational Rights and Privacy Act, Farm Credit Act, and data covered by HIPAA (i.e. Protected Health Information).

What rights does Nebraska's Data Privacy Act give to consumers?

Nebraska's Data Privacy Act gives consumers rights that are largely consistent with other US State Data Privacy Laws. Consumers - Nebraska residents acting only in an individual or household context, and not in a commercial or employment context, may:

- **Confirm** whether a controller is processing their personal data and access the personal data;
- **Correct** inaccuracies in their personal data, taking into account the nature of the personal data and the purposes of the processing of their personal data;
- **Delete** their personal data provided by or obtained about the consumers;
- **Obtain** a copy of their personal data that the consumer previously provided to the controller in a portable and readily usable format (to the extent technically feasible)(i.e. data portability); and

- **Opt out** of the processing of their personal data for the purposes of targeted advertising, the sale of their personal data, or profiling in furtherance of a decision that produces a legal or similarly significant effect concerning the consumer.

Nebraska's Data Privacy Act requires controllers who receive a request from a consumer seeking to exercise these rights to respond to the consumer within 45 days of receipt of the request, unless it is reasonably necessary given the complexity and number of the consumer's requests to extend that time for an additional 45 days and the controller notifies the consumer of the extension and the reason within the initial 45 days.

Controllers must inform the consumer within the initial 45 days of the justification for declining to comply and provide instructions on how to appeal the decision to the Nebraska Attorney General. The appeal process must be "conspicuously available and similar to the process for initiating [initial requests]." If the controller denies an appeal, the controller must provide an online mechanism for the consumer to contact the Nebraska Attorney General to submit a complaint.

What obligations does Nebraska's Data Privacy Act impose on controllers and processors?

Nebraska's Data Privacy Act applies to "personal data", which is defined broadly as any information that is "linked or reasonably linkable to an identified or identifiable individual" and, like other US State Data Privacy Laws, excludes de-identified data and publicly available information.

The law requires controllers to provide consumers a reasonably accessible and clear privacy notice that includes: the categories of personal data processed by the controller; its purpose for processing the personal data; information on how consumers may exercise their rights and appeal a controller's decisions; the categories of all third parties to which it shares the personal data and which categories of data it shares and a description of at least two methods through which the consumer may use to submit a request to exercise a consumer right.

Controllers must also:

- Limit the collection of personal data to what is adequate, relevant, and reasonably necessary in relation to the disclosed purposes with which the data is processed – unless the controller obtains the consumer's consent;
- Establish, implement and maintain reasonable administrative, technical, and physical data security practices that are appropriate to the volume and nature of the personal data at issue to protect the confidentiality, integrity, and accessibility of personal data; clearly and conspicuously disclose to consumers if they sell personal data to third parties or process personal data for targeted advertising and provide a clear method for consumers to opt out. Notably, similar to the California Consumer Privacy Act and the Connecticut Data Privacy Act, sale is broadly defined as the exchange of personal data for monetary or other valuable consideration by the controller to a third party;
- Not process "sensitive data" without the consumer's express consent, or in the case of a known child, in accordance with the federal Children's Online Privacy Protection Act of 1998. Sensitive data is defined as personal data revealing racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation or citizen or immigration status; genetic or biometric data that is processed for the purpose of uniquely identifying an individual; personal data collected from a known child; or precise geolocation data;
- Not process personal data in violation of state and federal laws that prohibit unlawful discrimination against consumers;
- Discriminate against a consumer for exercising any of the consumer rights contained in the act; and
- Conduct and document a data protection assessment of: the processing of personal data for purposes of targeted advertising; the sale of personal data; the processing of personal data for profiling, if the profiling presents a reasonably foreseeable risk of unfair or deceptive treatment or unlawful disparate impact on consumers, financial, physical or reputational injury to consumers, or a physical or other intrusion offensive to a reasonable consumer upon their "solitude or seclusion, or the private affairs or concerns", or other substantial injury to any consumer; processing sensitive data; or the processing of personal data that presents a heightened risk of harm to the consumer.

Nebraska's Data Privacy Act also imposes requirements on "processors" (a person who processes personal data on behalf of a controller). Processors must adhere to the instructions of the controller and shall assist the controller to comply with its duties or requirements under the act, including its obligations regarding consumer rights requests, security of data processing

and data protection assessments. Nebraska's Data Privacy Act requires that processing be governed by a contract between the controller and processor that outlines relevant privacy provisions set forth under the act.

Enforcement

Like most of the US State Data Privacy Laws, Nebraska's Data Privacy Act does not provide for a private right of action. The Nebraska Office of the Attorney General has exclusive authority to enforce violations. However, the Nebraska Attorney General must issue the controller or processor a notice of violation prior to initiating any action. A controller or processor will then have 30 days to cure the noticed violation. The Nebraska Attorney General may bring an action in court seeking various forms of relief, including, injunctive relief, civil penalties, and attorney's fees. A court may impose civil penalties of up to $7,500 for each violation.

Key Aspects of Nebraska's Data Privacy Act

- **Definition of a Controller**. Unlike most other US State Data Privacy Laws, Nebraska's Data Privacy Act does not provide for a minimum threshold of consumers' personal information a business must process or a percentage of revenue to be derived from the sale of personal data in order for the law to apply.
- **Activity Qualifying as a Sale of Personal Data**. As note above, similar to California and Connecticut, Nebraska broadly covers exchanges of personal data for valuable consideration as a "sale" of personal data, triggering heightened disclosure and control requirements for consumers for certain activity including online tracking.
- **Right to Delete**. Upon receiving a request to delete, a business must not only delete the personal data it has collected from the consumer, but also the personal data obtained about the consumer from other sources.
- **Permanent 30-day Cure Provision**. Many other state data privacy laws sunset their cure provisions after some months, with the expectation that businesses should have fully implemented the consumer privacy protections by that time. The Nebraska Data Privacy Act, on the other hand, will continue to provide an opportunity to rectify alleged deficiencies.
- **Obtaining Affirmative Consent**. Nebraska's Data Privacy Act requires controllers to first obtain consent before processing consumers' sensitive data, selling sensitive data, as well as before processing the sensitive data of a known child.
- **Processing Agreement Required between Controllers and Processors**. Like certain other US State Data Privacy Laws, the Nebraska's Data Privacy Act requires controllers to enter into contracts with data processors governing the processor's data processing procedures. Contracts under Nebraska's Data Privacy Act must set forth clear instructions for processing personal data, the nature and purpose of processing, the type of data subject to processing, the duration of processing, and the parties' rights and obligations. The law also requires processors to ensure each person processing personal data is subject to a duty of confidentiality with respect to the data and to delete or return personal data upon the controller's request.
- **Right for Consumers to Opt Out**. The Nebraska's Data Privacy Act permits consumers to opt out of the processing of personal data for targeted advertising, the sale of personal data, or profiling in furtherance of a decision that products a legal or similarly significant effect concerning the consumer.

CLICK HERE.

Utah Breach Notice Law Amended, Effective May 1

Utah, among other privacy laws it has enacted or modified recently, has also modified its breach notification law. This follows last year's changes to the law, which among other things codified the state's Cyber Center.

This year's modifications are primarily administrative. The law will now include a definition of "data breach" specifically for purposes of reporting to the Cyber Center (which definition mirrors the breach definition already in the law).

Additionally, the law now affirmatively states that the notification submitted to the Cyber Center as well as information submitted to the Center or the Attorney General will be confidential. (If submitted to the Utah Cyber Center following existing Utah's process for making confidentiality claims).

The law has also been amended to list the specific information which must be provided to the Cyber Center. The list is similar to the information which other agencies who receive notices require, including the date the breach occurred and the date of discovery. Also required is the number of people impacted, including those impacted in Utah and the type of information impacted. Also required is the submission of a short description of the incident.

Putting It Into Practice: Updating its breach notice law seems to be an annual occurrence for Utah. These changes are not significantly different from obligations under other states' laws. Come May 1, companies will want to keep track of these procedures for incidents that trigger Utah reporting requirements.

CLICK HERE.

COURT CASES

Municipal Violation Is Not 'Arrest Record' Covered by Wisconsin Fair Employment Act, Court Holds

The Wisconsin Fair Employment Act's (WFEA's) prohibition against discrimination based on employees' arrest and conviction record has always been considered broad, and its standard of allowing employers to make employment decisions only based on "substantially related" offenses is equally nuanced. The Wisconsin Court of Appeals has narrowed the scope of the prohibition on considering employees' arrest and conviction records by holding the WFEA does not prohibit employers from terminating employees based on noncriminal, municipal citations.

In *Oconomowoc Area School District v. Cota*, 2024 WI App 8 (2024), the School District terminated two employees' employment based on its belief that they stole and sold the School District's scrap metal and kept the proceeds for themselves. The School District based its termination decision, in part, on the employees' municipal citations for theft and a municipal attorney's representations that he believed the employees were guilty of theft.

The plaintiffs challenged their terminations by filing a complaint with the Wisconsin Department of Workforce Development, Equal Rights Division alleging the School District's actions constituted unlawful arrest record discrimination under the WFEA. An agency administrative law judge, the Labor and Industry Review Commission, and the county circuit court all agreed with the employees and found the School District violated the WFEA because municipal citations fell within the WFEA's definition of "arrest record."

The Wisconsin Court of Appeals disagreed and reversed the prior decisions, finding that municipal citations are not an "arrest record" under the WFEA. The appellate court's analysis focused on the legislature's intention when it used the phrase "or other offense" in Wis. Stat. § 111.32(1). The court concluded that because the legislature used the phrase "any felony, misdemeanor or other offense," it intended only to protect criminal violations, not civil, noncriminal offenses such as municipal citations. Thus, because the *Cota* employees received only noncriminal, municipal citations, the appellate court said the WFEA did not prohibit the School District from terminating their employment based on those citations.

The *Cota* decision further defines the scope of arrest and conviction record protections under the WFEA. Employers, however, should be cautious in relying on it to make employment decisions. The Labor and Industry Review Commission has petitioned the Wisconsin Supreme Court for review, and *Cota* could be overturned, likely with immediate effect.

CLICK HERE.

Muldrow v. City of St. Louis: Supreme Court Establishes New Harm Standard for Title VII Discrimination Claims

The U.S. Supreme Court's recent opinion in *Muldrow v. City of St. Louis* lowered the bar for employees asserting workplace discrimination claims related to transfers or similar employment actions under Title VII. The *Muldrow* decision eliminates the longstanding requirement imposed by most federal courts that employees must show an employment action caused "substantial," "material," or "significant" harm in order to maintain a Title VII discrimination claim. Local government employers are therefore advised to act cautiously when transferring employees.

In *Muldrow v. City of St. Louis*, the Supreme Court considered whether a transfer of a police officer to a different position, allegedly based on sex, violated Title VII of the Civil Rights Act of 1964, even if the transfer did not "significantly" harm the employee. The court answered yes, finding that transferring an employee to a position with similar responsibilities and pay violates Title VII if the transfer is discriminatory and causes "some harm."

The Supreme Court's opinion explicitly states that the threshold for showing "some harm" is lower than the "substantial harm" or "material adversity" standard previously employed by federal courts, although it leaves some room for interpretation as to how much lower it is. Although this was a 9-0 decision, the majority opinion and concurring opinions revealed differing thoughts amongst the justices about how "some harm" will be interpreted by lower courts. Regardless, it is clear that more workplace actions will be brought within the scope of Title VII, and employers are well advised to carefully document and clearly articulate the reason for the transfer.

Background of Title VII and *Muldrow*

Title VII prohibits an employer from "discriminat[ing] against any individual with respect to h[er] compensation, terms, conditions, or privileges of employment, because of such individual's race, color, religion, sex, or national origin." Plaintiff employees who challenge some employment action are usually required to show, among other things, that the employee experienced an adverse employment action, and that the action was taken because of the employee's membership in a protected class. In cases where employees allege discrimination related to some action by their employer that changes their working conditions but that does not involve hiring, firing, or compensation, courts have scrutinized whether the challenged action was actually an "adverse" employment action or merely a neutral (or even positive) change in the employee's working conditions.

Muldrow involves Police Sergeant Lisa Muldrow being involuntarily transferred to a position in a different district that had different duties but the same pay and comparable seniority and opportunities for advancement. Sergeant Muldrow sued the City of St. Louis Police Department, claiming that her transfer was an adverse employment action taken because of her sex, violating Title VII. Sergeant Muldrow alleged that the new position carried less prestige and required her to work weekends and wear a uniform rather than plain clothes. The city argued that it did not violate Title VII because Sergeant Muldrow's new role was similar to her prior one and provided the same pay and benefits. The city argued that to violate Title VII, the transfer must cause "material objective harm" or a "significant disadvantage" and Sergeant Muldrow's grievances failed to meet these heightened standards. The district court and circuit court agreed with the city and granted the city summary judgment.

The Supreme Court disagreed, however, finding that there was no basis in the text of Title VII for requiring a heightened level of harm, and thus an employee challenging an allegedly discriminatory job transfer under Title VII need only show "some harm" with respect to an identifiable "term or condition" of employment. This holding would apply to a range of employment decisions, including transfers that result in a different work location, work schedule, or different perks.

Justice Elena Kagan, the author of the majority opinion, cited a few prior circuit court cases and described how the new lower standard would alter their outcome. For example, in *Cole v. Wake County Board of Education,* a school principal was transferred into a non-school-based administrative role supervising fewer employees. Although the Fourth Circuit in *Cole* did not find this transfer to result in a "significant disadvantage," Justice Kagan stated that the transfer would violate Title VII under the "some harm" standard.

In summary, transfers based on an individual's race, color, religion, sex, or national origin violate Title VII if the transfer causes "some harm" to employees regarding the terms and conditions of their employment. This standard is lower and, unlike the objective material harm standard, it is not limited to changes in pay, benefits, or responsibilities.

What the Decision Means for Local Government Entities and How to Avoid Risk

This decision creates a new legal risk for government entities to consider when making transfer decisions. Moving forward, employers will be in a better position if evidence exists explaining the reason or reasons for transfer decisions that are not based on protected characteristics.

CLICK HERE.

EEOC Weighs In On Novel Artificial Intelligence Suit Alleging Discriminatory Hiring Practices

***Duane Morris Takeaways*:** *In Mobley v. Workday, Inc., Case No. 23-CV-770 (N.D. Cal. April 9, 2024) (ECF No. 60), the Equal Employment Opportunity Commission ("EEOC") filed a Motion for Leave to File an Amicus Brief in Support of Plaintiff and in Opposition to Defendant's Motion to Dismiss. This development follows Workday's first successful Motion to Dismiss, about which we previously blogged here, after which the Court allowed Plaintiff a chance to amend his complaint.*

For employers utilizing Artificial Intelligence in their hiring practices, this notable case is worth monitoring. The EEOC's decision to insert itself in the dispute demonstrates the Commission's commitment to continued enforcement of anti-discrimination laws bearing on artificial intelligence use in employment.

Case Background

Plaintiff, an African American male over the age of forty alleged that he suffered from anxiety and depression and brought suit against Workday claiming that its applicant screening tools discriminated against applicants on the basis of race, age, and disability. Plaintiff further alleged that he applied for 80 to 100 jobs, but despite holding a bachelor's degree in finance and an associate's degree in network systems administration, he did not get a single job offer. *Id.*, 1-2 (ECF No. 45).

Workday moved to dismiss the Complaint in part arguing that Plaintiff did not allege facts to state a plausible claim that Workday was liable as an "employment agency" under the anti-discrimination statutes at issue.

On January 19, 2024, the Court granted the defendant's motion to dismiss, but with leave for Plaintiff to amend, on the ground that plaintiff failed to plead sufficient facts regarding Workday's supposed liability as an employer or "employment agency." Shortly thereafter, Plaintiff filed his Amended Complaint. *Id.* (N.D. Cal. Feb. 20, 2024) (ECF No. 47.)

On March 12, 2024, Workday filed its Motion to Dismiss Amended Complaint, asserting that Workday is not covered by the statutes at issue – Title VII, the Americans with Disabilities Act ("ADA"), and/or the Age Discrimination in Employment Act ("ADEA") – because Workday merely screens job seekers rather than procuring them. *Id.*, (ECF No. 50.) On April 2, 2024, Plaintiff filed his opposition (*id.*, ECF No. 59) and, on April 12, 2024, Workday filed its reply. *Id.*, (ECF No. 61.) The motion is fully briefed and set for hearing on May 7, 2024.

The EEOC's Motion for Leave to File an *Amicus Brief*

On April 9, 2024, before Workday filed its Reply, the EEOC filed a Motion for Leave to File an *Amicus Brief* in Support of Plaintiff and in Opposition to Defendant's Motion. *Id.*, (ECF Nos. 60 & 60-1.) The EEOC noticed its Motion for hearing on May 7, 2024. *Id.*, (ECF No. 60.)

The EEOC describes *Mobley* as a case that "implicate[s] whether," Title VII, the ADA, and the ADEA, "cover[s] entities that purportedly screen and refer applicants and make automated hiring decisions on behalf of employers using algorithmic tools." *Id.*, at 1 (ECF No. 60-1.) The Commission argues that Plaintiff's Amended Complaint satisfies federal pleading standards "with respect to all three theories of coverage alleged." *Id.*, at 4.

First, with respect to Workday as an employment agency, the EEOC notes that Title VII, the ADA, and the ADEA, all prohibit discrimination by employment agencies. Under each statute, the term "employment agency" includes "any person regularly undertaking with or without compensation to procure employees for an employer." *Id.* The EEOC maintains courts generally construe "employment agency" based on "'those engaged to a significant degree' in such procurement activities 'as their profession or business,'" and the focus on the degree to which an entity engages in "activities of an employment agency." *Id.*

The EEOC argues, among these activities, screening and referral activities are classically associated with employment agencies. *Id.*, at 5. The Commission asserts that "[Plaintiff] has plausibly alleged that Workday's algorithmic tools perform precisely the same screening and referral functions as traditional employment agencies—albeit by more sophisticated means." *Id.*, at 6. In contrasting Workday's position, the EEOC urged the Court to find Workday's arguments that "screening employees is not equivalent to procuring employees," and that Workday does not "actively recruit or solicit applications" as unpersuasive. *Id.*, at 7.

Second, the EEOC argues leading precedent weighs in favor of Plaintiff's allegations that Workday is an indirect employer. Taking Plaintiff's allegations as true, the EEOC contends that "Workday exercised sufficient control over [Plaintiff's] and others applicants' access to employment opportunities to qualify as an indirect employer," and "Workday purportedly acts as a gatekeeper between applicants and prospective employers." *Id.*, at 11.

The EEOC argues Workday's position on sufficient control misses the point. Workday's assertion that it "does not exert 'control over its customers,' who 'are not required to use Workday tools and are free to stop using them at any time," is not the inquiry. *Id.*, at 12. Rather, the relevant inquiry is "whether the defendant can control or interfere with the plaintiff's *access* to that employer," and the EEOC notes that the nature of that control or interference "will always be a product of each specific factual situation." *Id.*

Finally, the EEOC maintains that Plaintiff plausibly alleged Workday is an agent of employers. The EEOC also maintains that under the relevant statutes the term "employer" includes "any agent of" an employer and several circuits have reasoned that an employer's agent may be held independently liable for discrimination under some circumstances. *Id.*

In analyzing Plaintiff's allegations, the EEOC argues that Plaintiff satisfies this requirement, where Plaintiff "alleges facts suggesting that employers delegate control of significant aspects of the hiring process to Workday." *Id.*, at 13. Accordingly, the EEOC concludes that Plaintiff's allegations are sufficient and demonstrate "Workday's employer-clients rely on the results of its algorithmic screening tools to make at least some initial decisions to reject candidates." *Id.*, at 14.

On April 15, 2024, the Court ordered any opposition or statement of non-opposition to the EEOC's motion for leave shall be filed by April 23, 2024. *Id.* (ECF No. 62.)

Implications For Employers

With the EEOC's filing and sudden involvement, Employers should put great weight on EEOC enforcement efforts in emerging technologies, such as AI. The EEOC's stance in *Mobley* shows that this case is one of first impression and may create precedent for pleading in AI-screening tool discrimination cases regarding the reach of "employment decisions," by an entity – whether directly, indirectly, or by delegation through an agent.

The *Mobley* decision is still pending, but all Employers harnessing artificial intelligence for "employment decisions" must follow this case closely. As algorithm-based applicant screening tools become more common place –the anticipated flood of employment discrimination lawsuits is apt to follow.

CLICK HERE.

INTERNATIONAL DEVELOPMENTS

Social media screening for job applicants: Human rights and privacy risks Alberta employers should be aware of

In the digital age, the recruitment landscape has expanded beyond traditional methods, with social media becoming a significant tool for evaluating potential candidates and completing background checks. However, the practice of "creeping" on candidates' social media profiles during the hiring process raises important legal considerations for employers.

Research from a recent study of Canadian employers indicated that 65% of companies surveyed use social media screening during the hiring process, and 41% of those companies had rejected applicants because of what they had found.[1] Despite the prominence of this practice, there are potential human rights and privacy pitfalls that an employer must be careful to avoid when screening a job applicant's personal social media accounts.

HUMAN RIGHTS CONSIDERATIONS

The *Alberta Human Rights Act* ("AHRA") provides legal recourse to job applicants if they are rejected based on a "protected characteristic." The protected characteristics are listed under paragraph 7(1)(b) of the AHRA and include race, religious beliefs, colour, gender, gender identity, gender expression, physical disability, mental disability, age, ancestry, place of origin, marital status, source of income, family status or sexual orientation.

In order for an unsuccessful job applicant to be granted a legal remedy pursuant to the AHRA, they must establish a *prima facie* case of discrimination. Generally the unsuccessful applicant must show that they have a protected characteristic, that they suffered a disadvantage or adverse impact, and that the protected characteristic was a factor that contributed to the disadvantage or adverse impact.[2] The onus then shifts to the employer to demonstrate that the applicant's protected characteristic was not a factor in the decision. An effective defence often involves demonstrating that the employer was unaware of the applicant's protected characteristic and therefore the protected characteristic could not have been a factor in the decision. As a result, employers are advised to avoid questions related to protected characteristics during job interviews and reference checks.

However, advancing a defence that an employer was unaware of an applicant's protected characteristic will be particularly challenging if the employer has screened an applicant's social media which has evidence of their protected characteristic(s). Social media can contain a plethora of information about an individual that crosses into the realm of protected characteristics, examples could be pregnancy announcements, posts about injuries or disabilities, affiliations with ethnic or cultural organizations, etc.

While the employer may have set out with good intentions, it is difficult to predict what one may find when conducting these searches. The inability to predict, control or limit what information is obtained by these searches presents risks that employers should consider before conducting such checks. Once collected, information can be difficult to disregard. The employer may stumble upon information it did not set out to find, and that information could factor into hiring decisions, either deliberately or through unconscious bias, in violation of the AHRA.

PRIVACY LAW CONSIDERATIONS

In addition to the human rights risks, private sector employers in Alberta must navigate the *Personal Information Protection Act* ("PIPA"). PIPA governs the collection, use, and disclosure of personal information and personal employee information. "Personal Information" is broadly defined as all information about an identifiable individual. Whereas "Personal Employee Information" is more narrowly construed and is defined as information reasonably required by an organization for the purposes of establishing, managing or terminating an employment relationship. Notably, the definition of "Personal Employee Information" expressly excludes information about the individual that is unrelated to the employment relationship.

PIPA permits employers to collect, use and disclose Personal Employee Information about prospective employees without consent for reasonable purposes related to recruitment.[3] However, before engaging in social media screening of the personal social media accounts of applicants, employers should ascertain their business purpose for undertaking such checks

and evaluate the appropriateness of doing so. Employers must demonstrate the reasonableness of utilizing social media for the collection of Personal Employee Information and must consider whether such a check will result in collection of information that is unrelated to the prospective employment relationship. It is imperative for employers to assess what unique insights a social media screening can offer that cannot be obtained through conventional methods like reference checks and interviews.

Employers should be cautious about inadvertently collecting information about third parties during social media screens, which may not be permitted under PIPA. PIPA also requires employers to take steps to ensure that the information they collect and use is accurate. Social media accounts may contain inaccurate or out-dated information about job applicants, and employers should therefore be cautious about collecting or relying on that information.

Depending on the nature of the information collected, if the information is publically available, and whether or not the job applicant is an external applicant or current employee, the employer may need to provide notice to the job applicant, or obtain their consent, before conducting a social media screen.

For more information, employers are encouraged to review the Guidelines for Social Media Background Checks developed by the Office of the Information and Privacy Commissioner of Alberta.

BEST PRACTICES

While social media background checks may appear enticing, there are legal risks associated with screening a job applicant's personal social media accounts. While this practice may provide insights into a candidate's character and qualifications, employers in Alberta must proceed cautiously. Respecting candidates' privacy rights, focusing on job-related information, avoiding discriminatory practices, and ensuring the accuracy of information gathered are paramount. The first and safest option may be to refrain from conducting social media screening of job applicants full-stop. Using this strategy, an employer protects themselves from unintentionally discovering that a job applicant possesses a protected characteristic, or violating privacy laws by collecting irrelevant, inaccurate or too much information. In particular, employers should consider the following questions before proceeding:

- Is the social media screen reasonable?
- Will the social media screen collect information that is related to protected characteristics, overly broad, or unrelated to the hiring process?
- Will the social media screen collect personal information about third parties?
- Is the information collected accurate?
- Is notice or consent required before conducting the social media screen?

Employers should establish a well-documented hiring process with transparent hiring criteria, educate hiring personnel on ethical and legal considerations, and seek legal guidance to mitigate risks associated with social media screening.

CLICK HERE.

EU Pay Transparency Directive

In just a few weeks, the EU Pay Transparency Directive (EntgTranspRL) will celebrate its first birthday. EU Member States have to implement it into national law by June 2026. It's not yet clear when this will take place in Germany.

A draft bill has been announced for the end of the second quarter of this year. But it's risky for employers to wait for the final legislation: the EntgTranspRL contains fundamental changes to the current German Pay Transparency Act (EntgTranspG), which employers should familiarise themselves with at an early stage.

Pay transparency before and during employment

The EntgTranspRL strengthens pay transparency even before the start of employment. In the future, employers will have to provide applicants with information on entry-level pay and its objective, gender-neutral criteria (eg in a job advertisement, before the interview or by other means). Employers can no longer ask about previous pay or make enquiries in this regard. In the current employment relationship, employers have to ensure their employees have easy access to the criteria for

determining pay, pay levels and pay trends. These criteria must be objective and gender-neutral. The directive does not regulate the form in which and the intervals at which the information must be provided. Member States can exempt employers with fewer than 50 employees from this obligation. It's currently not clear whether this will happen in Germany.

Individual right to information

In addition, employees have a right to information about their individual pay levels and – differentiated by gender – about the average pay levels for groups of employees who perform the same or equivalent work.

This entitlement is much more effective than the existing one for several reasons. Firstly, it's independent of the number of employees of the employer and the size of the comparison group. Secondly, it's based on the average pay level and not on the statistical median. Thirdly, all comparable employees have to be taken into account when calculating the average pay levels – not just those from the same company and the same region. Finally, employers must inform employees annually about their right to information.

Pay structures

In future, companies of all sizes will have to have pay structures that guarantee equal pay for equal work or work of equal value. The pay structures must be such that objective, gender-neutral criteria agreed with employee representatives can be used to assess whether employees are in a comparable position in terms of the value of their work. These criteria must not be directly or indirectly related to the gender of the employees. A reference to remuneration in accordance with a collective agreement will not be sufficient because – unlike the EntgTranspG – the EntgTranspRL does not contain a presumption of appropriateness for collective agreements. The key point of pay transparency is a gender-neutral job evaluation. In the opinion of numerous experts, this can only be achieved through analytical job evaluation methods, which will not have played a major role in collective agreements when assessing whether work of equal value exists – at least so far.

Reporting obligations and joint pay assessment

Employers with 100 or more employees will have to report regularly in the future, including on the pay gap between women and men. Alternatively, Member States can impose the reporting obligation on themselves. The timing and frequency of reporting will be regulated differently depending on the number of employees.

If the report reveals a pay gap of at least 5% between men and women that cannot be objectively justified or is not closed within six months of the report being submitted, the employer must carry out a joint pay assessment with the employee representatives. The aim of the joint pay review is to eliminate the unjustified pay differences within a reasonable period of time. If there's no employee representative body, one must be appointed as soon as a joint pay assessment becomes necessary. It should exist until the gap has been eliminated. The directive does not regulate the exact procedure and what the consequences are if, for example, no corresponding employee representative body is found.

Effectiveness of the directive

The EntgTranspRL also provides for a shift in the burden of proof in the event of a breach of transparency obligations and a limitation period of at least three years. Finally, Member States must create effective sanctions (eg fines based on gross annual turnover).

Practical advice

Employers should use the time until the implementation of the EntgTranspRL to review their approach to job advertisements and application procedures. Now is the time to review remuneration systems thoroughly for gender neutrality and make improvements where necessary. Employers can stand out on the job market through transparency and openness.

CLICK HERE.

MISCELLANEOUS DEVELOPMENTS

U.S. Bans Non-Competes Nationwide Except in M&A - A Corporate Perspective

On 23 April 2024, the United States Federal Trade Commission (FTC) issued a final rule, which effectively bans non-competition agreements for workers in all circumstances except in M&A (the "Rules").

Particulars of the Rule

The Rules represent a watershed moment in the evolution of non-competition agreements in the United States. Prior to their enactment, non-competition agreements for workers were lawful to varying degrees in all states except California. However, even in California, there was an exception permitting non-competition agreements in the context of M&A. This exception continues to apply as it is expressly stated in the Rules.

Going forward, non-competition agreements will not be allowed on a nationwide basis for all works, including senior executives. The existing non-competition agreements for workers who are not senior executives will also be invalid under the Rules on a going forward basis. Furthermore, employers are required to notify them of this fact within 120 days, with the FTC providing model language in the Rules to assist with the process. The existing non-competition agreements for workers who are senior executives remain valid.

The term "worker" includes employees and independent contractors (e.g. advisors). The term "senior executive" means a worker who was in a "policy-making position" whose compensation was US$151,164 or greater in the preceding year. The term "policy-making position" means someone who was in a position of final authority to make business decisions for a common enterprise.[1]

Potential Consequences from a Corporate Perspective

The exception in the Rules for M&A is highly consequential for corporate practitioners. Specifically, the Rules do not apply to "a non-compete clause that is entered into by a person pursuant to a bona fide sale of a business entity, of the person's ownership interest in a business entity, or of all or substantially all of a business entity's operating assets". Accordingly, as the Rules do not apply to M&A, existing state law on non-competition agreements in M&A will continue to apply. As stated above, non-competition agreements in the context of M&A is a common exception to restrictions against non-competition agreements, including in California where they have always been prohibited as a general rule.

The FTC noted that there are less obstructive ways to ensure an employer's protection of trade secrets following departures, including confidentiality and trade secrets undertakings. In practice, employers ranging from start-ups to established multinational companies may more actively monitor post-employment compliance of confidentiality and trade secrets undertakings. There may be unsettled questions arising from the use of claw-backs or deferred compensation arrangements to ensure compliance, which will have to be settled in the courts.

In the venture capital space, the Rules may facilitate the formation of more start-ups, as the Rules ease the burden that may have applied to founders and key employees who may be subject to the non-competition agreements of their former employer.

CLICK HERE.

Utah's New AI Disclosure Requirements Effective May 1

The Utah legislature has been busy, with another law effective May 1. This one is "privacy adjacent" but worth keeping in mind. The law, the Artificial Intelligence Policy Act, was signed into law in March. Among other things, it will require companies to respond "clearly and conspicuously" to an individual who asks if they are interacting with artificial intelligence and the communications are made in connection with laws regulated by the Utah department of commerce. (This includes the Utah Privacy Act, the state's sales practices law, its telephone solicitation laws, and many others.)

Artificial intelligence is defined in the law as an artificial system that is trained on data, that interacts with someone through text, audio or visual means, and creates output that is "similar" to a human, without human oversight. The law's disclosure requirement is a reactive one. The disclosure needs to happen only if "asked or prompted" by the individual.

There is one caveat to this reactive provision. Businesses who are in "regulated" occupations must make a prominent disclosure that they are using AI in the provision of those services. Regulated occupations include any licensed by the Utah Division of Professional Licensing. This includes many health care professions, as well as court reporting, athletic trainers, plumbers, electricians, and more.

The reactive nature of the law is unlike a California "chatbot" law. That law prohibits misleading people into thinking they are "interacting online" with a human if in fact they are interacting with an "artificial identity." The law provides an affirmative defense to have a clear and conspicuous disclosure that the tool is a bot. A bot is defined as an online account where actions are not those of a person (so encompassing more than generative AI, but also automated replies). In other words, the law requires disclosing the nature of the "artificial identity" prior to someone interacting with it. It is narrower than the Utah law, however, as it relates only to when someone is interacting with the bot to "incentivize" a sale (or to get someone to vote).

Putting It Into Practice: Companies who may be subject to this law (apart from any who provide services in "regulated occupations") may want to test any GenAI tools they are using to interface with the public. How do those tools respond if someone asks "are you AI," "is this a bot," "are you human" and the like? For those who are in regulated occupations, remember that the disclosure obligations are affirmative to the extent that the law applies.

CLICK HERE.