

# One Minute Memo<sup>®</sup>



## Proposed CORI Regulations Impose a Host of New Requirements on Employers Conducting Criminal Background Checks in Massachusetts

### Register Now For Seyfarth's Breakfast Briefing on April 4, 2012: Navigating the New Massachusetts Criminal Record Law

On May 4, 2012, major changes are coming that will require all Massachusetts employers conducting criminal background checks to reassess their practices. As we [reported previously](#), the Massachusetts Legislature overhauled the Criminal Offender Record Information ("CORI") statute in 2010, imposing a host of new requirements for users and providers of criminal history to be phased in over time. A few days ago, the Department of Criminal Justice Information Services ("DCJIS") issued 84 pages of Proposed Regulations implementing the last of the new requirements and announced a public hearing on the draft regulations scheduled for March 30, 2012. A few of the most important points in these new regulations are noted below. Seyfarth Shaw also invites you to [join us](#) at 8:00 a.m. on April 4, 2012, for a Breakfast Briefing, where our experts will provide an overview of the requirements which go into effect on May 4, 2012, an analysis of the proposed regulations, and an update on the DCJIS's public hearing. Seyfarth Shaw will also host a webinar on the topic on April 11, 2012 at 1:00 p.m.

### Proposed Regulations: Key Points For Employers

#### ***Notification To Applicant Prior to Potential Adverse Decision***

Employers who intend to take adverse action based on criminal history information must notify the applicant, provide the applicant with several specific pieces of information, afford the applicant an opportunity to dispute the accuracy of the criminal history at issue, and document all steps taken to comply with these requirements. Unlike with the federal Fair Credit Reporting Act, the new CORI requirement exists regardless of whether a third party is used to obtain criminal history information.

#### ***Using a Consumer Reporting Agency ("CRA") to Make Employment Decisions***

Employers using CRAs to collect criminal history information on employees or applicants are required to make certifications to the CRA regarding the employer's CORI compliance measures, in addition to providing disclosures to the individuals being screened both before the employer requests a criminal history report from the CRA and before taking any adverse action based on information that the CRA provides.

The regulations also provide a separate set of requirements that apply when an employer outsources the decision-making process regarding an employee's eligibility for hire to the CRA, rather than merely requesting criminal history information from the CRA.

### ***Obtaining CORI from DCJIS***

Employers who obtain criminal record information from DCJIS must submit acknowledgement forms for each applicant, verify the identity of the applicant by examining a government-issued identification, and certify that the applicant was properly identified. These acknowledgement forms must be maintained by the employer for one year from the date the applicant signs the form.

### ***Training Required***

Before requesting CORI, employers or CRAs must register for an account on the Commonwealth's new iCORI system, complete training, and adhere to annual renewal and re-training requirements.

### ***CORI Policy Requirement***

Employers who submit five or more CORI requests annually must maintain a CORI policy and provide it to applicants if the employer takes adverse employment action based on the applicant's CORI. These requirements apply whether the employer (or a CRA on the employer's behalf), obtains criminal history information from DCJIS or another source.

### ***Strict Recordkeeping Requirements***

Employers must store all hard copies of CORI in a separate, locked and secure location and limit access to the location to employees whom the employer has approved to access CORI. Electronic CORI records must be password-protected and encrypted and may not be stored using public cloud storage methods.

Employers are prohibited from retaining CORI for longer than seven years and are required to implement effective means of destroying or deleting such information, including scrubbing computer hard drives and deleting CORI from any back-up computer system.

If an employer disseminates CORI outside of its organization, the employer must keep a detailed dissemination log, which must be maintained for at least one year.

### ***Audits by DCJIS***

Employers who request CORI from DCJIS are subject to audit. During an audit, DCJIS staff can inspect CORI-related documents, including documentation of adverse employment decisions based on CORI. DCJIS may initiate a complaint with the Criminal Records Review Board (CRRB) against an employer for failure to participate in an audit or in the event that DCJIS determines the employer is not in compliance with the CORI law.

### ***Penalties for Violations of the CORI Law***

The CRRB has the authority to impose civil fines of up to \$5,000 for each knowing violation of the CORI law. Certain violations may also subject an employer to criminal prosecution.

## **Strategy & Insights for Compliance with the Massachusetts CORI Reform Act**

In addition to our upcoming Breakfast Briefing and webinar, Seyfarth Shaw will soon publish a Strategy & Insights piece providing a comprehensive analysis of the new CORI requirements and the steps that employers can take to avoid liability under the revised statute.