Sterling Backcheck

How Might the RCMP (CPIC) Policy on the Release of Criminal Records Affect Your Screening Program?

Sterling Backcheck

Introduction

In a recent letter to the heads of Canadian police agencies, the Canadian Police Information Centre (CPIC) raised concerns regarding inconsistent and non-compliant background screening practices performed by police agencies and third-party providers with which those agencies have agreements.

Guidelines regarding the use and disclosure of criminal record information were originally set out in 2010 in the form of a Ministerial Directive (MD) issued by the Minister of Public Safety. In concert with the MD, the Canadian Criminal Real Time Identifications Services (CCRTIS) of the RCMP issued the Dissemination of Criminal Record Information Policy, which prescribes the framework within which third-party companies and their police partner agencies must operate when providing name-based criminal record and police information checks.

In recent years, inconsistent practices resulting in policy violations and compliance issues have been observed in the background screening industry, leading CPIC to initiate a review of its policies and guidelines.

In this document, we will discuss the common pitfalls that have caused this review and explore what it could mean for your organization's background screening program.

Legal Framework of Criminal Record Screening by Third Parties

In Canada, background screening processes and procedures are defined at the federal level by the RCMP, based on various federal statutes,[1] and at the provincial or territorial level by various freedom of information and privacy laws. These laws and policies inform the framework within which the industry operates.

Published in 2010, the Ministerial Directive Concerning the Release of Criminal Record Information by the Royal Canadian Mounted Police outlines the conditions under which police services can release criminal records, fingerprints, photographs, and related information maintained in the RCMP National Repository of Criminal Records. Specifically, it is the MD and associated RCMP (CCRTIS) policy which are currently under review by CPIC.

Common Compliance Pitfalls

1. Inconsistent Standards and Practices

To provide background screening services, companies in the private sector must enter into an agreement with a Canadian police agency (also known as a Category I CPIC Agency), which is accountable to the CPI Centre in respect of its use of the CPIC system. Over time, CPIC has observed a lack of oversight and accountability for background screening companies by their police partners.

To mitigate the risk of fraudulent or other harmful practices and to enforce compliance, police agencies are required to screen and audit their background screening partners, both prior to entering agreements and on an ongoing basis. It is evident that inconsistent standards and practices have been applied across different police jurisdictions, leading to CPIC system integrity concerns. In addition, staff at screening agencies may not be screened adequately, which is concerning considering the amount of personal information that is gathered on applicants during the criminal record screening process.

2. Misuse of Official RCMP Trademarks

Another common issue involves the inappropriate use of RCMP official trademarks. In some cases, trademarks are being used to advertise locally-sourced criminal record screening products, giving the incorrect impression that the RCMP is involved in the search. They may also be included in the company's marketing materials or private website. This implies that they are endorsed by the RCMP when this is not the case. A favorite ploy is to claim to be RCMP-accredited. The RCMP does not accredit background screening companies – only private fingerprinting companies. It has no program for that. Instead, it provides policy on accreditation for police partner agencies to apply to their agreements with third party companies.

3. Identity Verification and Language for Consent

Identity verification and consent verbiage are two other areas that often fail to meet the standards prescribed in CCRTIS policy.

With respect to consent language and the language contained in response results, the RCMP prescribes both. Companies are required to provide their sample wordings when entering into agreements with police services. Consumers should be aware of these requirements and ensure that their provider — current or prospective — is using consent and response language that meets federal standards.

Regarding identity verification, the CCRTIS policy defines acceptable processes. Since name-based criminal record screening comes with a risk of identity fraud, the RCMP requires applicants to verify their identity before the check can begin, using various in-person and online identity verification options available. Completing this requirement in a hasty manner (or ignoring it entirely) can create high-risk scenarios: for example, allowing an applicant with a relevant criminal record to avoid detection and to obtain a "Clear" background check result.

[1]Specifically, the Canadian Human Rights Act, the Criminal Records Act, the Youth Criminal Justice Act, the Identification of Criminals Act, the Privacy Act, and the Police Record Checks Reform Act (Ontario).

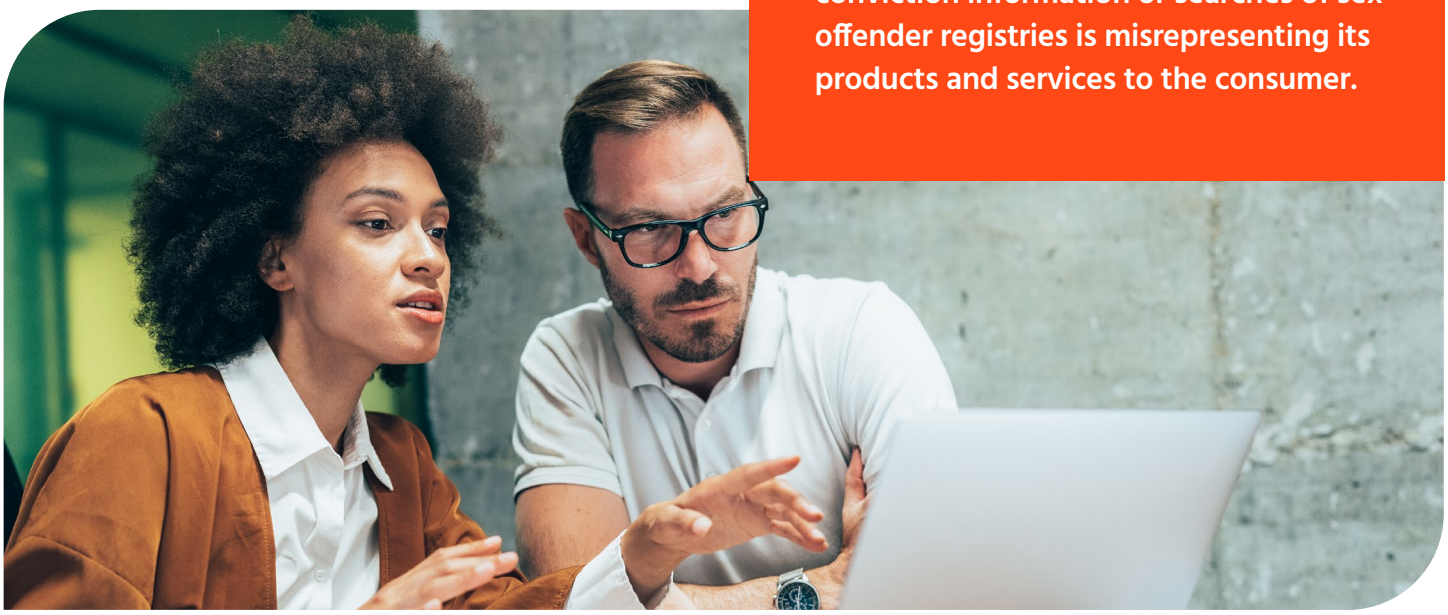
Consumers should acquaint themselves with ID verification standards. Take a good look "behind the curtain" to ensure that this crucial step is being completed in a robust and compliant manner that meets or exceeds RCMP policy. Note also that it is the responsibility of the police partner agency working with the company to examine the company's ID verification processes to confirm they are compliant. Consumers should ask their current or prospective provider these questions:

- How are applicants' identities verified? (Examples: in-person, using Knowledge Based Authentication (KBA), AI/Machine Learning, facial recognition technology, over video chat, leveraging other ID processes)
- Have their process(es) been authorized/approved by the police partner agency/agencies?
- Do their processes meet/exceed the standards defined in RCMP (CCRTIS) policy?

4. Restricted Area of Disclosure

Misrepresentation of the services provided is another issue among some private sector providers. For instance, unlike the US, Canada has no public-facing sex offender registries. In addition, youth convictions are annotated to distinguish them from adult convictions and cannot be reported as part of a criminal record check[2]. Unfortunately, this has not prevented some providers and even police jurisdictions from providing criminal screening services that include this information, a practice that Ontario's Police Records Check Reform Act set out to address in 2018.

Any company claiming to provide youth conviction information or searches of sex offender registries is misrepresenting its products and services to the consumer.



[2]The sole narrow exception is disclosure associated to a position in government. Even then, the Youth Criminal Justice Act applies time limits to periods of disclosure that are based on the sentence received for the conviction.

5. Non-Compliant Vulnerable Sector Verifications

The CPI Centre has identified the conduct of Vulnerable Sector Checks (VSC) outside of local police jurisdiction as cause for concern. The VSC — or Vulnerable Sector Verification (VSV) as it is described in the MD — is a search for specific sexual offences subject to a record suspension (formerly known as a pardon). It is designed for people who volunteer or work in a position of trust or authority with children or other vulnerable persons. According to the Ministerial Directive, the issuance of VSV results may only be provided by the police jurisdiction where the applicant resides; however, there are many examples where these checks have been (and are being) conducted by other police services.

Sterling Backcheck possesses deep expertise regarding Vulnerable Sector Verifications. We see opportunity for improvement in this area with respect to the current policy framework. While we continue to advocate for change, we also work to ensure our clients understand this topic and how the VSV may apply to their circumstances. We provide proven and trusted advice that both defines industry limitations while illuminating opportunities organizations can pursue when navigating this complex and often misunderstood subject.

Sterling Backcheck has always prioritized compliance. As an active member of the Professional Background Screening Association, Sterling provides industry thought leadership, guidance and best practices.

What Does This Mean for Your Organization?

The upcoming CPIC policy review is intended to address long-standing concerns over reported non-compliance within the background screening industry. Many non-compliant practices observed in the private sector are the result of cost-cutting measures intended to entice consumers to obtain criminal record checks at a lower price. Less reliable companies are willing to cut costs, even if doing so could endanger applicants' personal information and put their clients at risk. Simply put, compliance costs more.

Sterling Backcheck has always prioritized compliance, even when it may not be more expedient or cheaper to do so. For instance, when a criminal record check cannot be completed due to a close match in the RCMP criminal records database or a pending charge that may be awaiting a disposition, we refer applicants to their local police or to an accredited fingerprinting company to obtain the RCMP-certified criminal record product (only possible through submission of fingerprints). We also insist on observing the strict RCMP requirements for identity verification, even when it could delay the screening process.

According to the CPI Centre, there are companies that are not sufficiently engaged in managing their relationships with their police partners. Time and time again, we have observed instances of private providers cutting corners. The CPI Centre's policy review intends to place greater accountability on police agencies for ensuring that the companies they have agreements with are compliant. To understand the potential impact, it is worth noting that the RCMP currently uses identifiers, called Originator Identity Number or ORIs, to track and audit individual police agencies' use of CPIC when they provide services to companies. These identifiers work similarly to internet service provider numbers, allowing the RCMP to require that these channels be the only ones used for the purpose. In concert, the dedicated channels ensure an audit trail that the CPI Centre reviews to identify non-compliant practices which could result in non-compliant agencies and companies losing the right to access CPIC.

The Sterling Backcheck Difference

Proactive engagement can also entail direct participation in the industry. In this regard, Sterling Backcheck is always out in front of policy and compliance issues. Far from passive, we have proactively raised compliance questions and concerns with our police partners and educated them about potential pitfalls when they arise.

When the CPI Centre announced that police partners would be required to evaluate and approve identity verification methods used by their partner companies, we took steps to educate our partners and the CPI Centre on our processes. Since then, we have joined the Digital Identity and Authentication Council of Canada (DIAAC) as a sustaining member, continuing to move ahead with superior identity proofing solutions that meet or exceed RCMP policy.

We also make a continuous effort to remain aligned with emerging legislation, like the Police Record Checks Reform Act of Ontario and Quebec's new language law, Bill 96. Our Senior Advisor in Public Safety Information Management, Chuck Walker, was previously Director General of CPIC and the CCRTIS (Canadian Criminal Real Time Identification Services), an experience from which he drew to draft Sterling's standard operating procedures for processing criminal records checks, in collaboration with our Police Partner Agencies. These proprietary procedures are aligned with relevant policy and legislation and provide for consistent processes across our police partner agencies. As a result, we do not foresee that our clients will be affected by CPIC's upcoming policy review. We will keep a close eye on the situation and update our clients as more information is made available.

DIACC

Sterling Backcheck has joined the Digital Identification and Authentication Council of Canada, a non-profit coalition of public and private sector leaders committed to developing a Canadian framework for digital identification and authentication.

During the search for a screening provider, it may be tempting for companies to look for the lowest price, but compliance should always remain top-of-mind. Companies putting upfront costs above all other considerations may find themselves paying for that mistake as costly non-compliance issues arise.

Sterling Backcheck has always prioritized compliance over expediency. Contact our experts to learn how our criminal record screening process can help you stay on top of compliance requirements.

Chuck Walker
Senior Advisor — Public Safety Information Management

Prior to joining Sterling Backcheck in 2014, Chuck was the Director General of the CCRTIS (Canadian Criminal Real Time identification Services) and the Director General of the CPIC (Canadian Police Information Centre). As a former chief custodian of the National Repository of Criminal Records maintained by the RCMP, Chuck has deep expertise regarding the criminal record screening industry in Canada, and advocates for a strong partnership between private screening providers and police agencies to best serve clients' and applicants' interests. Chuck oversees Sterling Backcheck's police partner agency relationships, including our standard operating procedures, which are central to the criminal record and police information check processes.

Sterling
Backcheck

About Us

Sterling (NASDAQ: STER) is a leading global provider of background and identity services, offering background and identity verification services to help our clients create people-first cultures built on a foundation of trust and safety. With operations around the world, Sterling's tech-enabled services help organizations across all industries establish great environments for their workers, partners, and customers.

Want More?

Sterling regularly publishes cutting-edge research and insight on the latest trends in human resources, talent acquisition and management, and hire processing.

For more information, visit us at: sterlingbackcheck.ca.