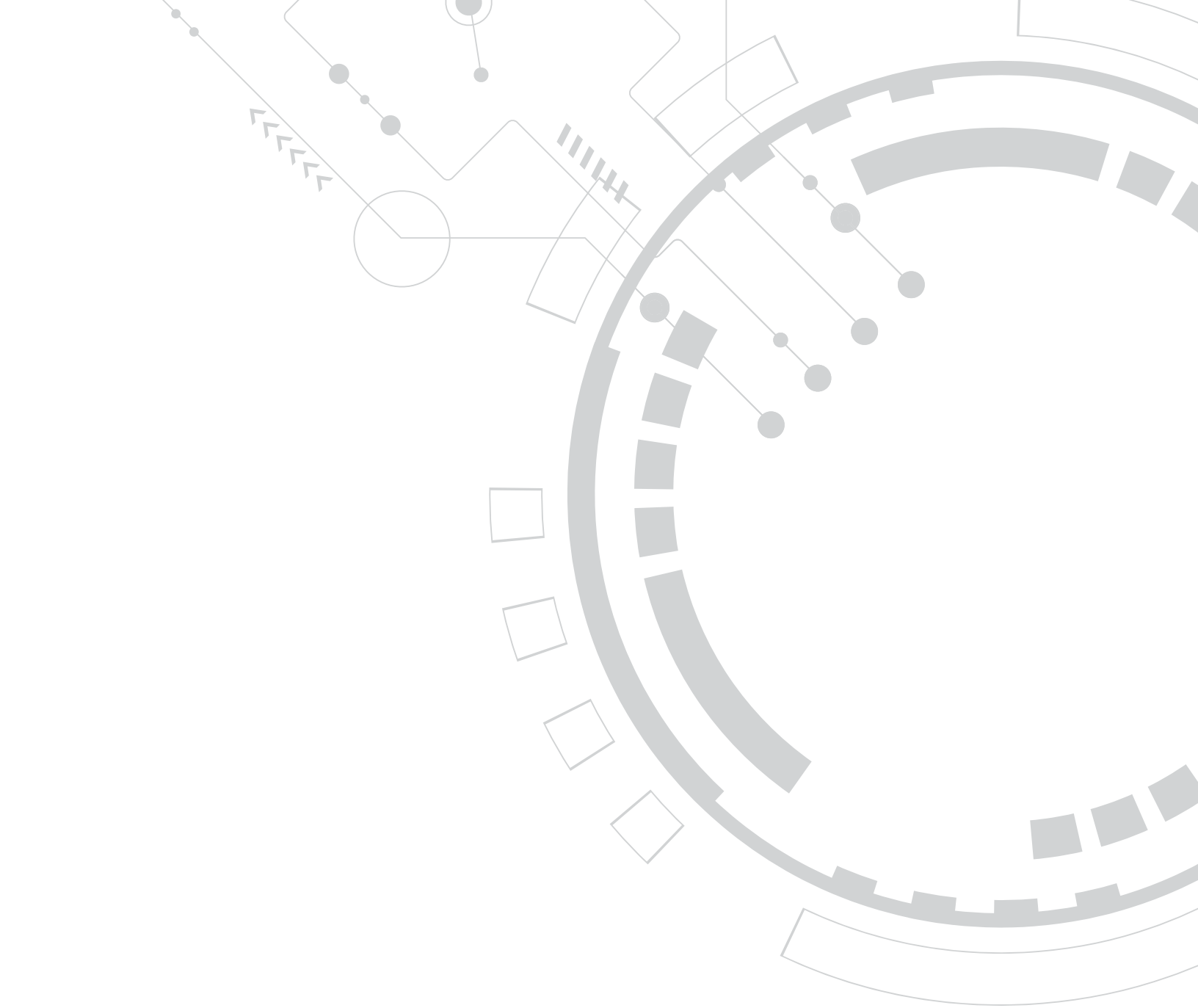




Credential Management for the Future of Work

How to protect the public and mitigate risk with
learner and credential verification



Table of Contents

01	Introduction	03
02	Context	04
03	Risk	05
04	Solutions	07
05	Learner Verification	07
06	Credential Verification	08
07	Recommendations	09



INTRODUCTION



We're heading into perhaps the biggest skills gap Canada has seen for the skilled trades, as we see a mass exodus of older generations from the workforce without enough trained workers to fill the gap.

DAN GIURESCU

Over the past decade, online learning has reached near-ubiquity for workplace training, re-certification, and job up-skilling. Beginning in 2020, the COVID-19 pandemic pushed its popularity to new heights: enrollment numbers more than doubled in 2020 and increased by 32 per cent the following year, peaking at 189 million.¹ In 2020 alone, there was a four-fold increase in the number of individuals seeking out online learning on their own, a five-fold increase in employer-provided online learning opportunities, and a nine-fold enrollment increase for learners accessing online learning through government programs.²

Far from being a tech-forward luxury, online learning has entrenched itself as a mainstream – and often, preferred – modality for workplace training. Access to high quality online learning, especially for high-stakes training in regulated industries, has been a true game-changer that's provided new skills and opportunities for employees and organizations alike. But its convenience has come with new challenges: primarily, the potential for learner and credential fraud.

In an ADP analysis of 2.6 million self-submitted background checks, it was found that:

- **23% of individuals had falsified credentials or licence details,**
- **41% of individuals had lied on their resumes about their education, and**
- **44% of individuals had lied about their work history on their resume.**³

Credential fraud is on the rise as online training creates new challenges in verifying leader identities, software and scammers create a burgeoning market for false credentials, and a high-turnover employment market drives some to fabricate their details in the hope of securing a newer, better job.⁴

The “great resignation” in the wake of the pandemic, along with emerging skills gaps and difficulty finding the right talent, could lead to even bigger issues for employers in regulated industries.

“We're heading into perhaps the biggest skills gap Canada has seen for the skilled trades, as we see a mass exodus of older generations from the workforce without enough trained workers to fill the gap,” said Dan Giurescu, the co-founder and CEO of Credivera, a credential verification provider. “At the same time, we're investing heavily in infrastructure. How do we not only get enough trained workers, but also ensure they have the right credentials for this safety-sensitive work?”

That's where good credential management comes in.

Credential management can mitigate the risks of fraud, and meet the demands of verifying credentials in an increasingly digital world. Technology tools like LearnerVerified, digital wallets, and the Credivera exchange can protect the public from the risks of credential fraud. Here's how.

¹ <https://www.weforum.org/agenda/2022/01/online-learning-courses-reskill-skills-gap>

² <https://www.weforum.org/reports/the-future-of-jobs-report-2020/digest>

³ <https://www.accredible.com/blog/the-future-of-credentialing>

⁴ <https://www.citizen.digital/business/employers-to-carry-out-background-checks-as-fake-degree-cases-rise-154453/>

23%

of individuals had falsified credentials or licence details

41%

of individuals had lied on their resumes about their education

44%

of individuals had lied about their work history on their resume

CONTEXT

It's intuitive that the digitization of our work and learning lives has opened up a new realm of opportunity for fraudsters and cheaters. With online learning, it's now possible to have someone else take your course or exam for you. With tools like photoshop, it's simple to create a fraudulent credential. There are even full-fledged "diploma mills" and other profitable fraud operations that sell fake credentials for a few hundred dollars.⁵

Common Fraud Tactics

- Having someone else take the course and/or exam
- Using image software to alter or create false credentials
- Buying fraudulent credentials from a third party
- Making false statements on a resume, LinkedIn profile, or in an interview
- Using "cheat sheets" while taking an online test or exam⁶

This digital dishonesty can range from embellishing details on a resume to buying a fraudulent safety license in order to get a job. The statistics vary, but one well-cited ADP study found that over 40 per cent of people have "adjusted" their resumes in the pre-hiring phase.

Fraud can happen at any point in the worker lifecycle, including:

- Application/pre-hiring
- Interview
- Background screening during hiring process
- On-the-job training
- Re-certification
- Entering a new jobsite
- Entering a new contract

⁵ <https://www.mintzglobalscreening.com/media/distribution-of-fake-safety-certificates-puts-public-at-risk/>

⁶ <https://www.fastcompany.com/90708363/credential-fraud-is-a-major-concern-for-businesses>



Safety training is one of many critical layers of controls in the industry. Ensuring workers are properly trained and certificates are valid is a priority. **MURRAY ELLIOT**

RISK

The risks inherent in credential fraud are incredibly far-reaching. Particularly when working in highly regulated industries with high-stakes training, credential fraud can result in serious public harm, safety risks, reputational risks, financial risk, fines and Ministry of Labour repercussions, and even stock price impacts, for publicly-traded companies. Here are some real-world examples of the risks and consequences.

FAKE SAFETY CERTIFICATES IN ALBERTA

In 2021, RCMP investigators in Red Deer, Alberta uncovered a large-scale fraud where thousands of counterfeit safety certificates, such as first-aid training and hydrogen sulphide awareness training, were being sold all across Western Canada.⁷ The certificates were sold to workers at major safety-sensitive organizations, including Energy Safety Canada and the Canadian Red Cross.

“Safety training is one of many critical layers of controls in the industry,” said Murray Elliott, president and CEO of Energy Safety Canada, in response to the crisis. “Ensuring workers are properly trained and certificates are valid is a priority.”

The fallout grabbed headlines across the country, and created significant reputational risk to the impacted

organizations. It also sparked conversation about what other safety-sensitive sectors have been experiencing similar upticks in credential and training fraud. The issue has been on the rise in mining, construction, transportation, organization with WHMIS training, and many more regulated industries.

UNCREDENTIALLED ENGINEER CREATES AUDIT RISK

As another example, prior to engaging with Credivera, a recruitment partner once placed an engineer in a high-risk position with a mid-stream company without verifying the source of their level 3 credential. A few weeks into the job, the company went through a COR audit.

As it turned out, the engineer did not have the correct credential, and had been running an entire steam-fitting operation. This put many people’s safety at risk, and could have been completely devastating for the individuals and the company.

“This company was a publicly-traded company, so a lapse like that could directly impact their ESG score, and their stock price – plus their trust from investors,” said Giurescu.

⁷ <https://www.cbc.ca/news/canada/edmonton/alberta-rcmp-fraud-fake-safety-certificates-1.6237221>

FORGED CERTIFICATES FOR HEALTH-CARE WORKERS

Also in 2021, a small Montreal training company faced fraud charges for forging and selling certificates to uncredentialed health-care workers.⁸ The certificates, which allegedly sold for \$800 each, enabled untrained workers to serve vulnerable and ill populations as orderlies.

With an ongoing shortage of orderlies, health-care assistants, and personal support workers in Quebec amidst the ongoing COVID-19 pandemic, many organizations have been desperate to hire staff. It remains to be seen how many health-care workers have been employed with these fraudulent certificates, and have been treating patients without training.

LEARNER FRAUD CAUSES DIRE CONSEQUENCES

There have also been high-profile situations where learner fraud has resulted in serious consequences. In the legal case *R. v. Rose's Well Services*, for instance, an Alberta employer was convicted of safety offences after two workers were badly burned in a fire while off-loading hydrocarbons from a tanker truck. As part of its due diligence defense, the employer pointed to the fact that its workers had taken the Petroleum Safety Training from Enform, an online program providing basic safety training for oil and gas workers. However, at trial, one worker testified to helping his co-workers through the program and even answering the exam questions for many of them.⁹



This company was a publicly-traded company, so a lapse like that could directly impact their ESG score, and their stock price - plus their trust from investors.

DAN GIURESCU

⁸ <https://montrealgazette.com/news/local-news/couple-charged-with-selling-fake-orderly-training-certificates>

⁹ <https://www.thesafetymag.com/ca/topics/technology/can-you-spot-the-fake-credentials/184131>

SOLUTIONS

How can technology, training, and credential management solutions mitigate these risks? Tools like We Know Training's LearnerVerified (LV) and Credivera's digital wallet can catch and prevent fraud before it ever becomes an issue. Training that makes use of learner verification technology, and verified credentials that ensure transparency and trustworthiness, can help your organization overcome the emerging challenges of workplace fraud.

LEARNER VERIFICATION

LearnerVerified is a technology offered by We Know Training, which adds a layer of defensible security to any course by ensuring the right person is attending. It uses sophisticated monitoring technology including facial recognition to track who is taking the course, if they are away from their screen, or if they are being assisted by someone else.

Capabilities like these can dramatically mitigate the risk of learner fraud in an online environment. However, organizations do need to address any privacy concerns that may arise from this level of learner security. That's why We Know Training uses secure, cloud-based proprietary technology, which meets SOC 2 Type Compliance and GDPR standards to protect learners' data.

LearnerVerified can be added to any online training course you offer, and it will verify learner attendance and independent completion with these three steps.



Step 1: Photo verification

Learners take a photo of themselves using their computer's built-in camera the first time they log in to their course. LearnerVerified records and stores this photo for verification.



Step 2: Identity verification

Valid government picture ID is stored on file and matched to each learner's photo to validate their identity.



Step 3: Monitored attendance

LV monitors attendance throughout the course by capturing learners' photos to flag micro-moments of prolonged absences or other anomalous activity.

VERIFIABLE CREDENTIALS

Verifiable digital credentials provide a level of security and trust while virtually eliminating fraud and human error. In short, verifiable credentials are data objects (certificates, training documents) consisting of claims made by the issuer (government agency, educational institute) attesting information about an individual.¹⁰

The digital credentials produced by Credivera use blockchain technology to provide tamper-proof credentials that stand up to scrutiny.¹¹ There is no manual data entry or human intervention at all – it's all automated through a secure API. These digital credentials provide full traceability through every step of the process, and can integrate with LearnerVerified so that an employer can see everything in one place and in real time.

Contained within an individual's digital wallet, verifiable credentials are highly portable across trusted, global networks.

How it works

In practice, verifiable credentials create a secure communication ecosystem between the parties that issue, manage and verify the credentials. The three components of a verifiable credentials ecosystem are:

- 1. Issuer:** training provider that issues the credential
- 2. Holder:** individual learner who holds the credential
- 3. Verifier:** third-party employer that requests credential verification

This verifiable credential model is decentralized, placing the holder of a credential at the centre of the ecosystem, giving those individuals complete control of their credentials and identity. The holder can then securely share their credentials with a verifier and micro-choose which details they want to share, an emerging concept known as self-sovereign identity. These shared records can be revoked at any time by the holder.

There are many benefits to the verifiable credentials solution. Using verifiable credentials gives training providers instant global reach, increasing brand exposure and building trusted relationships with future clients. It also supports:

- **Visibility:** Maximize visibility of alumni and training programs to grow student base.
- **Reputation:** Enhance industry reputation to promote brand and alumni relations.
- **Administration:** Optimize internal resources with faster response to credential requests and proactive management of course renewals.
- **Trust:** Issue fraud-proof verifiable digital credentials to build trust with your customers.

¹⁰ <https://www.credivera.com/blog/understanding-verifiable-credentials>

¹¹ <https://www.credivera.com/blog/understanding-verifiable-credentials>

CONCLUSION

As technology has created new challenges and risks in the workplace, it has simultaneously provided us with new solutions. Integrating learner and credential verification are the future-proof solutions employers need to start building the workplace of tomorrow, today.

As learner and credential fraud continues to rise, it is more important than ever to implement these solutions in your workplace – especially for regulators, associations, government, and licensing bodies that provide high-stakes training.

Investment in these solutions is minimal, particularly when compared to the risks to public safety, reputation, and financial health that credential fraud can cause.

Protecting the public looks different in our evolving digital world, and strong learner and credential management is an essential piece of the puzzle.

RECOMMENDATIONS

1. Leverage technology tools to verify your learners' identities during training, particularly online training.
 2. Take measures to ensure the right person is completing online testing or exams.
 3. Create a defensible, high-integrity compliance program that will hold up to ministerial, regulatory, or legal scrutiny.
 4. Verify credentials at the source via trusted digital credentials, not paper ones which can be easily altered.
 5. Be aware of upcoming credential expirations, and verify that your team is current and compliant.
 6. Double-check and independently verify credentials from candidates who come from recruiters or placement agencies.
 7. Empower your organization with a technology solution to make sure learners and credentials are verified with the highest degree of trust.
- 



ABOUT WE KNOW TRAINING

We Know Training is a fully-managed solution provider for online training that matters. As a technology-enabled training company, we help you create and deliver exciting, engaging courses that make a true impact. We're your one-stop solution partner to streamline and monetize your training, empower your learners, and move the needle on your business goals. With offices in Toronto, Edmonton, and Cambridge, We Know Training supports regulators, associations, government and licensing bodies across Canada and internationally.

weknowtraining.ca

ABOUT CREDIVERA

Credivera is the world's first secure, open exchange for verifiable credentials. A leader in workforce management and digital identity, Credivera gives employees, employers, and organizations that issue credentials increased productivity and control of how important credentials are stored and shared. The Credivera Exchange optimizes personal privacy and trust, with up-to-date verifiable credentials secured in a digital wallet, resulting in reduced risk for all. Founded in 2017, with offices in Toronto and Calgary, Credivera supports regulated industries and global technology firms in over 30 countries worldwide.

credivera.com

