How Digital Credentials can Prevent Fraudulent Certification and Qualifications

Whitepaper

Credly by Pearson

Overview

Fraudulent certifications and qualifications are a global issue that have a detrimental impact on credential issuers, learners and organizations.

Fake credentials have escalated into a global problem and **a billion-dollar industry**. A primary reason is the intense competition in the job market, which drives individuals to enhance their qualifications or obtain specific certifications to distinguish themselves from other candidates.

Fraudulent credentials provide an undue advantage for those lacking genuine qualifications or desiring to stand out in the market without investing money and time. Other individuals use them to improve their personal image and meet expectations to improve their employability.

Credential fraud is a significant problem worldwide, with the **proliferation of educational and training credentials** exacerbating the issue. For example, as reported in the Washington Post, there is a "maze" of nearly a million unique education credentials in the United States, including not only degrees but also badges, certificates, licenses, apprenticeships, and industry certifications. And more have popped up during the pandemic, as career switchers seek education and training.

"The more pressure we put on people to have credentials, and the more important they are for opening the door or getting a raise or a promotion, the more the bad guys are going to take care of the demand side of the curve."

Allen Ezell
Retired FBI Agent Specialized in Investigating Educational Fraud

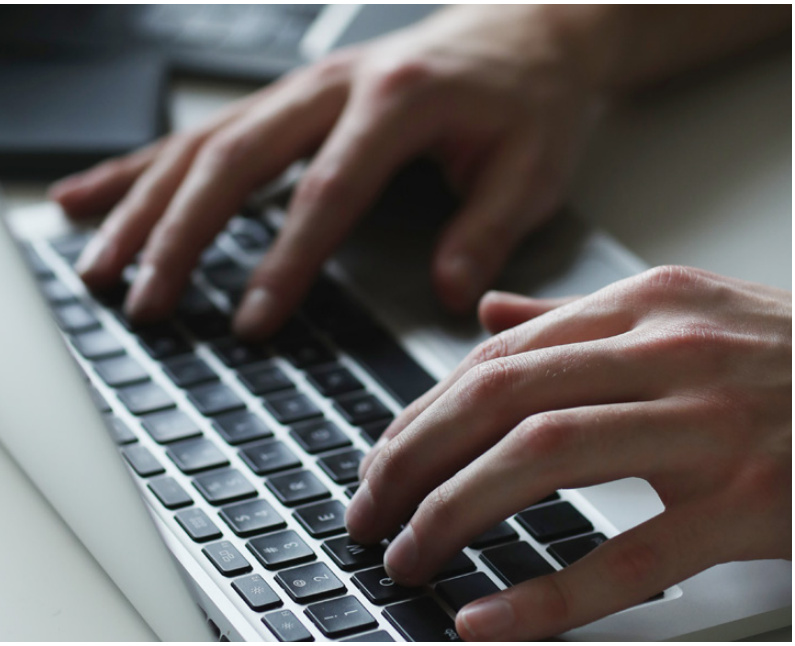
Over-stretched human resources, admissions and issuing departments mean the majority of fraudulent activity goes undetected. But there is substantial evidence of widespread fraud, whether it is a falsehood on an employee or applicant's resume, an embellishment on a social media profile or the presentation of completely falsified qualifications and certifications:

- According to a 2018 study by HR consultancy the Florian Mantione Institute, as many as **65% of resumes are misleading in their claims**.
- 60% of applicants claim high levels of competency in skills they didn't often use at all, while 33% include achievements and certifications they did not earn (**Checkster, 2020 survey**).

And according to the American Association of Collegiate Registrars and Admissions Officers (AACRAO), even though document fraud ranges from minor alteration to complete fabrication, "it is all **fraud**."

While the issuing organization might not be aware of those who committed credential fraud, these "indirect" or "deceptive" frauds can undermine the credibility of the issuing organization and cause harm to others who have earned their qualifications legitimately.

This whitepaper highlights the negative impact of fraudulent certification and qualifications on issuing organizations, credential earners and employers, and presents digital credentials as a secure, verifiable alternative. Additionally, it offers a 'Credential Fraud Prevention Checklist' to help reduce credential fraud and preserve the integrity of your certification programs.



What are Fraudulent Credentials?

Certification and qualification fraud refers to the act of dishonestly obtaining, presenting, or using qualifications or certifications that are unearned, altered, or counterfeit. These types of fraud can undermine the credibility of educational and professional institutions, lead to unqualified individuals being hired, and create an unfair advantage for those involved in the deception.

There are different forms of fraudulent certifications and qualifications:

- The presentation of a certificate from a recognized institution that has been falsified.
- The presentation of a certificate from an unrecognized institution.
- False assertion of having obtained a certification when this is not the case, whether on a CV/Resume during an interview or on a personal profile.
- Misrepresenting the outcome or level of certification or qualification achieved.
- Using an expired certification or qualification.

The Consequences of Credential Fraud to Key Stakeholders

Fraudulent credentials pose a significant issue for higher education and training organizations, certification issuers and employers as they undermine their legitimacy and reputation. For earners, they cheat honest candidates out of opportunities for further education or employment.

- **Issuers:** Fake qualifications pose **a reputational risk** for certification issuers and other academic institutions. Skepticism about the value of legitimate qualifications damages a brand and can lead to reduced demand for certification and result in financial losses.
- **Credential Earners:** Earners rely on credible and verified credentials for their own professional development, allowing them to showcase their achievements and commitments. If they are unsure about the reputation and trustworthiness of a certification program, they may hesitate to sign up and be reluctant to affiliate with the issuing organization.
- **Employers:** In the context of a **global skills shortage**, hiring qualified staff is crucial for addressing the gap and reducing staff turnover. Yet, fake credentials can lead to hiring unqualified candidates, resulting in decreased productivity, increased training costs, and potential legal liability. Employers may also face damage to their reputation if they are found to have hired individuals with fraudulent qualifications (particularly in the case of C-suite and senior managers).

Real-life Cases of Credential Fraud and Their Impact

Industrial impact: In the US, **states are rooting out fake nurses** after a federal investigation uncovered a network of nursing school operators, centered in South Florida, that sold diplomas to students without the proper training. About 7,600 students paid an average of $15,000 for the bogus certificates, from 2016 to 2022. Around 2,400 went on to obtain jobs as registered nurses in multiple states. In some cases, lawyers assert that states are questioning the credentials of nurses who earned diplomas legitimately.

Financial cost: Ronald Zarrella, the CEO of Bausch & Lomb, **was found to have lied about having an MBA from New York University**. He had only taken a few courses at the university but never completed his degree. The news of Zarrella's lie was widely reported, which led to negative publicity for the company. In terms of financial implications, Bausch & Lomb's stock price fell by more than 5% after the news broke. As a result, Zarrella was forced to resign from his position.

Reputational damage: Marilee Jones, the Dean of Admissions at MIT, was in 2007 **found to have lied about her academic qualifications**. She claimed to have degrees from three universities, including a PhD, but it was later discovered she had never earned any of them. The revelation caused MIT a significant loss of credibility. Jones was forced to resign, and her actions damaged the reputation of those who had legitimately earned degrees from the institutions she claimed to have graduated from.

What are Digital Credentials?

Digital credentials offer verified proof of a learner's competency and skills. They're a smarter, data-rich alternative to traditional paper-based certificates, providing earners with a shareable portfolio of verifiable achievements that can continue to grow through the course of their careers.

By using a platform like **Acclaim**, qualification and certification providers can easily create, and issue digital credentials and digital badges backed by verifiable data. By enabling a strict, clear verification process, they significantly reduce the risk of credential fraud and make it quick and easy for badge earners, educational institutions, and employers to check their authenticity.

Additional Benefits of Using Secure Digital Credentials:

Issuers

- **Enhanced brand reputation:** By issuing secure digital credentials, organizations can minimize the risk of forgery and tampering. Demonstrating a dedication to innovation and security enhances their brand image and helps attract more learners or clients.
- **Efficient tracking and management:** Issuing organizations can track and manage digital credentials more efficiently, monitoring their usage and identifying trends or potential issues.
- **Cost savings:** Issuing digital credentials can be more cost-effective than printing and distributing physical certificates, reducing administrative and logistical expenses.

Credential Earners

- **Easy sharing and verification:** Secure digital credentials can be easily shared with potential employers, educational institutions, or other stakeholders. This simplifies the verification process, as recipients can quickly confirm the credential's authenticity.
- **Portability and accessibility:** Digital credentials are accessible from anywhere, anytime, making them more convenient for credential earners. They can be stored and managed online, eliminating the need for physical copies.
- **Enhanced credibility:** Secure digital credentials, backed by rigorous authentication and verification processes, increase the credibility of the earner's qualifications, making them more attractive to employers and peers.

> *"I think the biggest benefit of earning a digital credential is confirming the associated knowledge to help me in my daily role and professional development... Having digital badges allows customers I have not dealt with previously to get a quick understanding and verification of my areas of knowledge and build confidence in the level of assistance they are receiving."*
>
> **Brent Brady**
> Esri Digital Badge Earner

- **Up-to-date qualifications:** Features like expiration notifications encourage earners to stay current with their certifications, ensuring they maintain relevant skills and knowledge in their industry, which can in turn, enhance their employability.

Employers

- **Standardization and interoperability:** Secure digital credentials based on open standards promote standardization and interoperability across different platforms and systems, making it easier for various stakeholders to exchange and validate information.
- **Streamlined verification process:** Secure digital credentials enhance both time and cost efficiency in verifying candidates, enabling organizations to get the right people for the job to boost skills and competencies.
- **Reduced risk of reputational damage:** Secure digital credentials offer a reliable and streamlined solution for employers to verify and validate candidates' qualifications and ensure they recruit genuinely qualified individuals.
- **Improved skills and knowledge:** Digital credentials encourage individuals to maintain up-to-date qualifications, leading to a more skilled and knowledgeable workforce.

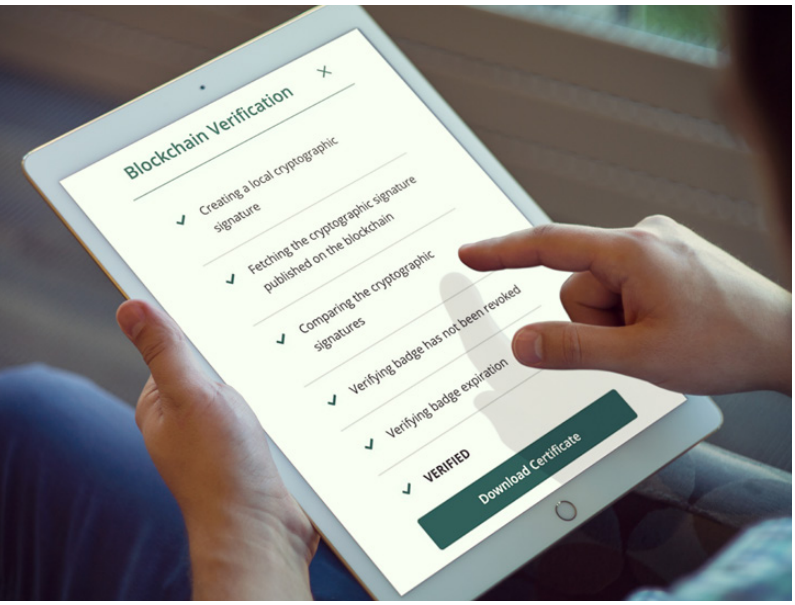
Case Study: ICF Tackles Credential Misuse with Secure Digital

International Coaching Federation (ICF), a leading global organization for professional coaching, started their credentialing program in 1998 with 35 credential holders. In 2019, they had just under 30,000 ICF credential holders worldwide. The exponential growth has also meant ICF started to see a huge spike in misusing credentials marks and needed an easily managed and scalable platform to help issue their credentials.

Traditionally, like many associations, their credentials were provided as simple jpeg files, so earners could share them online. But slowly, they began to see expired and fraudulent credentials being presented. This negatively affected ICF's reputation and increased their administrative burden when enforcing the correct usage of their credentials.

To solve the issue, ICF started using Acclaim to award secure, portable, and easily shareable digital credentials for their earners.

In the two years since their digital credentials program launch, ICF has seen **a 62% increase in the number of active credential holders** and a 5% rise in their retention rate. They've also seen a significant decline in the reports of mark misuse.



Validation and Authentication: How Acclaim Ensures the Security of Digital Credentials

With **Acclaim**, organizations can confidently embrace digital transformation while minimizing the risks associated with fraudulent certifications and qualifications. These are the key features of the Acclaim platform that enable authentication and verification:

Blockchain technology: By leveraging **blockchain**, Acclaim creates a decentralized, tamper-proof storage system for credentials. Each credential is stored as a unique block on the blockchain, which ensures the data cannot be altered without the consensus of the network. By providing a transparent, verifiable, and secure method of storing and validating credentials, the technology makes it difficult for fraudsters to create fake certifications.

Robust authentication and verification processes for issuers and badge earners: Acclaim implements rigorous authentication and verification processes for both issuers and recipients. Issuers must be validated and verified before they can issue digital credentials, ensuring that only legitimate organizations can create and distribute them. Likewise, recipients must authenticate their identities before receiving and sharing their credentials, reducing the chances of identity theft and misrepresentation. (A robust process doesn't mean a complicated one; **accepting a secure badge takes only a few steps**).

Real-time monitoring and tracking of issued credentials: **Acclaim Analytics** provide real-time monitoring and tracking of issued credentials. This feature allows issuers and other authorized parties to keep track of the status of each credential, including when it was issued, who received it, and when it was last accessed or shared.
This real-time monitoring can help detect and prevent fraudulent activities, such as unauthorized sharing or tampering with credentials.

Integration with other systems for efficient data exchange and validation: Acclaim supports **integration with many industry-leading software and custom apps**, such as human resources or learning management systems (LMS), to enable efficient data exchange and validation. This integration allows organizations to verify the authenticity of a digital credential quickly and securely during any activities requiring qualification validation. By streamlining this process, organizations can reduce the risk of fraudulent certifications and qualifications entering their systems.

Expiration notification emails: The expiration notification email feature on the Acclaim platform is an additional measure to maintain the integrity and credibility of digital credentials. By automatically sending email notifications to badge earners when their digital credentials are about to expire ensures they stay informed about their credentials' validity, and prevents accidental use of expired certifications. It also encourages them to keep their qualifications current, maintaining the value and relevance of their professional skills.

Credential Fraud Prevention Checklist

To help you establish a reliable and secure credentialing process, we've developed this comprehensive checklist. Follow these best practices to minimize credential fraud and maintain the credibility of your certification programs:

- ☐ Implement a secure digital credentialing platform that offers robust authentication, encryption, and verification features.
- ☐ Integrate your digital credentialing platform with other systems (LMS, HR platforms, etc.) for efficient data exchange and validation.
- ☐ Train staff members on the proper issuance, management, and verification of digital credentials to minimize human error and vulnerabilities.
- ☐ Establish a clear and transparent policy regarding handling credentials and personal data, addressing privacy concerns and data protection.
- ☐ Educate stakeholders (learners, employees, employers) on the importance of secure digital credentials and how to verify them.
- ☐ Encourage the use of secure methods for sharing and showcasing credentials, such as sharing through the credentialing platform or social media integrations.
- ☐ Periodically audit and review the effectiveness of your fraud prevention measures and adjust as needed.

Safeguarding Your Data with Rigorous Security and Privacy Measures

The Acclaim platform offers secure digital credentials and prioritises protecting your data and badge information. We uphold various **ISO** certifications, comply with GDPR, and enforce rigorous security measures. We also receive comprehensive training in data protection and privacy practices.

Why Acclaim?

Acclaim is the network of choice where 3,000+ certification, assessment, education providers and employers issue their credentials. With increasing levels of fraud across the board, organizations must utilize digital credentials to safeguard credentials earners, employers and themselves from the negative impacts of fraud.

We empower organizations worldwide to design and issue secure badges, scale and easily manage their credentialing program with advanced analytics.

Want to learn more?

Learn why Acclaim is the first choice for organizations seeking a secure digital credentialing program by getting in touch, and our expert team can provide you with a demo of Acclaim.

GET STARTED

Credly by Pearson

Credly is helping the world speak a common language about people's knowledge, skills, and abilities. Thousands of employers, training organizations, associations, certification programs, and workforce development initiatives use Credly to help individuals translate their learning experiences into professional opportunities using trusted, portable, digital credentials. Credly empowers organizations to attract, engage, develop, and retain talent with enterprise-class tools that generate data-driven insights to address skills gaps and highlight opportunities through an unmatched global network of credential issuers.