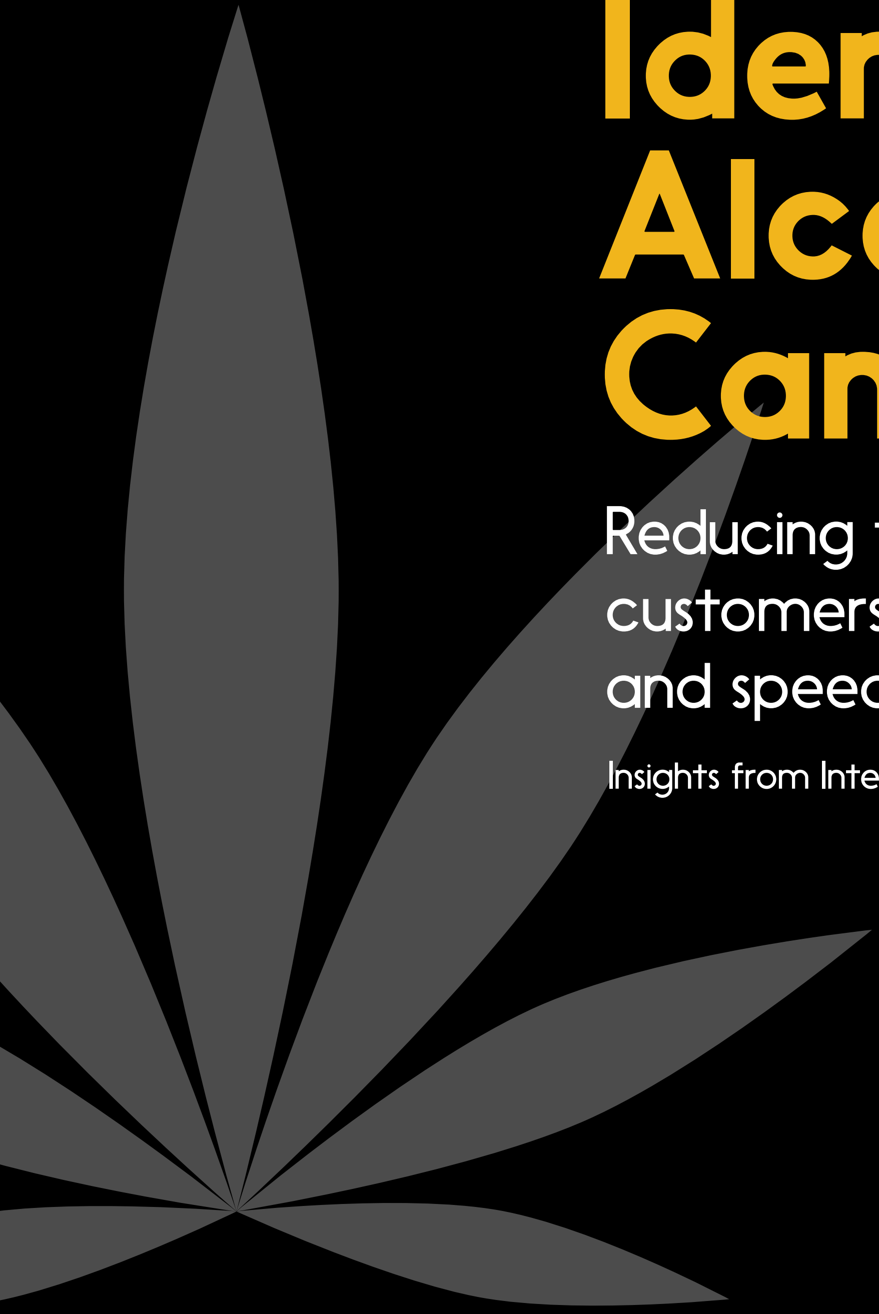
Digital Identity in Alcohol & Cannabis

Reducing fraud, protecting customers and staff, and speeding transactions

Insights from Interac Corp.



> "Verifying the age of a customer is a fundamental part of many transactions, and the presentation of physical ID has until recently been the only choice for meeting this requirement.”

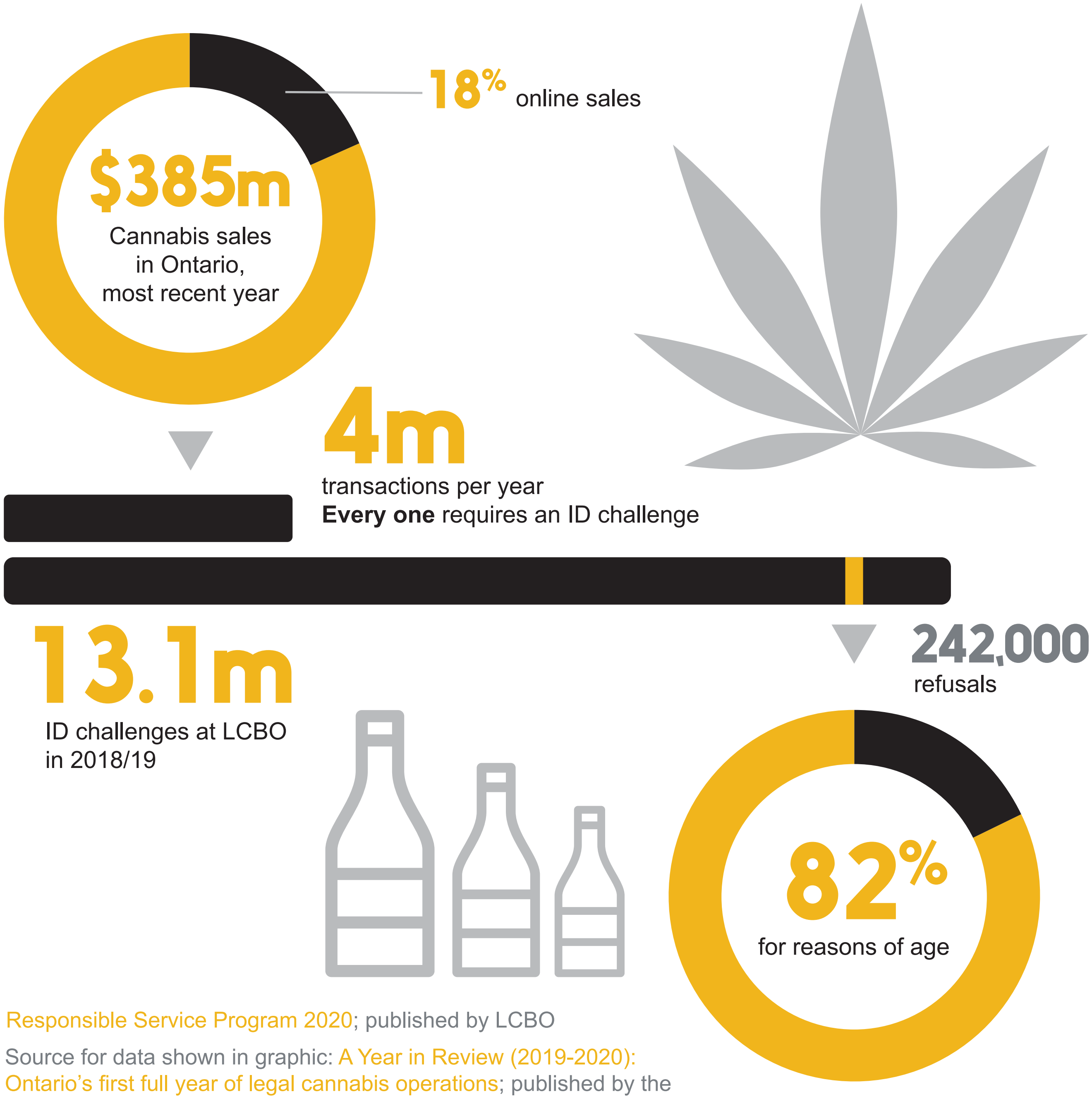
Introduction

The alcohol retail industry has gone through many transformations over the decades, while cannabis, recently legalized, is arguably going through its very first. Despite their difference in age, however, both tightly regulated substances are simultaneously facing the challenge of how to do business in a world shaped both by digital commerce and by an unexpected pandemic. In meeting this challenge, digital ID has a significant role to play. Verifying the age of a customer is a fundamental part of many transactions in these sectors (it happens, for example, with each of the four million annual cannabis transactions in Ontario*), and the presentation of physical ID — a driver's licence, for instance — has until recently been the only choice for meeting this requirement. Physical ID, however, has limitations: it is notoriously vulnerable to fraud, it is inconvenient and slows transactions for both merchants and for customers. It involves a risk of viral transmission (passing an ID card to a cashier for inspection), and by making available information — like a customer's name and address — not strictly needed for the sale, it undermines privacy. As we will see in this white paper, digital ID holds the potential to address all of these shortcomings — in doing so, helping alcohol and cannabis retailers serve their customers more effectively than ever.

* A Year in Review (2019-2020): Ontario's first full year of legal cannabis operations; published by the Ontario Cannabis Store (OCS)

How big is this problem?

Alcohol sales in Canada today prompt millions of ID verifications by retailers — more than 13 million in Ontario last year alone.* While cannabis sales are still a long way from the levels set by alcohol, the share of cannabis transactions made online is already significant. Every sale, online or in-person, requires an ID verification. Driving cost, time, and risk out of this process through digitization presents a huge opportunity for retailers and for consumers.



$385m
Cannabis sales in Ontario, most recent year

18% online sales

4m
transactions per year
Every one requires an ID challenge

13.1m
ID challenges at LCBO in 2018/19

242,000
refusals

82%
for reasons of age

* Responsible Service Program 2020; published by LCBO

Source for data shown in graphic: A Year in Review (2019-2020): Ontario’s first full year of legal cannabis operations; published by the Ontario Cannabis Store (OCS)

How digital ID helps

A verifiable, fully digital identity credential offers several important benefits on both sides of the retail counter (whether online or in-person).

Retailers

Digital ID **reduces identity fraud**, giving retailers a high level of assurance that each customer is who they say they are.

Digital ID **reduces costs and improves the sales flow**. Retailers don't need to invest in expensive new technology like ID scanners and can process sales more rapidly.

Digital ID **reduces risk**, ensuring that customers are of legal age, protecting retailers from legal liability in cases where a clerk might fail to recognize a fake physical ID.

Users

Digital ID **improves privacy and security**, requiring customers to share only minimum information to prove their age (vs. sharing their entire driver's licence), conveyed in a cryptographic, fully-secure format illegible by the salesperson.

Digital ID **offers greater convenience**. It's one less thing to carry (and to possibly lose), and a contactless "tap" of a phone is a lot easier than searching your wallet for a physical ID.

Digital ID **speeds up online purchases**, since an ID check can be completed almost instantly at the time of ordering rather than manually when goods are delivered.

Using digital ID: a walkthrough

Step 1: Open digital wallet

A customer arrives at the counter with the wine she has chosen for this evening's dinner party. Asked for proof of age, she pulls out her mobile device and opens her digital wallet.

Step 2: Choose tap or scan

The cashier asks the customer if she would prefer to tap or scan the ID in her digital wallet. She decides to tap and makes that selection in her digital wallet.

Step 3: Authentication

The cashier presents the terminal to the customer, who taps her mobile device to present a proof of legal age. This "cryptographic proof"* is then securely verified against a trusted source (e.g. government database) for immediate authentication.

Step 4: Pay with digital wallet

After receiving her confirmation notification, the customer then proceeds to pay for her wine using her digital payment wallet and wishes the cashier a good day.

Online purchases would follow a similar path, with the difference that the cryptographic proof of legal age would be uploaded to a site directly from a customer's device via the Internet, rather than by tapping a phone or scanning a QR code in person.

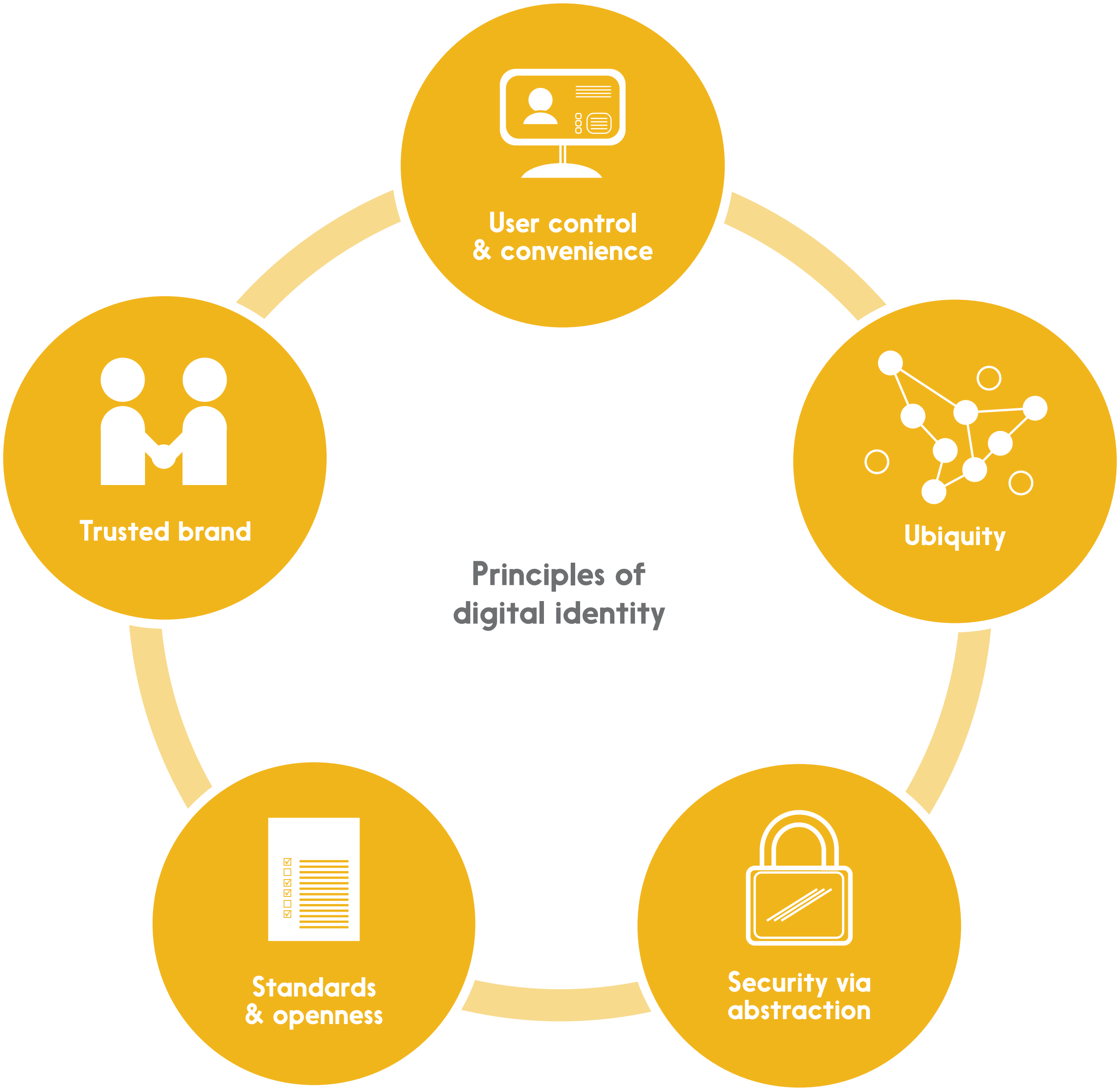
* See next page

What is a cryptographic proof?

Cryptographic proofs allow a person to prove to an entity (e.g. merchant) that they have the information being requested (e.g. age) through a proof without revealing that information. The merchant verifies the proof with a trusted source (e.g. government database) and processes the transaction.

Our principles

Digital identity is easy to theorize about, but architecting and implementing a comprehensive, secure, and sustainable system is another matter entirely – and an important part of getting it right is having a clearly articulated set of principles to guide the effort. We believe that there are five:



User control & convenience

No one wants to entrust a system with their personal details if those details are going to be transferred to and stored by numerous parties – especially if this happens without the user's knowledge and express consent. While ensuring user control, an identity system must also be convenient and easy; if it isn't, it won't be adopted by users, many of whom are already used to intuitive apps on mobile devices.

Standards & openness

In any dynamic system, it's difficult to predict what the future will look like – so it's important to build today's solutions on universally-agreed standards. Not only does this reduce costs by eliminating the expense of building and then later having to adapt custom, one-off solutions, but it enables solutions built by others in the future to "plug into" the initial solution. Openness encourages adoption, innovation, and flexibility.

Ubiquity

Security risks abound when people create different identities and passwords for each public and private service they access. They'll often default to a single, easy-to-remember (and easy to crack) password, for example. At the same time, a digital identity that only applies to a handful of services will probably not be well-adopted. A ubiquitous system is a more convenient and a more secure system.

Trusted brand

No user is likely to adopt an identity solution built or maintained by an organization they don't trust. The question of identity is simply too important, and the impact of identity theft too great, to leave this to chance. Further, building a large-scale (and ubiquitous) solution will require the cooperation and coordination of many players, and these players need to trust each other and the organization leading the effort.

Security via abstraction

Even with the best user controls, a certain amount of identity data must be part of transactions in any given ecosystem. A highly effective way of securing that data is to "abstract" it, by replacing a private identifier with a publicly-available one (like a person's email address) or by replacing it with a randomized number that serves as an authorized "token" for the purposes of the transaction – and is not useful for any other purpose.

Conclusion

Supported by a set of foundational principles like those presented here, the move away from traditional physical ID to a highly-secure, fraud-resistant, convenient digital ID is one with the potential to address many of the more difficult challenges faced by alcohol and cannabis retailers in both their brick and mortar and their online channels. Lower risks, reduced costs, greater sales velocity, and happier customers are among the tangible benefits waiting to be seized by enterprises and governments who are ready and willing to make this potential real. Alcohol and cannabis, meanwhile, is only one of the many sectors that digital ID will support and improve; we'll be exploring other industries and their use cases in upcoming white papers.

If you're interested in collaborating with Interac on the future of Digital ID, drop us a line at **digitalid@interac.ca**

"Lower risks, reduced costs, greater sales velocity, and happier customers are among the tangible benefits waiting to be seized."

For more information on this topic, visit innovation.interac.ca

Published August 2020

Except as permitted by law, this document shall not wholly or in part, in any form or by any means, electronic, mechanical, including photocopying, be reproduced or transmitted without the authorized consent of Interac Corp. This document is for informational purposes only and Interac Corp., by publishing this document, does not guarantee that any information contained herein is and will remain accurate. Interac Corp., including its agents, officers, shareholders and employees shall not be held liable to any party or parties for any loss or damage whatsoever resulting from reliance on the information contained in this document.