



## DIACC Industry Insights: Digital ID in Commerce



### **What is Digital ID and How Does It Impact Key Industries and Their Customers?**

This paper is the third in a series prepared by the Digital ID and Authentication Council of Canada (DIACC) highlighting the potential impact that digital ID could have on key sectors of the Canadian (and global) economy.

In this third paper, we focus on the commerce industry.

### **What is Digital ID?**

Identity is a type of information about an entity (for the sake of simplicity, a person) that uniquely describes the entity within a given context. In other words, identity is a collection of indicators (or attributes) about a person (entity) that make that person unique. Digital identity (ID) is a set of attributes that links a physical person

with their online interactions. Digital ID refers to one's online persona - an online footprint. It touches important aspects of one's everyday life, from financial services to health care and beyond.



## What You Need To Know

- Digital ID technology could transform the way e-commerce operates, as it will lighten the burden of handling an increasing amount of sensitive data, and the reliance on data.
  - Digital ID enables data minimization, which is the selective reveal of one's data, as appropriate for the transaction. With data minimization, individuals have more control over their own data.
  - Increasing transaction complexity, as well as volumes, are trends that are driving the need for more efficient and effective identity systems.
  - In Canada, e-commerce is exploding, both in sales and the number of online shoppers. In 2017, there were 18.5 million e-commerce users in Canada, and by 2021, there are expected to be an additional 5.21 million users shopping online.
  - Retail e-commerce sales are estimated to reach over C\$55 billion by 2020.
  - Regardless of the payment type, device, or service provider, digital ID can enable a more personalized, private and efficient shopping experience, both online and in stores.
  - In a digital environment, payments require a great deal of trust, as there is no ability to "see" the person on the other end of the transaction. Having confidence and trust at both ends of the interaction
- enables growth in the digital economy, and it critical to the success of retailers and brands.
- Younger generations are much more likely to use financial services or digital payment systems from brands they know and trust.
  - Digital-savvy customers have developed high expectations of e-commerce transactions, such as seamless service delivery. Failure to meet these expectations has significant consequences for organizations, such as loss of business to a competitor, loss of revenue, reduced customer lifetime value, and negative reviews.
  - Identity is largely based on physical records (e.g. passports, identity cards). However, these documents can be falsified, altered, tampered with, lost or stolen. A strong digital ID system mitigates these risks as it uses secure user information credentials such as biometrics, PINS and passwords, or smart cards. As more and more services migrate online, it is crucial to provide a range of options for identification.
  - Payments via wearables (such as watches), are on the rise. Such solutions make plastic cards unnecessary. As no personal information is shared, fraudsters are unable to intercept.



## What This Means For Stakeholders

Digital ID has far-reaching impacts, for a variety of stakeholders. With valuable and private citizen information involved, a lot must be taken into consideration in a society that uses digital ID for interactions. To enable growth in the digital economy, and streamline the process for consumers and retailers, payments and digital ID need to merge.

### Consumers

- Consumers can use their digital ID to connect a retailer to a payment services provider to facilitate transactions.
- The degree of safety and security should reflect the size of the transaction, while ensuring ease and convenience for consumers.



- When user information is overexposed, this puts users at risk of identity theft and privacy breaches. The concept of data minimization - not giving up anything more than you need to - applies here, as it protects the privacy of the individual, and preserves anonymity.
- Sign up, login and check out forms are a hassle to fill out. Often, too much information is collected from users even when it's not required to complete a transaction, and instead, is used for the retailer's own statistical use.
- Consumers usually do not want their data being shared for advertising (unless they consent to it), and are unhappy to have their data sold to third parties.
- According to a recent survey by KPMG, fewer than 10 per cent of customers felt they had control over the way organisations handle and use their data today. A digital ID system would give users more control over their personal data.
- Mobile payment service Venmo offers a frictionless onboarding process - iOS and Android users who download the app will be able to directly link it to their bank accounts, using the same username and password they use for online banking.
- In 2013, AirBnB incorporated identity verification to its platform, adding more transparency and reducing the fear and friction that can arise when strangers do business.
- The number of people calling in for password resets would be minimized.
- An average user can have 150 login accounts they have to manage, each with different approaches to passwords and authentication.
- Passwords take up a lot of workers' and IT teams' time in recovery, and this can be detrimental to a business' productivity and bottom line.
- In verifying a consumer's address, identity verification is critical, and a more streamlined process would allow for errors to be caught.

## E-commerce

- Digital ID would facilitate faster transactions, and potentially easier verification of accounts.
- A secure digital ID system would not only benefit the safety of a person's personal information. With such a system, retailers would not have to hold as much identifiable information, which would decrease the likelihood of fraud or breach.
- For providers, having the ability to perform Know Your Customer (KYC) checks to satisfy regulator requirements is key. KYC procedures are also a legal requirement in order to comply with Anti-Money Laundering (AML) laws.
  - KYC refers to the steps taken to establish customer identity, understand the nature of their activities and assess AML risks. Having a digital ID system in place would enable this.
- With verified identity, web platforms such as those for peer-to-peer sales like eBay or AirBnB are more secure.
  - Building trust among users is critical to the success of these businesses, as the sharing economy market is estimated to grow from \$14 billion in 2014 to \$335 billion by 2025. It is a market that is challenged by some trust and safety concerns - how can users be sure that various services are reliable and safe, and providers are who they claim to be? Digital identity verification would allow for this.
- Businesses gain value from a structured and secure sales process, as customers enjoy a seamless path to purchase, increasing the probability of customer loyalty and retention.
- Abandonment rates (of abandoning a transaction prior to completing) due to poor customer experiences can result in loss of revenue for businesses. Today, almost 70 per cent of online shoppers abandon their shopping carts. Worldwide, this equates to \$4 trillion in lost revenue per year.
  - Common reasons for abandonment that would be mitigated with digital ID verification include the requirement to create an account, a long and complex checkout process and not trusting a website with credit card details.
  - To combat this and also deliver a positive customer experience, merchants must be able to accurately identify legitimate customers without intrusive authentication steps or additional friction.
  - Utilizing a digital identity solution at the checkout stage will offer a more efficient process for the customer and consequently improve conversion rates.



- By continuously authenticating users based on real-time dynamic identity, device and location, retailers are able to provide a seamless transaction experience, while also protecting against cyber-criminals.

### Retailers (in person)

- For retailers selling restricted goods and content, a digital ID system would allow for age verification.
- For instance, in the U.K., users can now use an app from DIACC member Yoti in convenient stores. Shop owners are provided with free QR code cards, which users then scan with their smartphones, and share their age. The app displays a photo of the user, offering proof of age for anyone purchasing tobacco, lottery tickets and other goods.
- Increased automation may reduce commercial transaction times and/or costs (i.e. faster interactions at the check out), resulting in increased efficiency.
- At airports, biometric verification such as Nexus facilitates faster and automated verification to get passengers through security.

### Businesses

- Lack of a consistent approach to regulation means that it is difficult for any solution to scale. Regulations vary from industry to industry, and from province to province.
- For instance, using an e-signature, one can purchase property in British Columbia, but one cannot use the same to purchase and activate a cell phone online anywhere in Canada.
- Digital ID could be used to improve processes that are difficult today, such as remotely conducting transactions from distant geographic locations.
- In retail, cross-border e-commerce is the fastest-growing sector, comprising more than half of e-commerce transactions.
- Despite high cross-border demand, some merchants are reluctant to expand their reach beyond borders, as these transactions are 69 per cent more likely to be rejected than those made domestically. This is because consumer identity data (i.e. national identity numbers or standards surrounding what constitutes a home address) can vary by region.
- Users behind cross-border transactions may not be real people at all - these

transactions are 15 per cent more likely to involve “bot” device spoofing, and 22 per cent more likely to involve identity spoofing.

- In 2018, there were 5.5 billion bot attacks against e-commerce retailers, compared to 1.8 billion in 2017.
- Statistics such as this highlight the true significance of digital ID in the commerce sector. It is important not to have any digital ID strategy, but one designed with privacy and principles of Canada's Digital Charter in mind, which embraces key principles such as safety and security, universal access and control and consent. A good digital ID system would combat this growing trend.
- As digital ID can be authenticated remotely across digital channels, digital ID could benefit those working in the ‘gig economy’ (i.e. freelancers and Uber drivers). With one click, platforms like Uber could verify these workers, and they could be trusted by both the platforms and customers.
- Additionally, having a singular identity across employers would provide formal recognition of their business expertise.







## Real-Life Applications

In September 2019, a new EU regulation, the [Payment Services Directive 2](#), is set to go into effect. Under this regulation, European banks and other payment firms will be required to implement strong customer authentication on various payments and other operations, such as logins to bank mobile apps and websites. When making an online transaction, each customer will need to be authenticated by at least two of the following: something they have, something they are, and something only they know (this could include an ID document, a biometric identifier such as a fingerprint, or a security question). As the prevalence of open banking and e-commerce grow, this authentication introduces an additional layer of security to defend against the

threat of fraud (e-commerce card fraud now accounts for £310 million in losses annually).

However, recognizing the negative impacts to the customer e-commerce experience with additional checkout steps, European authorities have agreed to extend the deadline for businesses to prepare for and adopt the new rules.

In Canada, [Verified.Me](#) from DIACC member SecureKey makes it easy for individuals to provide proof of their identity, using the information they've already provided to their financial institutions. The platform uses blockchain technology to securely and privately transfer users' personal information to trusted

network participants, providing them with easy access to the services they want, when they want them.

DIACC member GET Group NA recently announced that its GET Mobile Administrator will allow for DMVs and other ID card Issuing Authorities to provide mobile driver's licenses (mDLs) and other forms of mobile identification (mIDs). Furthermore, these will comply with global interoperability standards. With the system, updates to important information such as addresses can be made instantly, resulting in shorter lines at the DMV and improved service delivery.

## Reinforcing Key Values

Providing Canadians with control, consent and convenience are the core components of a digital ID system- these same values are set out in the DIACC's Digital Identity Ecosystem Principles.



Ensuring that privacy is exchanged on a need-to-know basis will improve consumer security, and enhances trust in their provider of digital transactions. DIACC holds that digital ID is critical to the growth and efficiency of the digital economy, and there is the potential to generate more than C\$15 billion of value to the economy.

Furthermore, privacy and user control are crucial components of DIACC's Pan-Canadian Trust Framework, the goal of which is to enable and support the establishment of a secure and privacy-enhancing Canadian digital identity ecosystem.

## Where do we go from here?

The challenge for many digital businesses is that they are trying to solve the problem of individual use cases in silos, plugging one gap while others remain vulnerable," noted LexisNexis Risk Solutions. "At the same time, without a holistic view of your end user across their entire customer journey, it becomes impossible to validate their identity at each touchpoint."

Reducing friction and improving the overall user experience is key.

So now the question becomes: how can you take action to progress digital ID?





- Explore current transactions that your business conducts online - how much assurance do you have that your customer is who they say they are?
- Examine the physical and paper-based transactions and consider what could be automated if that person could be digitally verified.
- Consider embracing a passwordless approach, as alternative authentication methods remove the need to remember or type passwords, leading to better user experience.
- Research firm Gartner forecasts that by 2022, 60 per cent of large and global enterprises and 90 per cent of midsize enterprises will implement passwordless methods in over half of their use cases.

- Alternative methods include mobile device authentication, email one-time passwords and behavioral biometrics.
- Start interacting with digital ID partners to discover how their tools and services could help you incorporate the benefits of digital ID into your organization.
- Collaboration is essential. Working together across the public and private sectors is key to creating a successful approach to the implementation of digital ID systems. Stakeholders must work together to achieve this balance of improving the payments experience and removing friction, without compromising security. .

Finally, join DIACC to have a seat at the table where frameworks and strategies are being developed so that they work for your organization. With members from both the public and private sector, strong collaboration is intrinsic to the work that we do.

### Contact

The Digital ID and Authentication Council of Canada

-  [diacc.ca](https://diacc.ca)
-  [@mydiacc](https://twitter.com/mydiacc)
-  [/company/mydiacc](https://company/mydiacc)
-  [/mydiacc](https://mydiacc)