Verification made easy.
Discover a secure and convenient way to verify your customers and deliver better digital experiences.
Get in touch
Unlock new digit
InLife

We Geek Out on Digital Verification:

Insights from Canadian Business Decision Makers

Report from Interac Corp.

Introduction

Trust is the foundation of any significant relationship, not just among friends and family members.

When consumers interact with a business, they need to trust their personal information will be protected and used for its intended purpose. For businesses, trust is equally important: in order to confidently and securely provide a high quality, personalized product or service experience, businesses must be sure that customers are who they say they are.

Think about the moment someone sets up a new bank account, starts a new job, enrolls in a school or simply creates an online profile with their favourite retailer. Being able to verify and trust the information being exchanged allows organizations to meet their goals, whether it's growing revenue during a challenging economic time, optimizing costs by making use of digital channels or reducing the risk of fraud.

This could explain why 91 per cent of business executives surveyed by consulting firm PwC in 2023 said the ability to build and maintain trust improves the bottom line[1], and why 79 per cent of consumers polled by Interac Corp. (Interac) amid Data Privacy Week said protecting their data is very important to building trust.[2]

> **Trust is the cornerstone of any meaningful relationship, whether personal or business related. By enabling digital verification solutions, organizations can build and maintain trust, ultimately driving growth, optimizing costs, and reducing the risk of fraud.**
>
> **Debbie Gamble,**
> ***Chief Officer, Innovation Labs & New Ventures at Interac Corp.***

Interac, Canada's most trusted financial services brand[3], recently conducted a survey of close to 300 Canadian business decision makers to learn more about:

- Current awareness of digital verification solutions
- Digital verification features that offer the biggest potential and promise
- Barriers to adoption and plans for the future

For most organizations, adopting digital verification processes will require collaboration across multiple areas such as business, IT, legal and sales. It takes individuals running those functions to identify and articulate the use cases where digital verification will bring value. Chief information officers (CIOs) and their teams need to assess the impact on everyday processes and to assist with the selection and deployment of the right solutions.

[1] https://www.pwc.com/us/en/library/trust-in-business-survey-2023.html#:~:text=The%20trust%20that%20businesses%20build,trust%20improves%20the%20bottom%20line
[2] https://www.interac.ca/en/content/news/control-is-top-of-mind-for-canadians-when-it-comes-to-online-personal-information-according-to-new-data-privacy-week-poll/
[3] As named by the 2023 Gustavson Brand Trust Index: https://www.uvic.ca/gustavson/brandtrust/top-10/index.php

The path towards digital verification can be streamlined if those in both business and IT have a deeper understanding of where their peers are on this journey today.

This report will explore the survey data in more detail to offer Canadian companies guidance on leveraging the digital verification solutions they need.

The Business Case for Advanced Verification

Canadian companies are deep into digital transformation, but their work is far from over. The quick pivot to e-commerce and remote work during the pandemic was only the beginning. Rapid advancements in technologies such as generative AI are opening up opportunities to completely reimagine the way businesses develop marketing collateral and provide customer service. Meanwhile, many companies are focused on offering omnichannel capabilities to market, sell and support customers based on their preferred way of engaging with a brand.

According to a Canadian recruiting firm's survey of CIOs released this year, however, two-thirds of IT leaders doubt their organization's ability to deliver on key initiatives, and issues such as cybersecurity threats are keeping them up at night.[4]

Achieving successful digital transformation will only be achieved by mastering the basics first. A great customer experience, for example, needs to be based on convenience while also balancing security, privacy and consent.

Contrast that with the way some businesses onboard new customers: by having them show up at a physical location with a printed piece of government-issued ID, and/or a printed utility bill with their name and address on it. These materials can be stolen or even faked, increasing the risk that customers aren't who they say they are.

This introduces friction at a critical stage of the customer journey – the point where organizations need to foster the trust that leads to long-term loyalty and greater customer lifetime value. It also ignores the fact that customer preferences are clearly moving towards digital channels. Earlier research from Interac, for example, found that nearly seven in 10 Canadians polled (69 per cent) expect to access all government services online.[5]

There are similar risks with traditional verification processes used for employee onboarding. Onboarding a new team member should be fast, easy and secure, allowing employees to hit the ground running. With more organizations looking to hire and employ people to work from remote locations or via a hybrid working model, manual and paper-based verification creates some obvious impediments.

Canadian businesses understand this: the Interac survey conducted for this report found that eight in 10 business decision makers polled agree that digital verification solutions make their organization safer for employees, and most see verification as equally critical for both customers and employees.

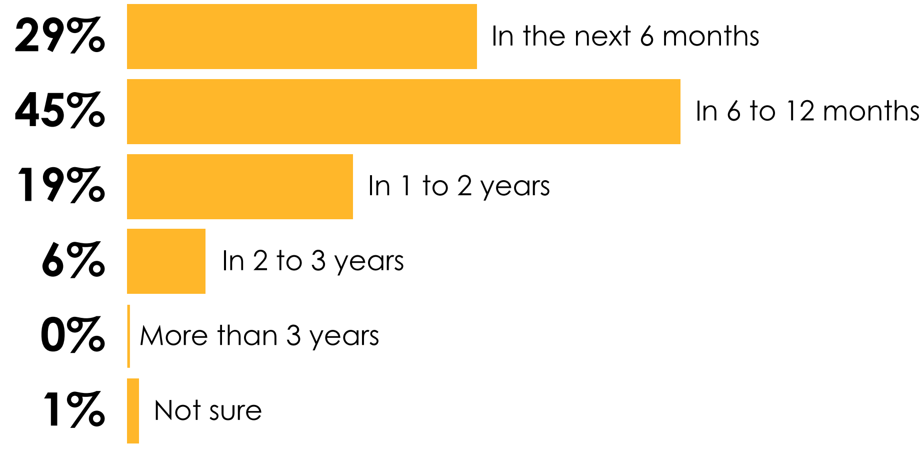
[4] https://www.randstad.ca/employers/workplace-insights/technologies/cio-priorities-in-a-dynamic-market/

[5] https://www.interac.ca/en/content/news/control-is-top-of-mind-for-canadians-when-it-comes-to-online-personal-information-according-to-new-data-privacy-week-poll/

The ability to digitally verify customer data doesn't just offer a better experience, but one in which everyone can be more confident that critical information is protected. As many organizations put more of their applications and infrastructure into cloud computing environments, malicious actors are developing ever more sophisticated ways of targeting them. In fact, a 2023 research study found that the number of successful data breaches in Canada has more than doubled in the past year.[5]

The Interac survey found that 57 per cent of surveyed business leaders are looking to adopt digital verification solutions or see value in understanding how these solutions can help their businesses. Almost half of those looking to adopt digital verification solutions will pursue these solutions in the next six to 12 months.

Almost half of businesses will pursue new digital verification methods in 6-12 months



The business case for digital verification – the "why" – is clear. A bigger challenge may be figuring out the "how." Looking at the processes and technologies in place today is a great place to start.

[5] https://www.interac.ca/en/content/news/control-is-top-of-mind-for-canadians-when-it-comes-to-online-personal-information-according-to-new-data-privacy-week-poll/

The Current Approaches to Digital Verification in Canada

When you think of terms like "customer onboarding" or "verification," what comes to mind?

For surveyed business decision makers, the answers ranged from: "Multiple data sources" to "biometrics." Others responded with thoughtful comments like, "We have to be sure information is accurate" and "It sounds like something important that any business dealing with large amounts of money should be doing."

When business decision makers were asked about their existing verification solutions, multi-factor authentication (MFA), push notifications and the use of government credentials were all on the list. But so were the use of email addresses and social media log ins. These methods were almost as common as more secure approaches:

41%

Employees have their identity verified by receiving a code or push notification to their phone or email - often known as two-factor or multi-factor authentication

40%

Customers share digital versions of government credentials with my business to access our services

40%

Customers have their identity verified by receiving a code of push notification to their phone or email - often known as two-factor or multi-factor authentication

39%

Customers access my business' services by using non-government credentials (e.g., banking details, email or social media log in)

36%

Our employees share digital versions of government credentials to access our services

33%

Employees access my business' services by using non-government credentials (e.g., banking details, email or social media log in)

5%

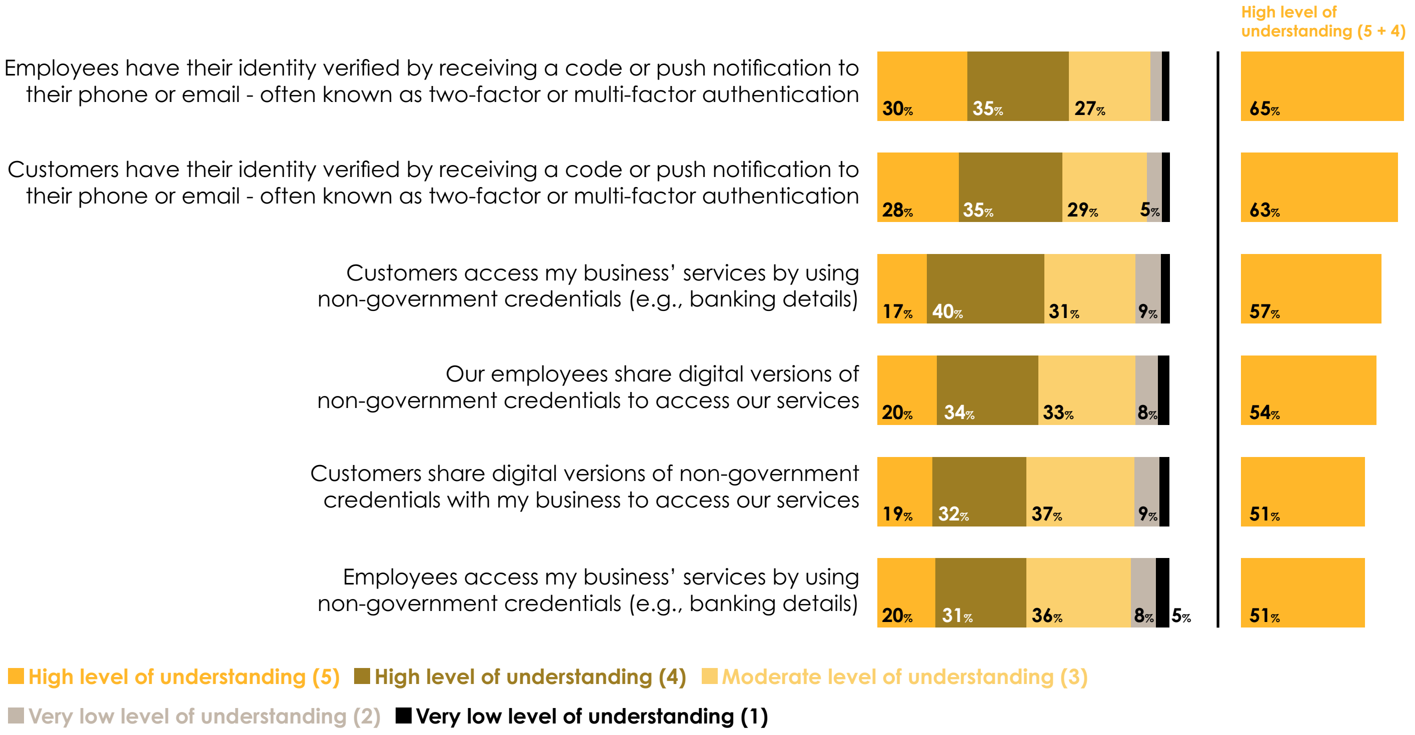
None of the above

This takes us back to the importance of trust. Businesses can't necessarily trust customer data they verify through email addresses and social media log ins, and customers don't always trust these methods either.

In the Interac Data Privacy Week poll, for instance, more than half of the respondents (58 per cent) said they use social media log ins to access online services, but only one in 10 trust these accounts with their personal information. Fifty per cent also said it was tedious to set up new usernames and passwords every time they engage with a business for the first time.[6]

[6] Ibid

Businesses have had to balance the need for verification with the impetus to stay competitive by expanding the range of digital experiences they offer customers. Those making key decisions don't necessarily have the background to distinguish between authentication and verification. It's a learning curve that the survey results suggested many business leaders have only begun to tackle.



Improving the understanding among business leaders of how digital verification works would likely also help address the top barriers to adoption. These include worries around data protection, followed by lack of education around the benefits of potential solutions.

47%
Concerns about data privacy

33%
Lack of education about the benefits of these solutions

29%
Concerns about data control/ownership

27%
Our customers don't understand this type of solution

25%
Our customers don't trust this type of solution

19%
Internal politics

16%
Not a current priority

16%
These solutions are too expensive

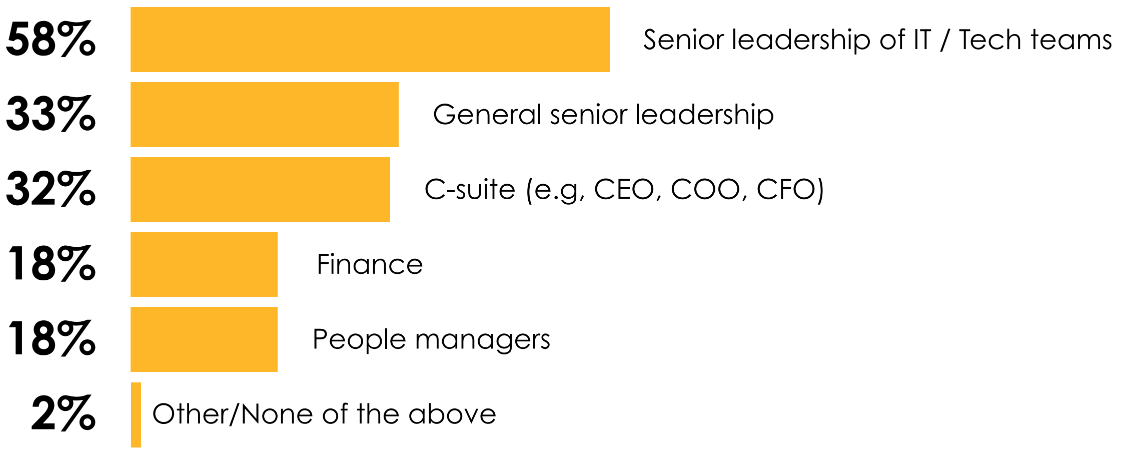
14%
Lack of demand from customers

8%
Don't trust that these solutions work as intended

9%
None of the above

Fortunately, verification solutions that leverage credentials from organizations in which Canadians report higher levels of trust, such as financial institutions, are available to support businesses of any size or industry.

Given the strategic importance of digital verification to businesses, there needs to be greater involvement from those who are directly responsible for the design, management and execution of customer experiences. Today, senior IT leadership are the most likely champions of digital verification, but only 32 per cent of business decision makers polled say members of their C-suite, such as the CFO, are involved in these discussions. That may need to change as digital verification becomes deeply woven into essential business processes.



As with any other area in which business and IT collaborate, the first item on the agenda is creating a vision for what the end state should look like.

Verification Reimagined: The Ideal Outcomes Businesses Want

Being customer centric is about more than offering relevant products and services to your ideal audience. It also goes beyond simplifying the process of buying and getting support after a purchase.

Customer centricity is about putting the people you're serving in control. It's designing experiences so they can interact through the channels they want, only using their personal information with their explicit consent, and shifting the way you engage with them as their preferences change. It also means treating customer information with the same protection you would use for any critical asset. The survey shows that 57 per cent of business decision makers agree that improving customer experience by enabling easier access to services is an appealing feature of digital verification solutions.

> **The consumer demand for digital interactions is only increasing, which means any business or organization that requires an element of in-person or paper-based onboarding is at risk of losing customers who are seeking out online, digital-first solutions. Businesses of all types need to be thinking about how they're going to enable their customers to interact with them digitally while also upholding the safety of their personal data.**
>
> **Neil Butters,**
> ***Vice President of Product,* Interac *Verified***

Digital verification is a fundamental part of customer centricity and gives customers options for how to verify or authenticate their personal information. It's an approach that works in everyday situations, like trying to access tax information from the government, booking air travel or providing accreditations to a potential employer during the hiring process.

Customer centricity was a clear priority in the survey results, where improving the customer experience was second only to the security of customer and employee data in terms of the most appealing verification features.

61%	Improving security of customer data
57%	Improving security of employee data
52%	Improving the customer experience by enabling easier access to services
52%	Improving the employee experience by enabling easier access to services
47%	Protecting our business against data breaches
47%	Reducing risk of fraud or inaccurate information being shared
33%	Maintaining compliance with regulations or data security standards
27%	Cost savings relative to in-person/physical verification and authentication
24%	Connection to national standards or verification systems
23%	Offering customers innovative ways to access existing and new digital services
2%	Don't know

That wasn't all, though: significant proportions of those surveyed want verification solutions that assist them in staying compliant with their industry regulations, reducing the risk of fraudulent activity, and saving costs compared to more manual ways of ensuring customers are who they say they are.

Nearly half of business leaders polled (47 per cent) also saw digital verification as a way of protecting against data breaches. Offering digital verification that bolsters trust could be a point of competitive differentiation among some industry sectors.

This raises another key consideration: whether Canadian businesses will present digital verification methods under their own brand, or that of a vendor brand. Again, the research was clear: Nearly 70 per cent of survey respondents who use digital verification either deliver digital verification under a vendor brand or have a vendor endorse it.

Why? According to survey respondents, using a vendor brand is more convenient. It also sends a valuable message to customers: "It appears to be a safer form and shows that a third party is involved in the security process," as one respondent said, while another added, "It ensures accountability and responsibility."

Delivering digital verification methods under a trusted vendor brand may also reflect the fact that Canadians access many different online services from many different organizations, often in a single day. The name recognition of a vendor brand can provide peace of mind and further strengthen the trust associated with the company delivering the digital verification service. Instead of wondering and worrying, customers can focus on getting the value they're looking for from the online services they're using.

Key Steps to Developing a Digital Verification Strategy

While the way forward may differ from one company to another, the following best practices can help position you for success:

Bring the right stakeholders into the mix

As noted earlier, technology deployments tend to achieve optimal results with both IT and business leaders at the table. Don't stop there, though: consult with those on the frontlines who will be assisting customers with digital verification processes and answering their questions. The better everyone understands the objectives and roadmap at the outset, the more likely you'll be able to deliver a consistent, streamlined customer experience.

Align on the most relevant KPIs

Is digital verification a way to boost operational efficiency? To decrease costs? What about enhancing the integrity of the services you're delivering by reducing fraud? Some companies might say "all of the above," but clarifying the key performance indicators (KPIs) associated with a digital verification initiative will help keep the project focused and results-driven.

Develop a trusted partnership

Vendor relationships need to encompass more than a financial transaction. Look for a company whose vision and core principles align with those of your own organization. You want a digital verification solution provider who leverages market-leading technology and partnerships, has a proven track record in operational excellence and constantly builds their capability to support future verification needs as they emerge.

Establish open and ongoing feedback mechanisms

Many companies already conduct routine customer surveys to gauge satisfaction and identify any areas for improvement. Think about adding questions that show the way digital verification is contributing to a more positive experience. Do the same thing with any employee experience surveys you run, especially after onboarding a new hire.

Conclusion

As more companies take advantage of the benefits of digital verification solutions, they can also routinely assess their progress and determine how to further improve operations.

This might include a mixture of both business-oriented KPIs (such as cost) and IT-oriented metrics, such as fewer IT security incidents and real-time fraud detection.

Ultimately, success with digital verification is largely predicated on having the best possible solution suite to meet your business needs. *Interac* Verified provides a suite of solutions that enable Canadians to digitally verify their data to access services offered by participating businesses and governments and provides a trusted network to help improve the lives of Canadians.

Digital verification has the potential to allow Canadian businesses to offer more efficient access to services, provide customers greater choice over how they share their data and redefine what it means to offer an outstanding experience. Visit Interac.ca/verified to learn more about *Interac* Verified.

Methodology: A 15-minute online survey was administered from March 10 to 20, 2023 by RepData.

The survey was administered to a pool of full-time Business Decision Makers (BDMs) across Canada. A total of 299 BDMs completed the survey.

For more information on verification, visit
interac.ca/verified

Published August 2023

Copyright 2023 Interac Corp. All rights reserved.
®™ are owned by Interac Corp.