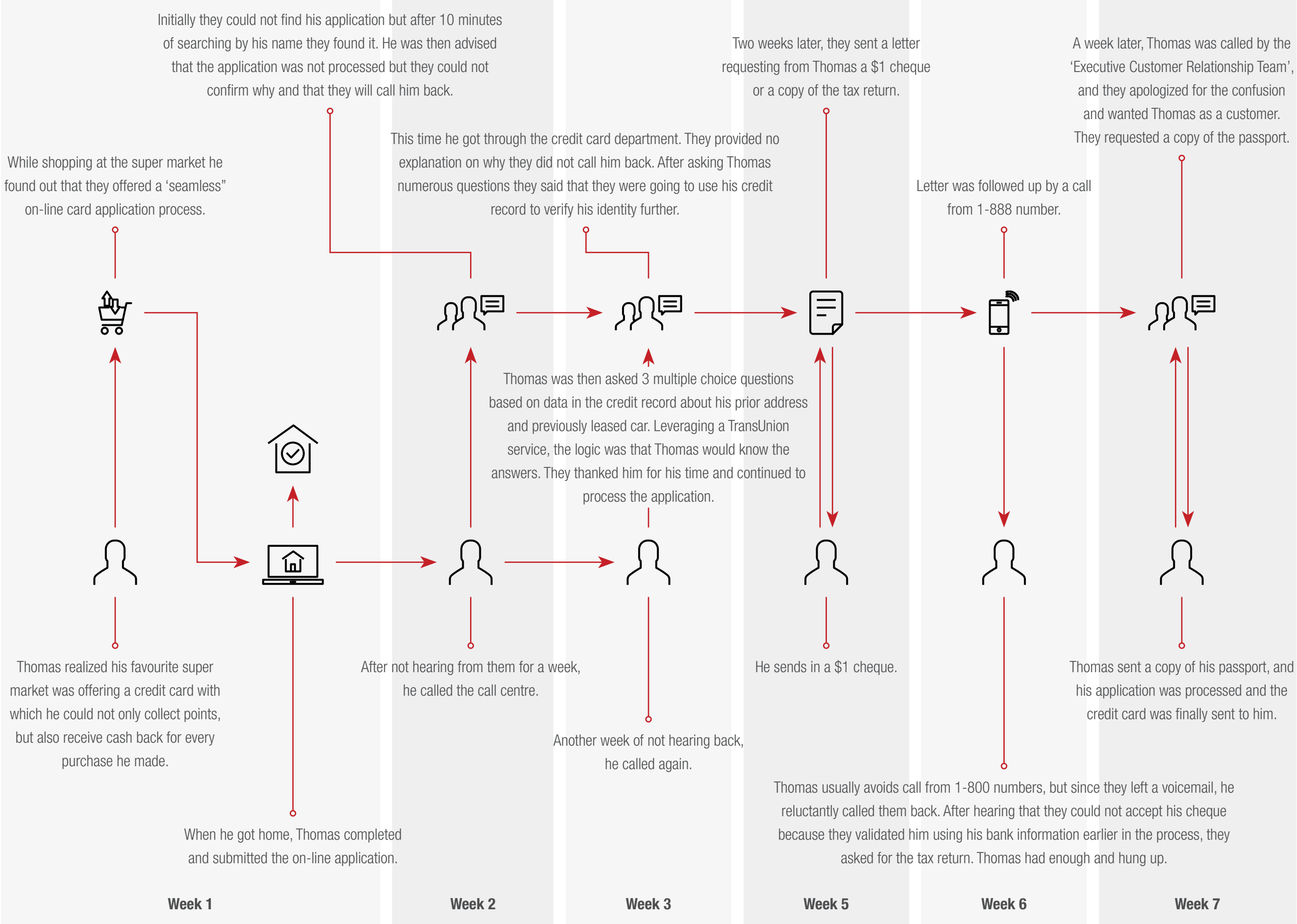
CAPCO

FUTURE OF IDENTITY VERIFICATION IN FINANCIAL SERVICES

PERSONA

This is a real-life customer journey scenario. Thomas tried to obtain a credit card from his favourite super market. Unfortunately the company mismanaged validating his identity and therefore his application, leading to a very poor customer experience.



Week 1

While shopping at the super market he found out that they offered a 'seamless" on-line card application process.

Thomas realized his favourite super market was offering a credit card with which he could not only collect points, but also receive cash back for every purchase he made.

When he got home, Thomas completed and submitted the on-line application.

Week 2

After not hearing from them for a week, he called the call centre.

Initially they could not find his application but after 10 minutes of searching by his name they found it. He was then advised that the application was not processed but they could not confirm why and that they will call him back.

Week 3

Another week of not hearing back, he called again.

This time he got through the credit card department. They provided no explanation on why they did not call him back. After asking Thomas numerous questions they said that they were going to use his credit record to verify his identity further.

Thomas was then asked 3 multiple choice questions based on data in the credit record about his prior address and previously leased car. Leveraging a TransUnion service, the logic was that Thomas would know the answers. They thanked him for his time and continued to process the application.

Week 5

Two weeks later, they sent a letter requesting from Thomas a $1 cheque or a copy of the tax return.

He sends in a $1 cheque.

Week 6

Letter was followed up by a call from 1-888 number.

Thomas usually avoids call from 1-800 numbers, but since they left a voicemail, he reluctantly called them back. After hearing that they could not accept his cheque because they validated him using his bank information earlier in the process, they asked for the tax return. Thomas had enough and hung up.

Week 7

A week later, Thomas was called by the 'Executive Customer Relationship Team', and they apologized for the confusion and wanted Thomas as a customer. They requested a copy of the passport.

Thomas sent a copy of his passport, and his application was processed and the credit card was finally sent to him.

Figure 1 – 2020 Identity Verification Client Experience

This is a real-world example of a recent client experience with a Canadian supermarket offering basic financial services to its clients. Even in 2020, with numerous advanced identity validation possibilities, clients can still experience scenarios such as this. This not only deters them from obtaining products and services from financial services companies, but it leaves providers of services and products without realized revenues.

INTRODUCTION

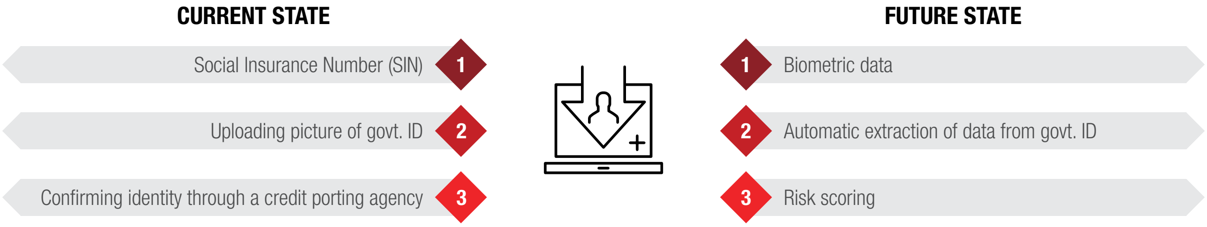
Protecting the client's identification has always been one of the top priorities for financial institutions (FIs). Over the years, these institutions continued to develop new products and services. The growth of these organizations meant that they were going to be servicing clients across multiple business lines. Two areas that have experienced tremendous growth in the past several decades are insurance and wealth management. From a wealth management perspective, what once was a traditional advisor-client model, has, over time, morphed into multiple business lines with many offerings. Most Canadian banks offer several options of the traditional several advisor-client models. These models include IIROC registered advisors catering to clients with more complex investment needs and MFDA registered advisors who offer more plain vanilla mutual fund offerings. Also, both banks and independent firms developed self-serve discount brokerage models, as well as robo-advisor offerings. Recently, on a global level, we have seen an expansion of hybrid service models as well.

On the insurance side, as the middle class grew, the appetite for hard assets grew. Those assets need to be insured. On the personal front, people became more accustomed to buying life and health (L&H) and property and casualty (P&C) insurance policies to protect themselves and their families from unfortunate events. Additionally, the need for a seamless digital experience is growing, where customers like to get everything done from the comfort of their homes. With this growing trend came new business models developed to acquire new clients and drive revenues and profits. It also meant new client touchpoints with insurance providers, log-ins and passwords required for client servicing.

In parallel with these businesses' growth, we have seen the demand and growth of digital capabilities grow over the past several years. With consumers' lives becoming more dependent on digital platforms and experiences came more opportunities for fraud, online scams, and identity theft. Financial institutions are not immune to hackers or cyberattacks. Identity theft has become one of the top priorities for financial institutions as hackers' fraudulent actions expose their client's assets and increase the institution's liabilities. Cybersecurity continues to be on top of mind for many financial institutions.

CURRENT STATE - WHAT ARE CANADIAN FINANCIAL INSTITUTIONS DOING?

Even in 2020, Canadian banks and their online competitors tend to use clients' Social Insurance Numbers (SINs) to confirm their identity through credit reporting agencies[1]. Some require a SIN and a government ID to be uploaded. Given that SINs are accessible via numerous databases, clients are left exposed. In particular, auto insurance companies have also been using government ID to pull third party reports, such as AutoPlus and MVR, to verify clients and their driving history. Security questions are another common method of verifying identity digitally. However, it is not considered a very secure solution because answers to some questions can be easily guessed or discovered. Multi-factor authentication (MFA) is another method that organizations use to verify clients' identities while logging into applications, online accounts, etc. However, 'trusted devices' set up as a part of MFA can get into the wrong hands and leave the organization exposed to fraudulent activities. Verified.me is another solution being used in Canada. Verified.me allows customers to share their personal information with their "connections," such as banks, to verify their identity quickly by leveraging their technology. Most Canadian banks use the technology; however, it is yet to be fully adopted by the insurance companies and wealth managers[2]. This technology works by allowing users to log-in to their online accounts using their log-in credentials from another financial institution's account. For instance, by logging-into their CRA account, an individual can utilize their online banking credentials, which raises privacy concerns among users. Companies have started experimenting with new technologies that can be more secure without compromising client experience. While technological trends are pushing the evolution of identity validation and management to become more remote, there are challenges in adopting these technologies. Some of the technologies available are biometrics, risk scoring and automatic extraction of data from government IDs (e.g., driver's license). Even though these solutions are available, organizations need to determine how to adopt these technologies and ensure that they are not exposing themselves to more risk?



CURRENT STATE

Social Insurance Number (SIN) 1

Uploading picture of govt. ID 2

Confirming identity through a credit porting agency 3

FUTURE STATE

1 Biometric data

2 Automatic extraction of data from govt. ID

3 Risk scoring

Figure 2 – Client identification: current state vs. future state

WHY SWITCH TO DIGITAL IDENTITY VALIDATION?

Hacking of personal information online as well as identity theft are common topics in the news. Synthetic ID fraud is also an on-going issue, where fraudsters create synthetic identities online by using legitimate social security numbers and fabricated personal information (such as name, email, etc.). These risks deter both individual consumers and firms from performing identity validations digitally. While the client convenience and overall process efficiency are obvious reasons to initiate digital identity validations, there are other reasons to do so and best practices that organizations can implement to counter digital identity validation risks.

From a client's perspective, there are several benefits. Clients can open accounts or obtain insurance policies from the comfort of their homes. Rather than meeting their wealth managers or their insurance provider, they can do everything from their smartphone. Saving time during a busy schedule is everyone's top priority. In addition, having a great customer experience that is seamless, safe and addresses all the client's risk concerns while saving time is beneficial for the client.

From the service provider's stance, wealth management firms, banks and insurance companies can provide a seamless digital experience to their clients and reduce fraud. Enabling digital capabilities also increases efficiencies that allow employees to shift their focus from manual processes and improve their productivity.

Furthermore, it is 2020, and it is simply time to evolve. We have seen organizations' efforts to move to cloud-based solutions, such as software as a solution (SaaS) and data as a software (DaaS) solution. Financial services organizations move away from manual processes where possible, making their organizations leaner with technology playing a more prominent role. They are also seeking to use remote platforms and find ways to move away from using legacy platforms that are more difficult to integrate. What should inspire confidence is that these types of solutions are growing in the market and that vendors are looking to develop these types of solutions and are developing solutions with better customer experiences and stronger security features. With vendors putting in both human capital and financial investments behind these solutions, we expect to see more resilient solutions to cyber risk and threats. Moreover, with economies moving to online work, and as this is becoming a new norm, moving towards digital identity validation is inevitably a must.

We will highlight some additional benefits of remote identity validation and how organizations can mitigate risks that come with it.

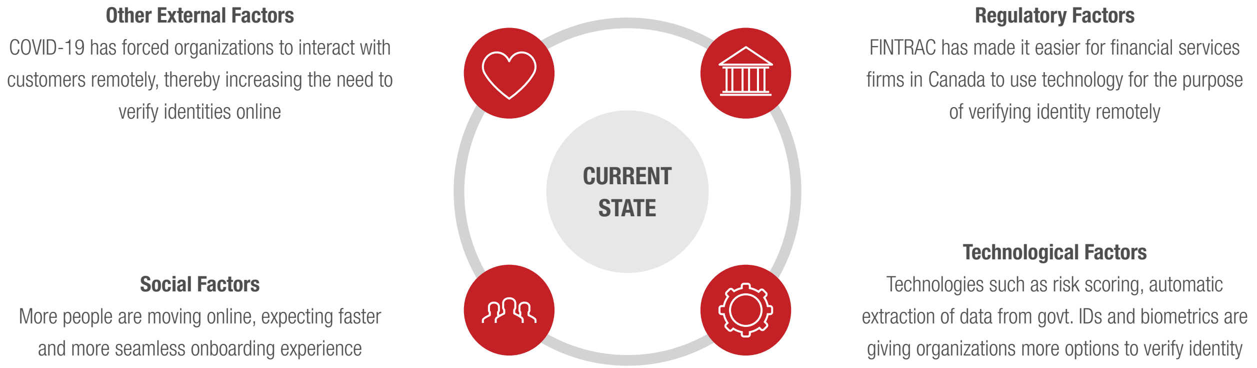
- **Minimize Fraud:** As mentioned earlier in this paper, there is always a risk of fraudulent activity when individuals are identified online. However, organizations can reduce fraud by ensuring a balance between security and client experience. For example, auto insurers can build a capability for prospects to upload a picture of their drivers' license instead of asking them to fill this information in. In this case, you improve client experience because prospects are no longer required to manually enter this information. At the same time, security is not compromised because the image of the driver's license can be analyzed for its authenticity. Organizations can go even further and ask the prospect to upload an image of oneself in real-time to ensure that the image matches the face on the ID. Since taking a 'selfie' only takes seconds, security is not compromised for the sake of client experience. This is not only limited to the insurance world. Banks and wealth management firms can also do the same when verifying identity online.

- **Identity Data and Analytics:** Enabling remote identity checks will bring organizations one step closer to a complete digital experience. This will allow them to gather useful insights on clients' identity, location and devices, which will improve their risk models and ability to detect fraud overtime. This will further enable the organization to provide a more tailored identity verification process to different types of clients. An example is a quick and streamlined process for low-risk clients but a longer multi-step process for high-risk clients.

- **Preferences Management:** Client preferences allow organizations to deliver a personalized experience and, most importantly, gives clients control over some aspects of their journey. Similarly, enabling remote identity verification will provide clients and prospects with another option to complete the process from the comfort of their homes. There will still be clients who would prefer to meet an advisor in-person to verify their identity and make the purchase. Still, they will have an option to complete this process remotely if something changes and they are unable to physically go to a branch. Organizations can also benefit from this by capturing insights about what percentage of clients use this feature and their demographic details, which is another step towards a highly personalized experience.

FACTORS INFLUENCING THE ADOPTION OF REMOTE IDENTITY VERIFICATION

Like any other change, the switch from in-person to remote identity verification is bound to be impacted by various factors. These factors will determine how organizations enable this technology and how consumers respond and adapt to it.



Other External Factors
COVID-19 has forced organizations to interact with customers remotely, thereby increasing the need to verify identities online

Regulatory Factors
FINTRAC has made it easier for financial services firms in Canada to use technology for the purpose of verifying identity remotely

Social Factors
More people are moving online, expecting faster and more seamless onboarding experience

Technological Factors
Technologies such as risk scoring, automatic extraction of data from govt. IDs and biometrics are giving organizations more options to verify identity

Figure 3 – Factors influencing the adoption of remote identity verification

Other External Factors: Covid-19

As we write this paper, the world is in a nine-month battle with the COVID-19 pandemic. While different countries have taken different measures, the impact on the world thus far has been tremendous. The first thought is the death toll and the pressure and over-taxation on the health systems globally. In addition, shutdowns have caused economic slowdowns that produced higher jobless rates, and the full impact on economies remains to be seen. The U.S. alone has witnessed the highest unemployment post-World War II[3]. Canada also witnessed high jobless claims, as there were two million Canadians out of work in April 2020[4]. That said, we are left wondering what this world will look like as a result of this pandemic. We cannot ignore the fact that businesses will have to find a way to function and continue their existence.

Businesses will have to find ways to operate more remote than ever. This will have a limited impact on marketing and offering products but a huge impact from a daily business operations perspective. Therefore, in the case of financial services firms, that will mean gaining new customers online. As there is a possibility of brick and mortar businesses to go down in numbers, and for physical locations for wealth managers and insurers to become a smaller part of their operating business models. These changes will also mean that identifying and verifying new customers will have to be done remotely. Firms will not have a choice but to explore solutions to help them identify new clients remotely, safely, and seamlessly.

Regulatory Factors

Governments are also realizing the importance of better customer experience and are changing standards that make it possible, such as enabling remote identity verification. Recent changes to anti-money laundering rules in Canada have been amended to use ‘authentic’ documents to verify identity, rather than just ‘original.’ So now clients can send in copies of their IDs to have their identity validated remotely[5].

FINTRAC, the regulator overseeing anti-money laundering (AML) related activities in Canada, allows financial institutions (FIs) to use technology to verify identity remotely. For example, ask clients to scan and send a picture of their government ID using their smartphones. The organization should then assess the validity of the ID by comparing visual features, security indicators, or any markers. Lastly, this should be supported by evidence that the client sharing the ID is, in fact, the same person listed on the ID. This can be done by a live video stream or sharing a real-time “selfie” along with the ID[5].

Technology Factors

With an increasing focus on improving client experience, several technological trends shape the space of remote identity validation. Increasing innovation in this space should encourage financial services organizations to invest in these technologies and evolve with their customers’ changing needs. Some of these technological trends include – biometrics, risk scoring and automatic data extraction from government IDs[5].

- **Automatic Data Extraction from Government ID.** Extracting data from an image of a client’s government ID is one of the popular ways that remote identity verification is being completed. It involves asking the client to scan a picture of their government ID using their smartphone, which is then processed to complete data extraction by the organization. In the background, the image of the ID is automatically analyzed for its authenticity and pre-fill some of the required client information (e.g., name, date of birth, etc.). The biggest benefit of using this tool is eliminating the need for any face-to-face interaction or even phone calls.

- **Biometrics.** Smartphones today have made the process of capturing a piece of a user’s biometric data effective and seamless. It is also being adopted in the financial services industry in cases where users can now log into their online banking account using a fingerprint scanner or facial recognition on their smartphones. Organizations can go even further and use this technology to validate the identity of their clients. For example, capturing an image of the client's face in real-time or asking them to upload a live video of their face can complement the copy of their government ID to provide another layer of verification. Some financial institutions have already started experimenting with this capability. For instance, a global bank now allows its business clients to send selfies, which are verified against a picture of their government ID using facial recognition software[6].

- **Risk Scoring.** This process involves assigning a score to a client or prospect's identity, which indicates how likely they are to commit identity fraud. To do so, personal information, online behavior and online presence from high-quality data sources are analyzed to find inconsistencies and assign a composite risk score. The idea is that the more inconsistent an individual's information across different sources is, the more likely they are to misrepresent their identity.

Social Factors

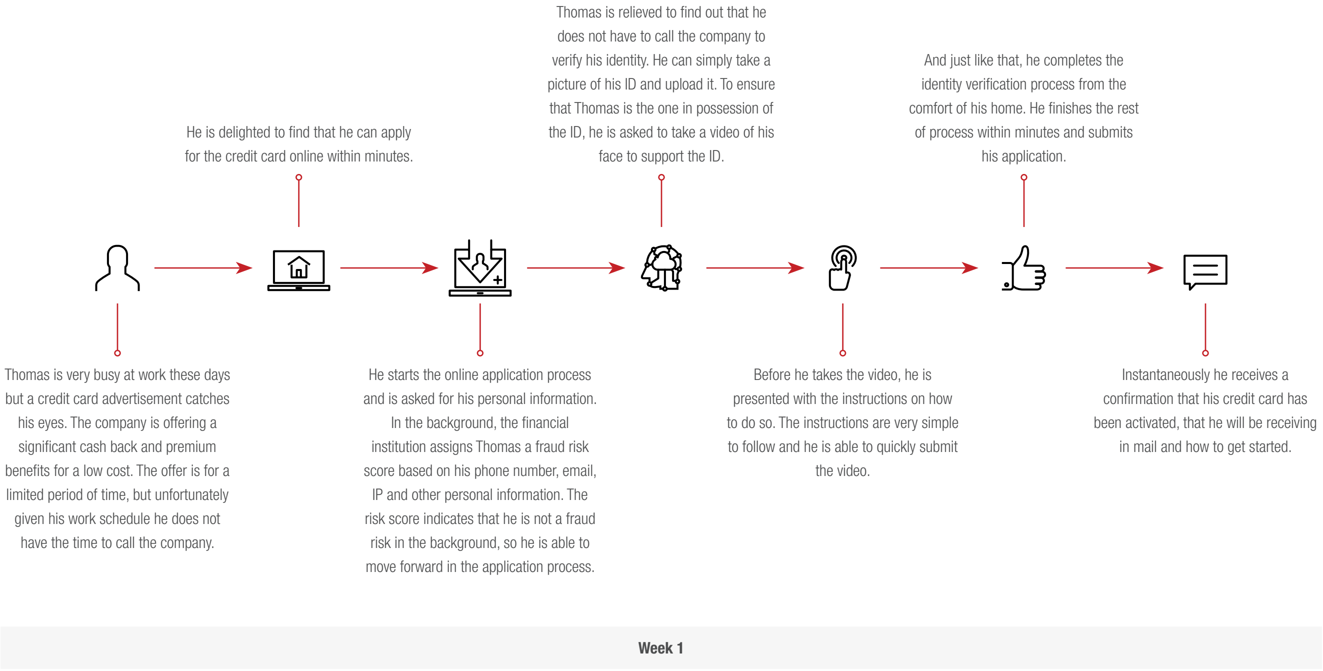
One of the social benefits of remote identity validation is that it provides a convenient way for customers to verify their identity from the comfort of their homes and at a time that works for them. With increasing mobile transactions and decreasing in-person visits to brick and mortar locations, technologies that can allow individuals to complete transactions from their home's convenience are highly sought after. We believe that these initiatives will become a higher priority for organizations, given the current global situation with the COVID-19 pandemic. This creates a big opportunity for financial services institutions to implement these solutions and get them to market faster.

Additionally, internet and smartphone usage has been on an upward trajectory in Canada in the last few years, indicating that technologies offered over these mediums show signs of potential. According to Statistics Canada, in 2018, over 90 percent of Canadians had internet connectivity in their homes, and 88 percent of these used smartphones to conduct online activities, including online banking[7]. This trend, coupled with the convenience of artificial intelligence (AI) and analytics-driven tools, will allow consumers to adopt these technologies faster.

Consumers of both wealth and Insurance products are starting to expect faster onboarding with digital tools that streamline AML and KYC checks. Remote identify verification fits perfectly in this space by offering clients a way to complete these checks using their smartphones. Upcoming fintechs and insurtechs offer a digital onboarding experience to consumers, making it more convenient for them to complete their purchase. Lemonade, a US-based P&C insurtech, allows users to get a quote and bind their policy within minutes[8]. This should motivate traditional FIs to move in a similar direction by using tools that enable remote verification checks.

The future of remote identity verification could bring a social challenge as well. Biometric data typically includes pictures of people's faces or their fingerprints, which may cause reluctance to share this information with financial institutions. Financial institutions have traditionally been a prime target for data breaches and add fuel to the fire. However, implementing a strong cybersecurity program by capturing and verifying identity in a secure way can help counter this challenge. Additionally, educating clients about how this data will be used and stored when they explore this service can also help alleviate some of that reluctance.

The following is a customer journey that shows how identity validation could be completed in future-state, given the best practices and tools discussed in this paper.



Thomas is very busy at work these days but a credit card advertisement catches his eyes. The company is offering a significant cash back and premium benefits for a low cost. The offer is for a limited period of time, but unfortunately given his work schedule he does not have the time to call the company.

He is delighted to find that he can apply for the credit card online within minutes.

He starts the online application process and is asked for his personal information. In the background, the financial institution assigns Thomas a fraud risk score based on his phone number, email, IP and other personal information. The risk score indicates that he is not a fraud risk in the background, so he is able to move forward in the application process.

Thomas is relieved to find out that he does not have to call the company to verify his identity. He can simply take a picture of his ID and upload it. To ensure that Thomas is the one in possession of the ID, he is asked to take a video of his face to support the ID.

Before he takes the video, he is presented with the instructions on how to do so. The instructions are very simple to follow and he is able to quickly submit the video.

And just like that, he completes the identity verification process from the comfort of his home. He finishes the rest of process within minutes and submits his application.

Instantaneously he receives a confirmation that his credit card has been activated, that he will be receiving in mail and how to get started.

Week 1

Figure 4 – Future Identity Verification Client Experience

CONCLUSION

Given all the factors considered, remote identity verification is here to stay, and we firmly believe that it will become more prevalent. We see the main drivers of this trend to be the current social norms and the fact that our lives are heavily dependent on technology. The future customers will expect remote access to all their products and services, and hence will be more open to being identified remotely as well. Although there is no single way to eliminate all risks regarding digital identity validation, organizations can explore ways to leverage different combinations of methods to mitigate risks. In order to have a structured approach to remote identity verification, firms should consider the following:

1. Explore remote identity verification solutions
2. Perform initial assessments on their current state
3. Understand and analyze how these new tools can be integrated into their existing business
4. Review vendor and solutions options available in the market
5. Partner with a trusted advisor to formulate target state, deliver and implement the solution

Some key best practices that need to be considered are:

1. Using a mix of solutions: For instance, not just capturing government ID, but also supporting that with picture or video of customer's face. In addition, supporting it with fraud risk scoring – IP, email, and phone number scoring.
2. Security of the data being captured (especially biometric) while explaining why the data is being captured and how it will be stored.
3. Make the solution flexible across multiple devices.

The idea of drones flying to car accident sites to assess damages would have seemed far-fetched a few years ago, but this is reality now. As technology evolves, the factors we listed will become more prevalent and some of these new realities will come to life. Firms should start assessing how they will develop capabilities to perform digital identity validation as well as how it will impact their business model.

SOURCES

1. https://www.cibc.com/en/privacy-security/privacy-policy/faq.html

2. https://verified.me/#:~:text=Network%20Participants&text=The%20Verified.Me%20service%20was,%2C%20RBC%2C%20Scotiabank%20and%20TD

3. https://www.ft.com/content/11ea56b0-cf02-4b14-8b50-8f1f3c6abdb8

4. https://business.financialpost.com/news/economy/canada-lost-almost-two-million-in-april-jobless-rate-soars-to-13

5. https://www.fintrac-canafe.gc.ca/guidance-directives/client-clientele/Guide11/11-eng

6. https://www.cnbc.com/2016/09/05/hsbc-customers-can-open-new-bank-accounts-using-a-selfie.html#:~:text=HSBC%20business%20customers%20can%20now,a%20driver's%20licence%20or%20passport

7. https://www150.statcan.gc.ca/n1/daily-quotidien/191029/dq191029a-eng.htm

8. https://www.fastcompany.com/3068506/lemonade-is-using-behavioral-science-to-onboard-customers-and-keep-them-hones

AUTHORS

Nick Jackson, Partner
Nick.Jackson@capco.com

Tijil Dewan, Associate
Tijil.Dewan@capco.com

ABOUT CAPCO

Capco is a global technology and management consultancy dedicated to the financial services industry. Our professionals combine innovative thinking with unrivalled industry knowledge to offer our clients consulting expertise, complex technology and package integration, transformation delivery, and managed services, to move their organizations forward.

Through our collaborative and efficient approach, we help our clients successfully innovate, increase revenue, manage risk and regulatory change, reduce costs, and enhance controls. We specialize primarily in banking, capital markets, wealth and asset management and insurance. We also have an energy consulting practice in the US. We serve our clients from offices in leading financial centers across the Americas, Europe, and Asia Pacific.

To learn more, visit our web site at **www.capco.com**, or follow us on Twitter, Facebook, YouTube, LinkedIn and Instagram.

WORLDWIDE OFFICES

APAC
Bangalore
Bangkok
Gurgaon
Hong Kong
Kuala Lumpur
Mumbai
Pune
Singapore

EUROPE
Berlin
Bratislava
Brussels
Dusseldorf
Edinburgh
Frankfurt
Geneva
London
Munich
Paris
Vienna
Warsaw
Zurich

NORTH AMERICA
Charlotte
Chicago
Dallas
Hartford
Houston
New York
Orlando
Toronto
Tysons Corner
Washington, DC

SOUTH AMERICA
São Paulo

WWW.CAPCO.COM

CAPCO