Sycurio.

Why secure payments are the key to omnichannel retail success.

Introduction.

The rise of ecommerce over the past several years has brought forth a new era of omnichannel retail. For retailers today, having an ecommerce website is merely table stakes.

Every brand, merchant and retailer must now be able to operate seamlessly through every possible communication channel – from the physical store to the website, via mobile app, social media platforms, phone, SMS text messages and more.

Omnichannel retail means being able to meet customers in the channel of their choice and allowing them to complete any type of transaction in that moment. Yet, as retailers have been diligently working to digitally transform themselves in order to become a more omnichannel business, consumer concerns around data security and privacy in many of these channels is holding back further growth.

To gain first-hand insight into consumers' level of confidence surrounding payments and data security through various retail channels, Sycurio commissioned a survey of 1000 North American consumers. It revealed that while ecommerce and social shopping are on the rise, consumer confidence in the security of omnichannel payments is low. This negative sentiment should serve as a call to action for brands and retailers to better address payment security and increase awareness of the measures they are taking to keep their customers' personally identifiable information (PII) secure. Above all, this research makes clear that data security and privacy are the keys to further growth and omnichannel success.

The rise of omnichannel retail.

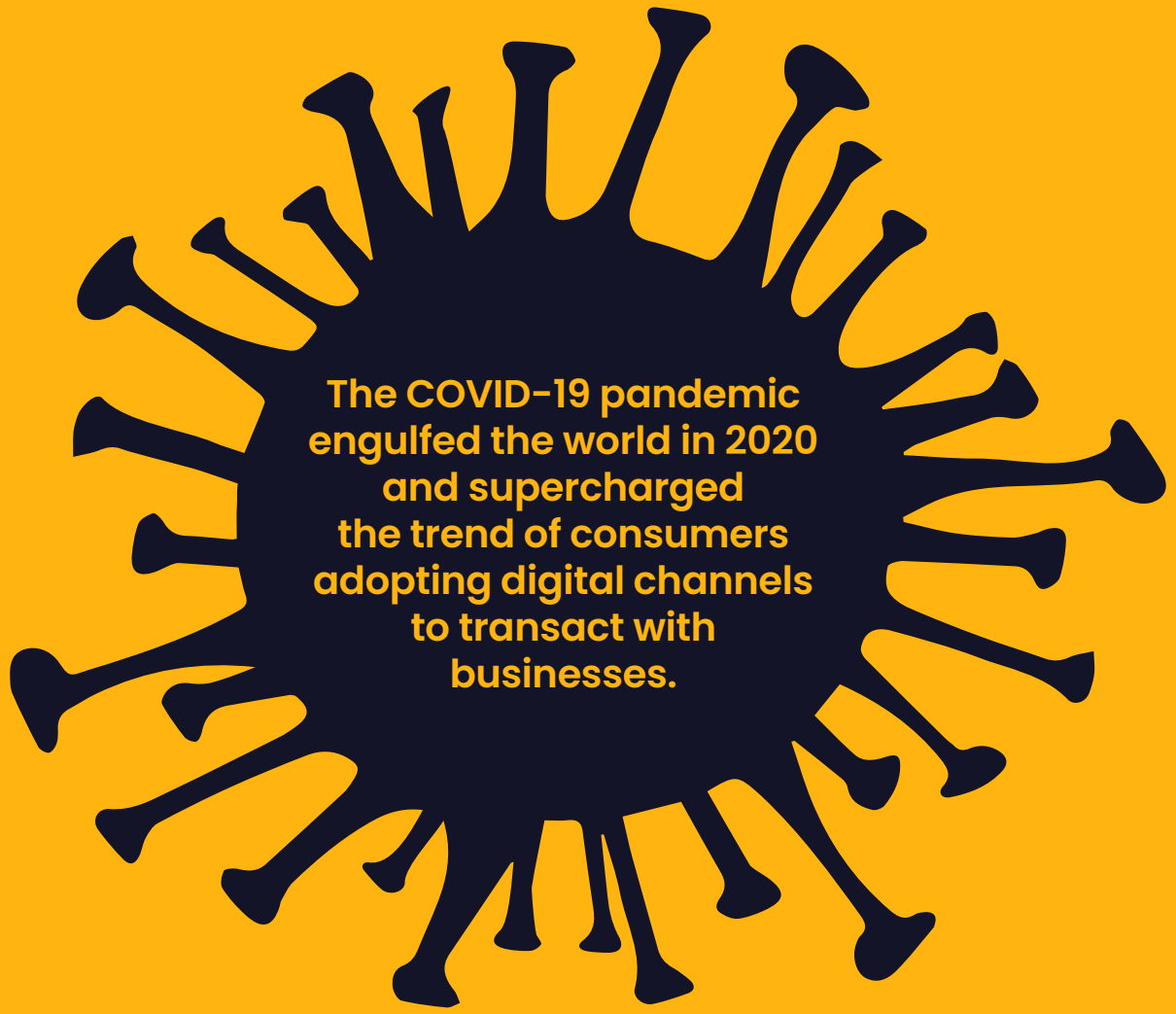
In short, consumers want a variety of options and conveniences at their disposal. For retailers to succeed in this environment, they must be able to meet their customers in whatever channel they are in at that moment and provide exactly what they want, he way they want it. This is the essence of omnichannel retail. It requires integrating all of a brand's online and offline touchpoints into one seamless operation that delivers a consistent and enjoyable customer experience across all channels, devices and touchpoints.

They might compare online prices on their smartphone while standing in front of an item in the store. They make purchases online for home delivery but expect the ability to conveniently return the item to the brick-and-mortar store if it isn't to their liking. They may engage with a retailer's chat bot on a social media platform while waiting on hold on the telephone with a customer service representative.

Previously, retail brands viewed their brick-and-mortar stores as a separate channel from their ecommerce website or their mobile application. However, today's consumer uses a mix of many different in-person and digital channels throughout their shopping journey and they expect a convenient and consistent customer experience across them all.

Over the past several years, the ubiquity of online shopping has transformed consumer behavior and fueled the rise of omnichannel retail.

Digital transformation in the retail industry had been driving the growth of omnichannel retail in recent years, but the COVID-19 pandemic that engulfed the world in 2020 supercharged the trend. As many physical stores closed and consumers avoided in-person shopping, new behaviors were formed. Online and mobile shopping for home delivery or curbside pickup increased dramatically.



According to *research from NielsenIQ*, the pandemic fueled a 50% increase in omnichannel shopping in the U.S. As these behaviors became entrenched over the course of a year, consumers will likely never return fully to the ways they shopped before. Now more than ever, they will continue to expect frictionless and convenient omnichannel options from every brand, merchant and retailer they interact with.

The pandemic fueled a 50% increase in omnichannel shopping in the US.

Pandemic pushes people to try new payment platforms.

Though these high consumer expectations might seem daunting for retailers, transitioning to an omnichannel approach brings many benefits to the retailer as well. A study by Harvard Business Review found that omnichannel customers spent more, made more repeat purchases and were more likely to make recommendations to friends and family.

In 2020, omnichannel customers spent an average of four times more than store-only buyers and 10 times more than digital-only customers.

As reported by retailer Target

Security and privacy concerns remain top of mind.

Yet even as omnichannel retail has been growing in popularity, data security and privacy concerns are holding back many consumers from taking full advantage of all the channels a retailer might provide. With widescale data breaches making headlines every day, consumers are rightfully concerned about the safety of their sensitive information, including their payment card details, when making purchases through various channels.

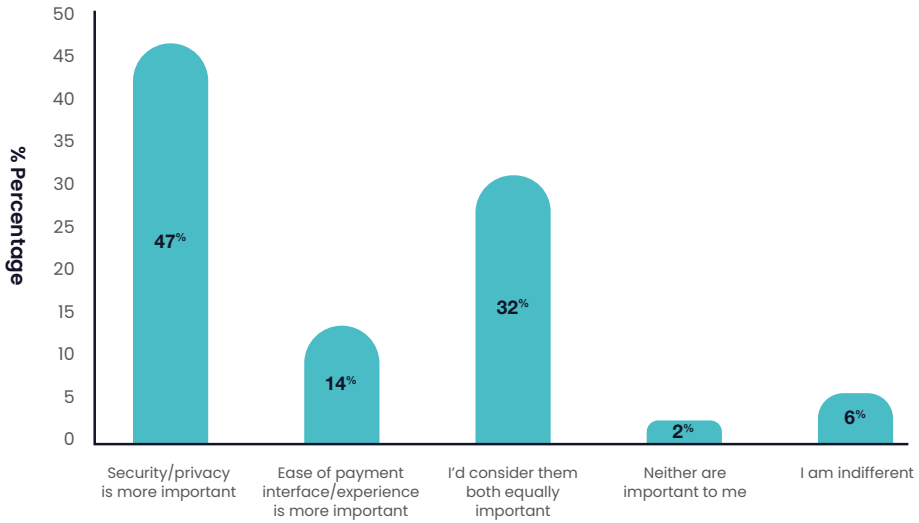
Younger generations were more likely to turn to online marketplaces for their shopping and gift-giving needs

To better understand consumers' concerns and their perceptions surrounding the security of different purchasing channels, Sycurio commissioned research with Dynata in April 2021, surveying 1000 North American consumers via online collection.

Exploring the data further, generational preferences begin to emerge. Younger generations were more likely to turn to online marketplaces for their shopping and gift-giving needs. Of those respondents ranging 18 to 34 years old, 47% plan to shop with online marketplaces for upcoming celebrations and events. Only 22% of those 55 years and older said they will shop with an online marketplace for similar needs, compared to 43% in this age group who said they plan to shop in-store for their gifting needs.

When asked which is more important during the purchasing process, consumers in our survey overwhelmingly chose data security and privacy (47%) over ease-of-use of the payment interface/experience (14%).

What do you find more important when completing a purchase: the security and privacy of your personal data or the ease of the payment interface/experience?



47%

chose data security and privacy

43%

plan to shop with online marketplaces

14%

ease-of-use of the payment interface/experience

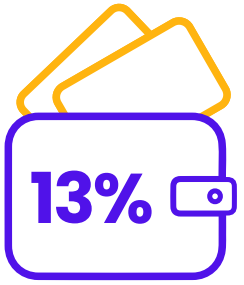
Social media isn't winning over wallets.

Consumers in our survey were particularly concerned about the data security and privacy implications of making purchases through newer digital channels, such as social media platforms. Though much fanfare has been made surrounding built-in purchasing features that social platforms like Instagram, TikTok, Facebook and Pinterest have rolled out recently, our research shows that consumers remain hesitant to use these capabilities. Only 13% of respondents said they use social media to complete a purchase, and a mere 5% said it was their preferred channel. In fact, more than half (56%) of consumers said they would not be willing to complete a transaction or provide their payment details over any social media platform.

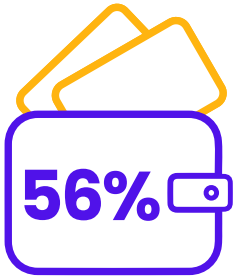
Though the majority of respondents are not willing to make purchases through social channels, as we dig deeper into the results, some generational differences do begin to emerge.

As one might expect, an overwhelming majority (nearly 80%) of consumers over the age of 65 said they would absolutely not give payment details over a social media platform. In contrast, younger generations expressed more comfort in social shopping, though there is still a great amount of reluctance even among this target market. Only 11% of those aged 25-34 and 17% of 18–24-year-olds stated that they regularly provide payment details over social channels.

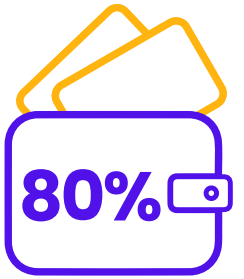
The reticence for even younger consumers to share their payment details through social platforms should signal to brands that communicating about the security of their purchase process needs to be of utmost importance. In order to win over consumers and entice future generations of shoppers to make purchases through their social channels, brands and retailers must assure their customers that their sensitive information will be kept secure.



of respondents said they use social media to complete a purchase



of consumers said they would not be willing to complete a transaction or provide their payment details over any social media platform



of consumers over the age of 65 said they would absolutely not give payment details over a social media platform

Consumer caution surrounding the phone.

It's not just newer, digital channels that consumers remain cautious of. Even traditional, long-lived channels such as the telephone raised data security concerns among consumers in our survey. Despite peoples' widespread reliance on communicating through the phone, there was a consensus of hesitation around verbally providing payment details to sales representatives or customer service agents over the phone. Our survey revealed that consumers are wary of making purchases over the phone and speaking their payment card information aloud to representatives, with just 10% of respondents saying they do so regularly. Moreover, only 18% of respondents said they have completed a purchase over the phone in the past 12 months.

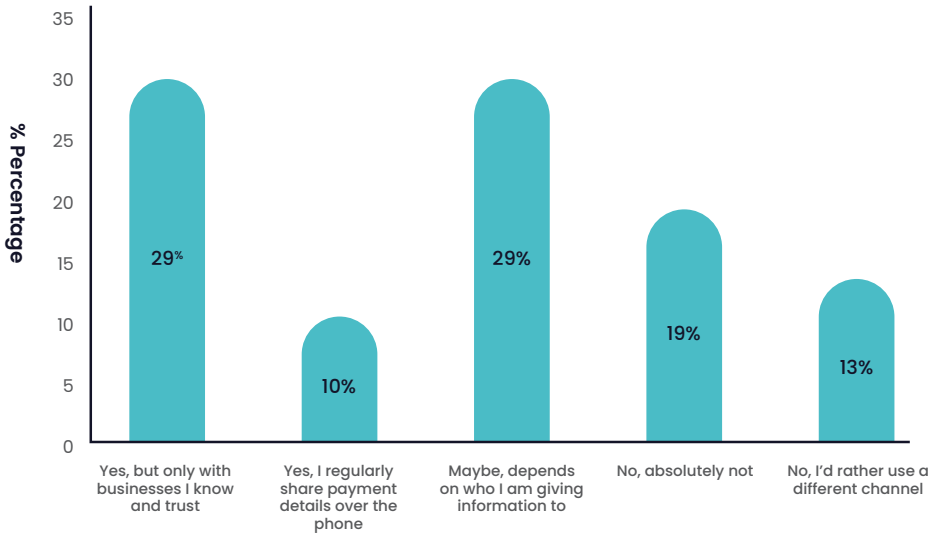
Perhaps surprisingly, the data from our survey reveals that younger consumers are making more purchases verbally over the phone than their older counterparts. Almost one-third (30%) of 18 to 24 year-olds in our survey said they will read their payment card details over the phone if it's a business they know and trust, compared to just 3.5% of survey respondents over the age of 55 saying they regularly share payment details over the phone.

30%

of 18 to 24 year-olds in our survey said they will read their payment card details over the phone if it's a business they know and trust – the most of any age group

The caution that consumers have around sharing their sensitive information over the phone is exacerbated by the knowledge that, since the beginning of the COVID-19 pandemic, many customer service representatives are now working from their homes and not in the retailer's physical contact center. Work-from-home arrangements introduce a wide variety of additional risks when it comes to unsecured customers' sensitive data. Agents may be using insecure Wi-Fi networks or personal devices that can be breached by hackers. Or, they may have housemates or family members who could overhear the phone conversation and jot down the caller's payment card details for their own use. Across the generations, all consumers remain wary of making purchases or sharing payment information via SMS text messages on mobile phones. Less than 10% of respondents said they have made a purchase this way during the past year. Text message marketing can be a highly effective communication channel and boost sales to existing customers, but retailers will miss out on this opportunity if their customers are skeptical of the security of this channel.

Would you complete a transaction and read aloud payment details over the phone?



40%

of the consumers in our survey agreed that the increase in customer care agents working from home has impacted their trust in the security of their personal payment information.

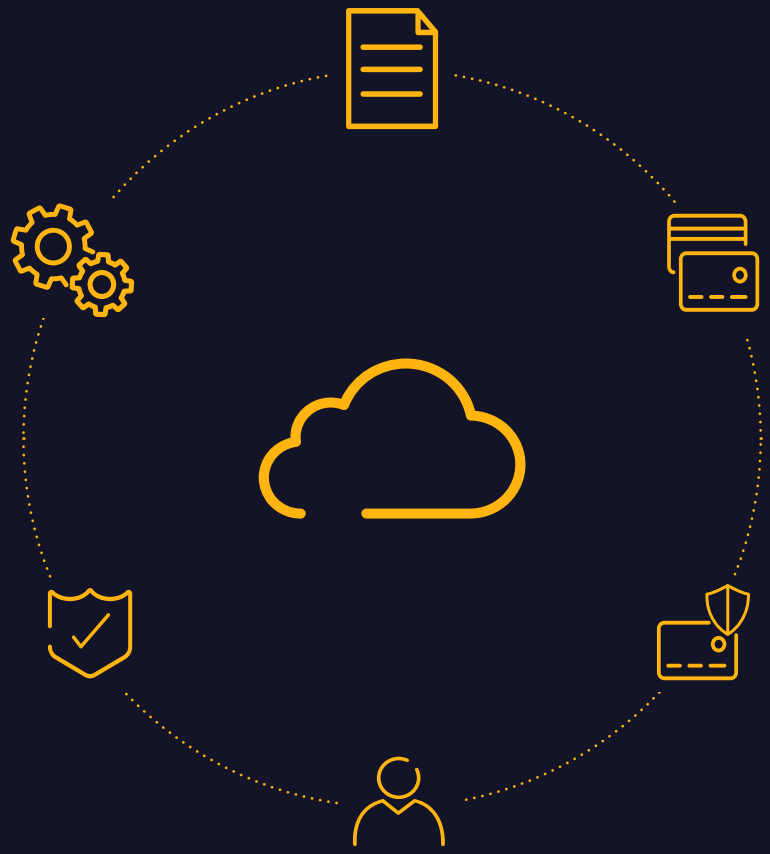
50%

of those in the 18- to 24-year-old range saying the increase in remote agents has impacted their trust.

Facing fears with strong data security.

In the rush to digitize their operations and embrace an omnichannel approach, many brands neglected to devote time and resources to educating their customers about the data security and privacy measures they have put in place to protect their payment channels. As retailers continue to aim for growth through all their channels, they will need to place greater emphasis on awareness campaigns that instill consumer confidence in the security of their payment processes.

With the right technologies and processes in place, retailers can enable safe, secure and frictionless omnichannel sales, increase revenue and attract and retain new customers. It begins with the use of secure payment platforms and adherence to the Payment Card Industry's Data Security Standard (PCI DSS).



Technology solutions such as Sycurio.Voice & Sycurio. Digital enable retailers to provide frictionless and secure payment processes across all of their digital, phone and even in-person channels.

Sycurio.Voice

Sycurio.Voice protects payments and purchases made over the telephone by allowing customers to discretely enter their payment card numbers directly into their telephone keypad rather than speaking them aloud to the agent on the line.

Using Dual-Tone Multi-Frequency (DTMF) masking and encryption, Sycurio.Voice securely routes the sensitive payment card data directly to the Payment Service Provider (PSP) for processing.

In an age where agents are often working from home, consumers can rest assured that if a retailer is using Sycurio.Voice, their payment information is never handled by the agent and is not being transmitted over an insecure home network or overheard by an eavesdropping housemate.

What's more, the agent can remain on the line with the customer throughout the payment process, helping them troubleshoot if necessary, while never hearing or seeing the cardholder data.

Sycurio.Digital

Similarly, Sycurio.Digital enables retailers to securely accept payments through any digital channel, whether on the website, in a chat window, a social media platform, email, SMS text messaging, QR codes and more. Customers simply click a secure hyperlink and enter their payment card details, which are encrypted and routed directly to the PSP for processing. At the same time, real-time progress updates are relayed to the retailer, enabling them to track the live journey of each link to ensure that the transaction is completed seamlessly and securely.

Sycurio sits outside the retailer's network infrastructure

Which means:

Payment information remains secure

The sensitive payment information remains segregated and secure, never touching the retailer's business infrastructure.

Reduce risk

By keeping the sensitive payment card data out of their network, retailers also reduce their risk of data breaches or being targeted in cybersecurity attacks.

Reduce scope of PCI DSS

Retailers need never again worry about processing, handling or storing the sensitive data. In addition to keeping the payment card data more secure, this also dramatically reduces the scope of compliance for PCI DSS, saving retailers time and money.

Conclusion.

The future of retail is omnichannel.

Consumers want the ease and convenience of being able to use any channel and any device at any time to make their purchases. Many retailers have made great progress in building omnichannel operations. However, consumer fears around the security of their sensitive data is holding back many potential customers from making purchases through these channels.

To capture more customers and increase omnichannel sales, retailers must begin communicating the strong data security practices they have put in place to protect their customers' sensitive information. With easy-to-use, secure payment solutions, retailers can achieve the best of both worlds – providing the frictionless experience their customers desire while ensuring their data is safe.

Sycurio.