

Balancing Security & CX.



Balancing security and customer experience.

As more companies embrace digital transformation and adopt remote or hybrid working models, meeting consumers' high expectations for fast, convenient, and frictionless digital services while at the same time maintaining strong security is becoming a real challenge.

This is especially true when it comes to enabling secure payments and purchases, where research shows that global payment fraud continues to rise and predicted to cost merchants \$40.62 billion by 2027.



Cost of global fraud by 2027
\$40.62 billion.

Consumers expect firms to keep their data secure. Surveys show that more than three-quarters of consumers will stop engaging with a brand following a data breach. So, how can businesses balance the need for strong data security with consumer desire for fast, frictionless digital processes?

Using the right technologies, businesses can ensure strong data security regardless of where your employees are working - remotely or in the office, while delivering the ease and convenience that are the hallmarks of an excellent customer experience.

Enabling a frictionless customer experience.

Every week major data breaches grace the headlines. Companies that handle consumer payment card data, must be aware of the need to not only follow best practices for data security and privacy, but also to meet and maintain compliance with the Payment Card Industry Data Security Standard (PCI DSS). The risk of falling short and suffering a data breach can be potentially catastrophic, resulting in not only regulatory fines but also the high costs of remediation and the potentially irreversible damage to brand reputation. Moreover, the potential loss of trust among customers can have lasting effects on sales long after the initial breach.

To safeguard consumers' sensitive data while still enabling a frictionless customer experience, organizations need to both ensure that they have the proper internal procedures and employee training in place, as well as adopt new and more secure, digital payment solutions.

Internal controls for strong data security.

Ultimately, a positive customer experience depends on strong data security so safeguarding customers' sensitive personal information and making sure it is not exposed in the event of a breach is a must.

To ensure that they are following best practices in the handling, transmitting, processing, and storing of customer payment card data, merchants should implement a PCI DSS security awareness training program for all employees. This helps employees to understand the proper methods to follow when handling sensitive customer information, as well as recognizing potential threats and appreciating the risks associated with insecure practices within the contact center. Training should be ongoing, with refreshers annually.



PCI DSS security **awareness training program** for all employees.

Beyond employee training, any business that accepts payments from customers must be sure they are following the highest level of data security procedures and controls throughout their organization. In addition to PCI DSS requirements, organizations should work to become certified against the internationally recognized ISO 27001 standard. This standard helps companies keep their data secure by following rigorous requirements for establishing, implementing, maintaining and continually improving their information security management systems and techniques. And when it comes to working with digital payments solutions providers or other partners, businesses should look for partner organizations that have attained all of the leading accreditations pertaining to secure payments, including not only ISO 27001 but also PA DSS, PCI DSS Level 1 Service Provider status, and checking that they are an official Visa Merchant and appear on the Mastercard SDP Compliant Service Provider listing.



Check your partners have **up to date & relevant** payment security accreditations.

Balancing Security & CX.

Sycurio.



Adopting secure, omnichannel payments solutions.

In addition to implementing a robust internal security program, one of the easiest ways for businesses to balance security with customer experience is to streamline the payment process by adopting new digital payment solutions that enable secure, omnichannel payments. Consumers today expect to be able to transact with businesses through any channel or device, whether it's over the phone, through the website, over email, online chat, social media, in-person and more. New omnichannel payments technologies make it easy for businesses to meet customers in the channel of their choice and enable a secure, seamless payment experience no matter what channel or device they choose.



For example, Sycurio.Digital enables businesses to create secure payment links that can be used in any digital channel, including e-commerce and m-commerce, email, social media, online chat, SMS and more. Sales or customer service representatives (CSR) can even use the solution to generate and display QR codes on printed bills or communications. The customer simply clicks the link or points their mobile camera at the QR code, then enters their payment details for a fast, convenient, and most importantly, secure payment process.

Sycurio.Digital

At the same time as the customer inputs their payment data, the solution relays real-time progress updates to the sales or customer service representative, notifying them when the payment page has been accessed and payment card data has been submitted, as well as when the payment service provider (PSP) has approved the transaction. Should the customer encounter any trouble at any point in the process, the CSR will see this and be able to offer support to solve the issue, leading to an improved customer experience.

Because there are no apps to download and no dongles or hardware necessary for use, Sycurio.Digital provides an extremely easy-to-use customer experience.



With flexible and customizable out-of-the-box or API-first deployment options, along with Pay-As-You-Go billing, you can get up and running in a matter of days. Moreover, it can also be deployed along with our flagship Sycurio.Voice solution for the telephone channel, enabling businesses to provide a unified, seamless customer experience for payments and purchases across all channels. At the same time, Sycurio's products ensure a highly secure payment process. That's because Sycurio.Voice&Digital keep the customer's sensitive payment card data out of the merchant business network environment completely; securely routing the sensitive information directly to the PSP for processing. By ensuring that the merchant business infrastructure does not need to process or store sensitive payment card data, Sycurio helps reduce the risk of a data breach and streamlines PCI DSS compliance.

Sycurio.Voice

Today's consumers have more choices than ever before. They have more choices of both channels and devices through which to transact with businesses, and they have more choices in terms of who they do business with. If they believe an organization is not handling their personal information securely, or if they do not have a stellar experience at every step of their customer journey, they will take their business elsewhere.



Organizations that want to remain successful today must provide not only a superior experience but also ensure a high level of data security, regardless of where their employees are located. With the right internal controls, employee training and new omnichannel payments solutions, they can balance strong security with excellent customer experience and a remote working strategy for a competitive advantage.