A Maxa Whitepaper

Growing E-commerce after SCA

maxa
online contactless

The EU has formally introduced its Strong Customer Authentication regulations as part of the PSD2 roll out.

Whilst this regulation aims to ensure greater security for all parties, it also creates potential problems for consumers, merchants and payments companies.

This White Paper sets out the scope of the challenge facing the industry – as well as the opportunity – and proposes a ground-breaking solution that delivers what everyone in e-commerce is looking for: faster, easier transactions, full regulatory compliance – and improved security.

ONLINE FRAUD: ACTION REQUIRED

Online fraud has been a constant and growing problem for everyone involved in e-commerce. The Emerging Payments Association (EPA) estimates that in 2018, e-commerce fraud cost UK businesses alone £310 million. Across Europe, Europol has identified e-commerce fraud as a key systemic risk, with two-thirds of payment card fraud stemming from Card Not Present (CNP) transactions – the standard designation for e-commerce transactions in transaction processing systems.

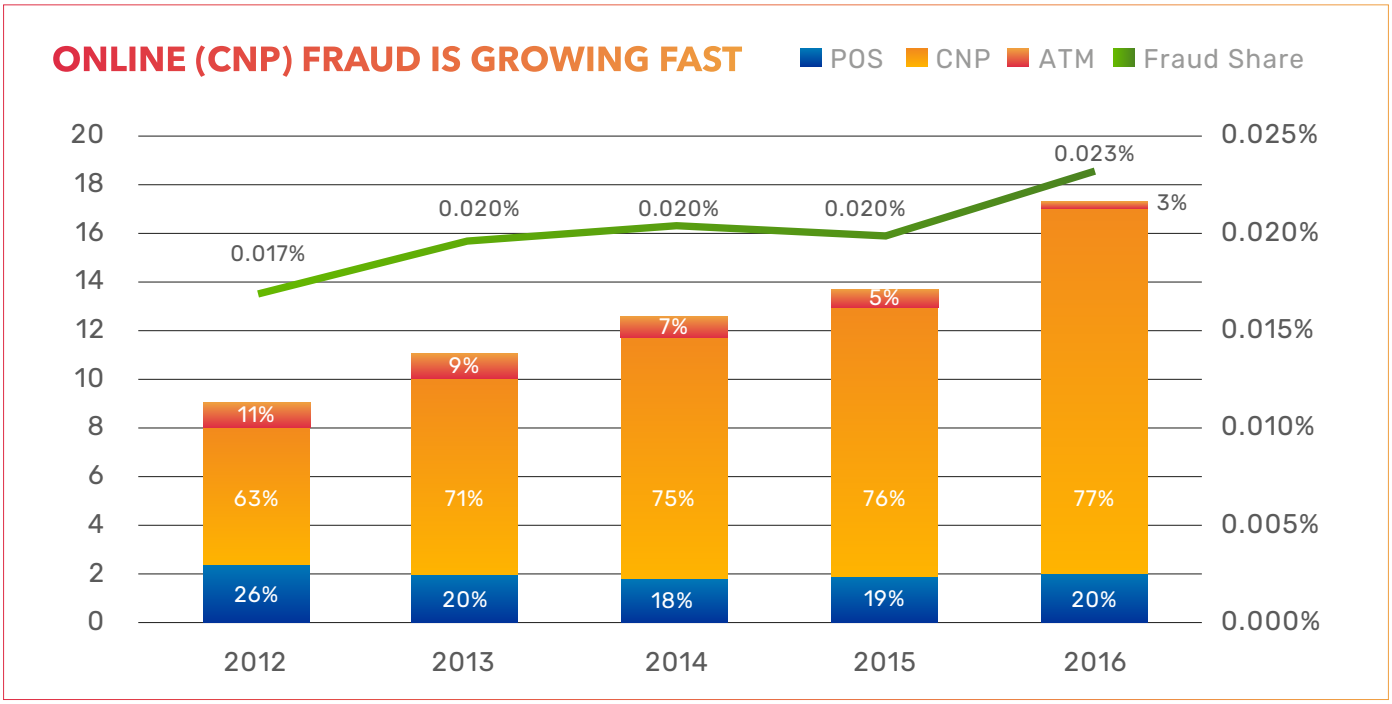
Coupled with this rise in online fraud, the industry faces a proliferation of different payment methods preferred by various markets across the EU. The Netherlands prefers direct bank transfers, but Portugal favours the e-cheque and Scandinavia embraces alternative payments. In the UK, one in five UK consumers regularly use PayPal to buy goods and services online, whereas in Germany, paying on open invoice is well established as the most popular method of online payment, used by 70 percent of German online consumers. Yet none of these methods is really much more secure than any of the others: in a single fraud wave in 2015, German online fashion retailer Zalando was defrauded of Euro 18.5 million by fraudsters operating a fake identity scam.

Figures from the ECB for the period 2014-2016 demonstrate the extent of the problem – not only is CNP fraud (typically enacted in an e-commerce transaction) claiming a bigger share of fraud than any other kind of card crime – it's also growing faster than in any other category. So fast, in fact, that online security company Risk Ident estimates that e-commerce fraud grew by 16-18 percent between 2016 and 2018 in the UK – and by 16 percent in the US over the same period. ***See below.***

Add to this growing risk profile the fact that cross-border e-commerce fraud within the Single European Payments Area, or SEPA, is the single fastest growing category of fraud loss, and the need to take action becomes clear.

PSD2 AND SCA: REGULATORS MAKE THEIR MOVE

Given the increase in e-commerce fraud across the continent, it comes as no surprise that the EU decided to take action to enhance e-commerce security across the Union. On October 8, 2015, the European Parliament adopted a proposal from the European Commission to create safer and more innovative European payments with its second Payments Services Directive, or PSD2. These new



maxa

rules aim to better protect consumers when they pay online, promote the development and use of innovative online and mobile payments such as through open banking, and make cross-border European payment services safer.

On November 16, 2015, the Council of the European Union passed PSD2, which came into force on 13 January 2018. In addition to enhancing e-commerce security, the regulations are envisaged as breaking the perceived stranglehold banks have on customer data and marketing channels, opening these up to third-party providers via "Open Banking."

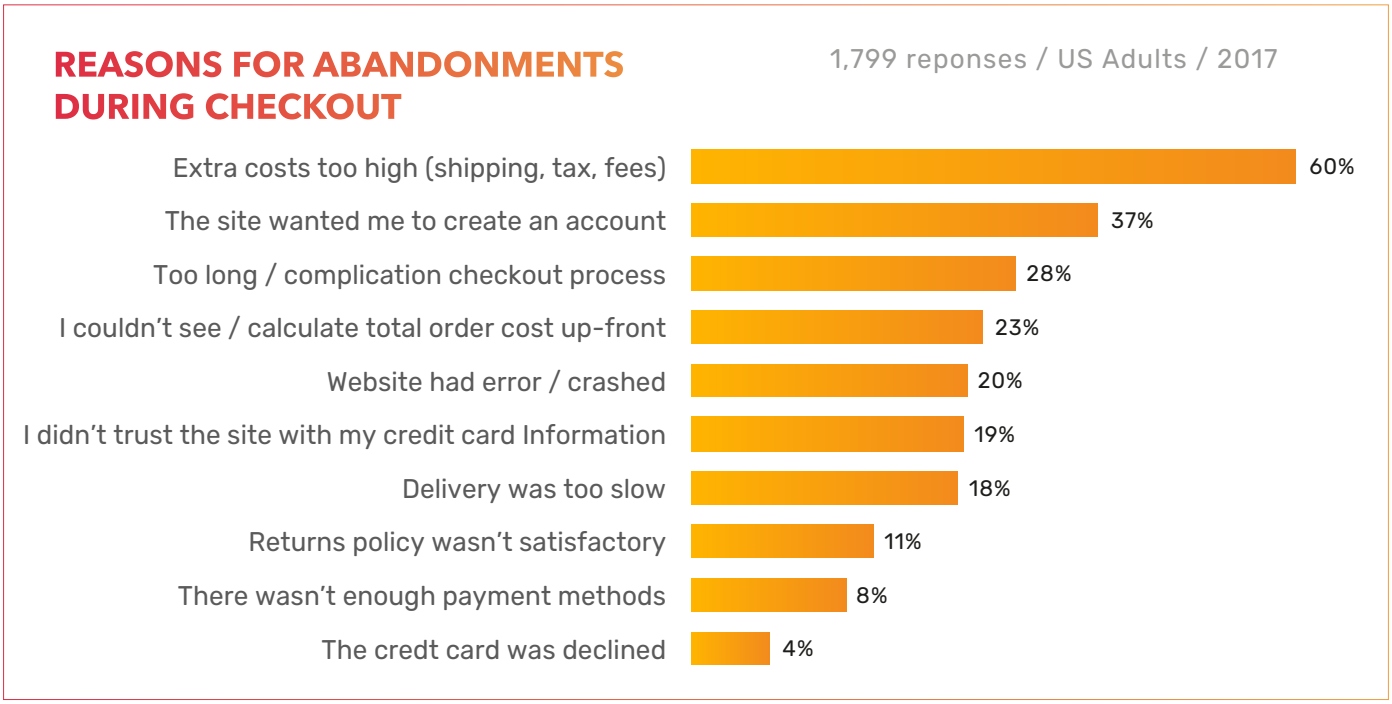
When it comes to e-commerce security, the PSD2 regulations mandate strong customer authentication (SCA) for the majority of electronic payments. The SCA portion of PSD2 is scheduled to take effect from the 14th September though, as we'll see below, doubts expressed by industry regarding the implementation of SCA rules have led to a confused situation.

SCA: WHAT'S REQUIRED – AND WHY IT'S A CHALLENGE

As things stand, the SCA regulations mandate two-factor authentication for all online transactions with a value in excess of 30 Euros. In practice, this means the development of an authentication system for online transactions based on the use of two or more elements categorised as knowledge (i.e. something only the user knows), possession (something only the user possesses) and inherence (something the user is.) SCA further stipulates that these elements must be independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

So far, so good. The problem with SCA as things stand is that the industry anticipates these requirements will only exacerbate an existing and growing problem – cart abandonment. This occurs when consumers become disenchanted with the security and information requirements stipulated by a merchant's website (or their acquirers), leading to abandoned sales, lower revenues for the merchant – and lower fees and card usage for issuers and acquirers.

As the chart from Jilt Consulting below demonstrates, a lack of trust in the checkout process, and onerous checkout processes themselves, are most likely to cause US consumers to abandon their e-commerce transactions. Jilt's research was undertaken in 2017 – and concerns




MEMBE
SINCE

the United States, a country not covered by the SCA provision except for inbound e-commerce to EU consumers. Imagine how much more acute this problem will be when SCA is applied to the situation in Europe.

However laudable the aims of SCA as a regulation, there is considerable concern in the industry that, as things stand, SCA's provisions will only lead to more cart abandonment and reduced growth in e-commerce. As a sales channel, e-commerce is currently growing at between 7-8 percent per year across Europe, and now accounts for $346 billion in total sales volume– a figure projected to rise to $479 billion by 2023.

A wide variety of consumer and industry surveys suggest that SCA's provisions could put this strong growth pattern at risk. In June this year, e-commerce security firm Gocardless published research based on 4,000 interviews with consumers in the UK, France, Germany and Spain. The study found that nearly half of UK consumers (43 percent) said that "speed and ease of payment" was the most important factor when paying for something online, with one third of French and German online shoppers agreeing with this statement.

Whilst shoppers in all markets placed high value on a secure checkout process, the research found that 44 percent of UK shoppers had abandoned an online order because of complex or lengthy security, while 48 percent had done so in Germany. And when it comes to the new provisions mandated by SCA, nearly half (45 percent) of UK consumers would be frustrated with a favourite brand that introduced new security processes during online checkout and a fifth (23 percent) would shop less with that brand if it introduced new security measures. Interestingly, the need to give away complex security information made as many people feel suspicious as safe, with 40 percent of consumers saying they did not trust this practice.

Nearly half of UK consumers (43 percent) said that "speed and ease of payment" was the most important factor when paying for something online.

THE NEED FOR SPEED: CONSUMERS AND INDUSTRY UNITE

The results of the Gocardless study are mirrored in research undertaken by the UK's Emerging Payments Association (EPA). According to the EPA's survey of payments professionals, the introduction of SCA will see so-called "step-up" authentication requests increase from its current level of two percent of transactions to around 30 to 50 percent of transactions. At the same time, the EPA predicts that transaction declines will increase from around three percent of all transactions to 25 -30 percent: in other words, they predict that nearly one in three transactions could be declined once SCA comes fully in to force.

As the EPA's study notes, "the entire payments ecosystem is not ready for SCA, and requires more time before active enforcement starts." 75 percent of the issuers surveyed by the EPA say they are now compliance-ready with SCA. However, this does not mean they are operationally ready.

Recognising this fact, the EU has acted on an opinion provided by the European Banking Authority (EBA), and devolved responsibility for the implementation of SCA to member states over an 18-month period, which will lead to the full implementation of SCA and enforcement actions by April 2021. The UK's Financial Conduct Authority has subsequently led the way among member states, agreeing a phased implementation of the Strong Customer Authentication (SCA) rules which came into effect on Saturday, September 14th.

This implementation will span 18 months, and the FCA has already confirmed that it will not take enforcement action against firms if they do not meet the relevant requirements for SCA "in areas covered by the agreed plan, where there is evidence that they have taken the necessary steps to comply with the plan." In another 18 months, however, the FCA expects all UK firms to have made the necessary changes and undertaken the required testing to be able to apply SCA's

provisions to all transactions – whatever the effect on sales, profits and customer service.

In summary, the most recent comments from the EBA have recognised the challenge facing the industry to meet the SCA deadline. The EU has also accepted that on an exceptional basis, Local Competent Authorities (local regulators) may decide to work with issuers, acquirers and other relevant stakeholders, to provide additional time to allow issuers, acquirers and merchants to migrate to SCA-compliant solutions. This is on the condition that the financial institution has set up a migration plan, agreed it with their Local Competent Authority, and will execute the plan in an expedited manner.

A REPRIEVE – AND A SECOND REVOLUTION?

The most recent comments from the EBA and the UK's FCA represent a reprieve, of sorts, for all European businesses conducting e-commerce. However, the respite will be temporary, with full implementation still expected by April 2021 in the UK's case – and possibly sooner in other markets.

As things stand, there are a number of options being suggested to help the industry solve its SCA compliance problem from an operational perspective – although none of them are, as yet, wholly satisfactory. The main options proposed include one-time passwords provided by SMS to a mobile device, in-app authentication using two-factors to confirm a consumer's ID, biometric evaluations and 3D Secure version 2 technology, or 3DS v2 – the major solution being promulgated by Mastercard and Visa and their partners at EMVCo.

However, each of these solutions presents its own set of challenges: one-time passwords (OTPs) depend on over-the-air connectivity for mobile devices, rather than just near-field communication, and recent reports have criticised OTPs for being notoriously prone to hacking through insecure nodes in mobile networks. Biometric solutions appear more promising but are still in their early stages as a means of two-factor authentication, and two-factor authentication in-app effectively represents another layer of form-filling and password completion – those very factors which lead to the growing level of cart abandonment seen across developed markets.

3DS v.2 is perhaps the most promising of the solutions currently proposed by industry. This system, developed by EMVCo and promulgated by major banks and card schemes, uses rich data points based on a bank's knowledge of its customers to confirm their identity. In the case of low-level e-commerce transactions, it is possible for this identity confirmation to happen without the friction of any secondary factor. At higher transaction levels, however, the system will rely on PIN entry and/or biometric factors as a minimum. At the time of writing it would appear that, despite steps in the right direction, the industry is still struggling with how to square the circle of maintaining compliance with SCA requirements and giving online shoppers the speed, ease and security they want.

At the same time as this debate about SCA compliance continues, the payments sector is experiencing a second revolution, one which may prove to have as much impact on online commerce as it is currently having on physical payments. This is the growth in contactless card transactions across Europe and other geographies globally.

CONTACTLESS: IN TOUCH AND ON TIME

Contactless payments by card using Near-Field Communications (NFC) represent a massive change in consumer payment habits around the world. Because they work using an upgraded version of 1990s payments infrastructure (i.e. cards and terminals, now equipped with NFC technologies) it's possible to underestimate the significance of this change.

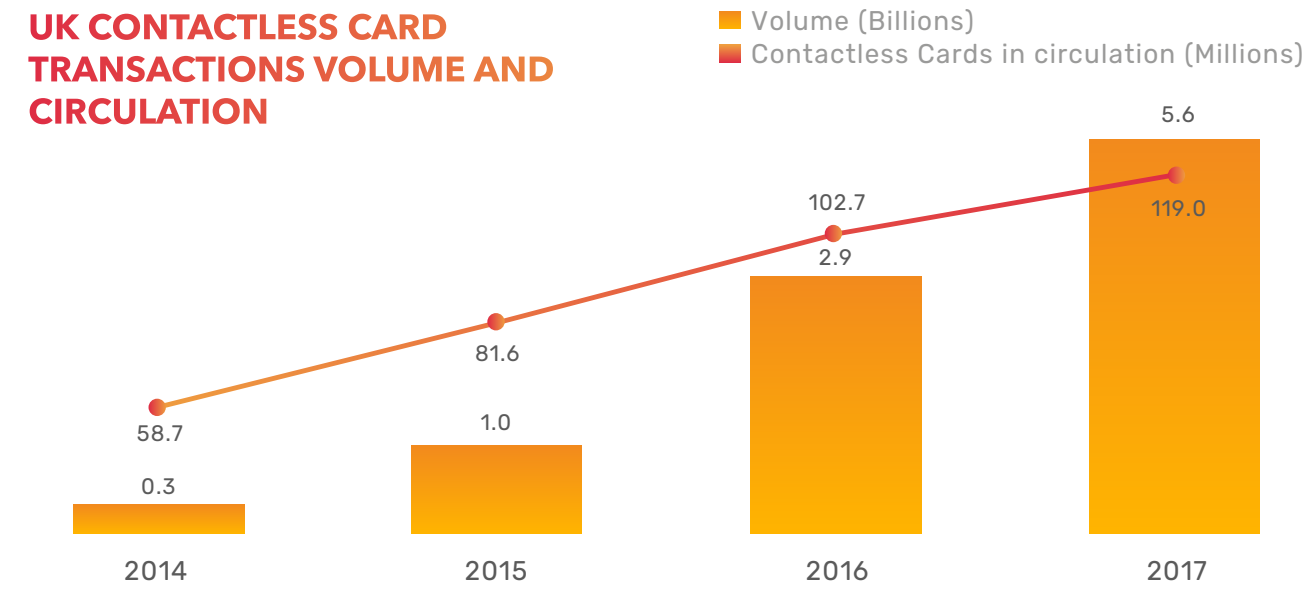
The facts speak for themselves: Transparency Research estimates that, over the next six years, contactless payments will soar by a Compound Annual Growth Rate (CAGR) of more than 55%

per annum to reach $14.11 billion in the US alone. In the UK, growth has been yet more impressive, with 5.6 billion contactless transactions undertaken in 2017, and more than 120 million cards in circulation.

In June 2019, UK Finance announced that the 18-34 age group in the UK was to all intents and purposes now cashless, with 17 percent of this age group using contactless cards or credit cards exclusively. The UK Finance report also noted that total contactless transaction volumes had grown by 31 percent in a single year to reach 7.4 billion total transactions, and that 7 in 10 UK citizens now use contactless cards as their preferred method.

Indeed, global studies demonstrate that where contactless payments are available, consumers would rather use them compared to Chip and PIN-enabled card transactions. Even in notoriously "cash" markets such as Germany, consumers now prefer contactless to chip and PIN by a margin of 52 percent to 48 percent; in more tech-savvy markets such as the UK or Nordics, that figure rises to around 60-65 percent, according to figures from Barclaycard.

UK CONTACTLESS CARD TRANSACTIONS VOLUME AND CIRCULATION



Source: UK Cards Association, UK Finance

GLOBAL CONTACTLESS PAYMENT TRANSACTION MARKET VOLUME

By region, 2017 (US$ Bn)

Source: Transparency Market Research, 2017

The reasons behind the growth in contactless transactions are not hard to find: contactless transactions are quick and easy, and do not require a card to be inserted into a device, nor the provision of a Personal Identification Number (PIN). More than this, contactless transactions are consistent with the wider digital payments transformation, in which – for younger consumers especially – the use of a mobile device equipped with a wallet enables "tap and go" contactless transactions in the physical world, as well as e-commerce transactions.

"In the world today, we are seeing the emergence of two major trends: contact-less and e-commerce. Maxa's ground-breaking technology stands at the convergence of these two trends."

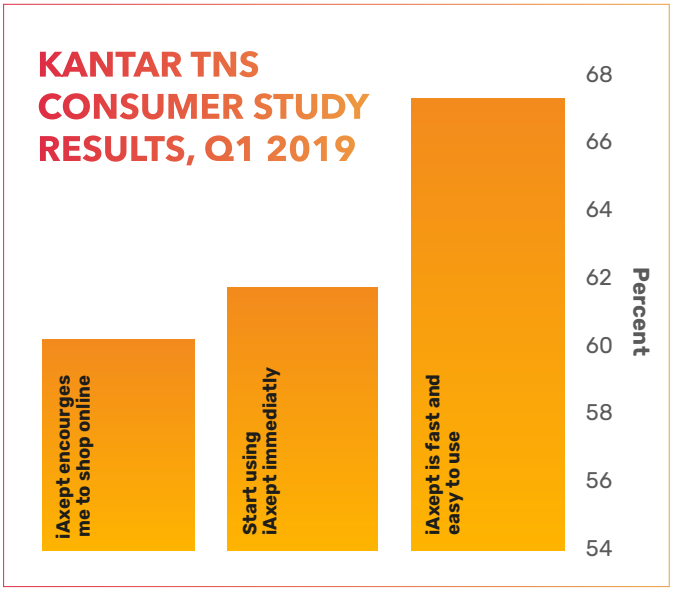
MAXA: WHERE CONTACTLESS MEETS E-COMMERCE

As we've seen above, there are two major trends emerging in the payments world today: contactless payments, and the move towards e-commerce. Maxa's ground-breaking technology stands at the convergence of these two trends, offering SCA-compliant eCommerce transactions using contactless cards to provide both consumer identification and transaction confirmation. Maxa is quick and easy to use, popular with consumers, and secure.

HOW IT WORKS

With Maxa, the consumer's mobile device acts as a point of sale terminal for online transactions. For the first time, Maxa makes SCA-compliant, card-present credit and debit transactions for e-commerce possible. All consumers require is a payment card, a mobile device, and one tap of their contactless-enabled payment card against their mobile device. For higher-value transactions, consumers simply key in the same PIN they use at their ATM or in Chip-and-PIN transactions: no need to remember third-party passwords, transfer iris or fingerprint information, or run the risk of missing a one-time-password communication.

Following one tap from the consumer, their mobile device then communicates with the merchant's website to confirm the transaction. The beauty of Maxa is that, because the consumer's card is physically present in the transaction, each purchase is treated as a card-present transaction, reducing the risk of card-not-present fraud and eliminating the need to fill out countless checkout boxes. Furthermore, the presence of two factors – the consumer's payment card + PIN – means that Maxa is an SCA-compliant solution.
The industry now has a solution which is fast, easy-to-use, compliant with regulatory demands, and secure. Perhaps best of all, research undertaken by Kantar TNS in Finland reveals that consumers are responding enthusiastically to Maxa.



In a recent (Q1 2019) test of Maxa's system with consumers, 59% said that Maxa would encourage them to shop more online. 60% of consumers who expressed an interest in Maxa wanted to start using it immediately, and 67% said they found it "fast, and easy to use."

For issuers, acquirers and merchants, Maxa will drive up card usage online, growing fees and transaction volumes in the process. Although e-commerce is projected to grow at around 7-8% per year over the next five years, payments players using Maxa can expect much higher growth rates as consumers grow used to the simplicity, speed and security Maxa offers.

MOBILE NETWORK OPERATORS: ANOTHER ADVANTAGE

Maxa also offers significant benefit to Mobile Network Operators (MNOs). Before Maxa, MNOs were reliant on a direct link between their devices and a wallet or bank account. This effectively meant they were "renting out" space on their SIMs to financial institutions, free of charge. Now, MNOs can experience continuous profit improvement with Maxa. On the one hand, consumers will increase their e-commerce over mobile devices, taking advantage of Maxa's simplicity and speed to pay for streamed video content, bridge tolls, snacks and other services safely. Maxa also offers MNOs' customers the opportunity to top up their pre-paid mobile account with one tap from anywhere without using a wallet. This generates increased customer loyalty, higher Average Revenue Per User (ARPU) and reduced customer churn.

At a time when increased regulatory demands are casting doubt over the future growth of e-commerce, Maxa gives consumers the chance to pay online in a way that is as easy, fast and secure as contactless payments in physical shops. Given that the system is SCA compliant and based on proven technologies like contactless cards, Maxa provides the payments business with a unique opportunity to accelerate e-commerce revenues, build customer loyalty and meet new regulatory requirements under the EU's SCA regulations. Above all, the evidence is there that consumers love this system, and can't wait to get started using it.

To find out more about how Maxa bridges the gap between contactless payments and e-commerce, and how it will fit your payments strategy as an SCA-compliant, secure solution, please get in touch with us:

www.maxagroup.com
info@maxagroup.com

www.maxagroup.com | info@maxagroup.com

maxa
online contactless