A Maxa Whitepaper

Online Commerce's toughest challenges:

secure online transactions, reduce friction and increase sales.

maxa
online contactless

Today, all business is going digital, and fraud is following. Banks and merchants are battling constantly to fight against the rising tide of online fraud. As things stand, efforts to secure online commerce have involved more user friction – which, in turn, could lead to reduced e-commerce revenues and profitability.
Doug Gray, CCO at Maxa, reviews the current landscape and presents a solution based on proven technologies that taps into trends consumers love.

M-COMMERCE ADVANCES

It's a given these days that the world is going digital. A recent study from FIS Global predicts online commerce will grow at 7 percent a year globally, reaching US$4.6 trillion by 2023 – this compares positively with physical retail sales, predicted to grow at a little less than 4 percent over the same period. So e-commerce is picking up a greater share of consumer spending, year after year. Dig a little deeper, though, and things get more interesting. The same FIS study tells us that m-commerce will grow at 19 percent on average over the next five years, to reach US$2.29tn by 2023. By that point, around half of all online sales will be via mobile devices.

The growth in mobile commerce presents huge opportunities for banks and merchants. But it also promises significant headaches, not least in the area of fraud, which is migrating online at speed.

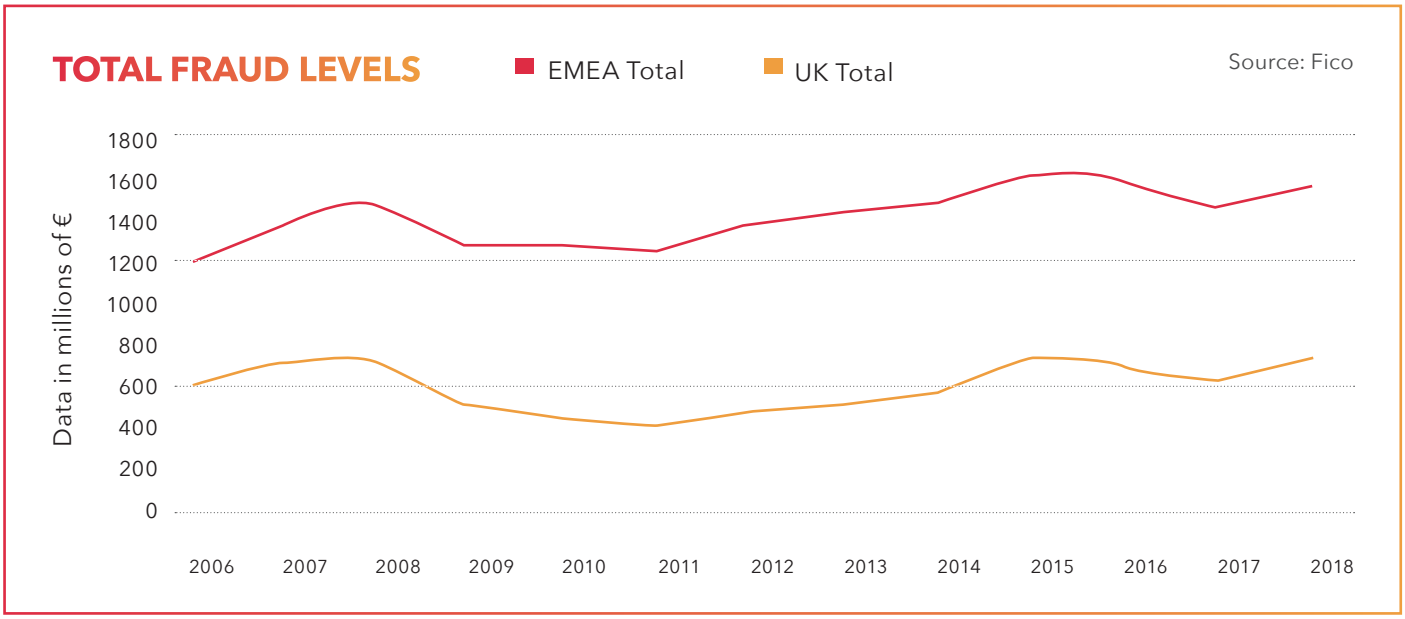
2018 statistics from FICO show that Card-Not-Present (CNP) fraud – the kind most closely associated with e-commerce – now accounts for around 70 percent of all fraud. Fraud types relating to physical transactions, such as counterfeit cards, have long since been minimised as an issue – but that fraud has migrated online. As this graph demonstrates, the industry has made valiant efforts to reduce CNP fraud in recent years; however, the sheer speed at which business is migrating online, and the extent to which fraudsters constantly adapt their methods to avoid detection, has made it hard for industry to catch up.

> **"ID fraud rose by 58% in the UK last year alone."**

The most recent figures from FICO also show another worrying trend emerging: a sharp rise in ID fraud, relating to the theft of One-Time Passwords (OTPs) used to secure e-commerce transactions over desktops and mobile devices, and "SIM jacking", in which consumers are tricked into giving away their login identities. This kind of fraud rose by 58 percent in the UK last year alone.

WHAT WE NEED: FRICTIONLESS, FAST AND SAFE

The market needs a solution that improves security, especially in a mobile environment. At the same time, any new solution must not increase friction for end users, as a mid-2019 study from GoCardless makes clear. After interviewing 4,000 consumers from major European markets, GoCardless found that 44 percent of UK online shoppers had abandoned an order because of complex or lengthy security processes, while 48 percent had done so in Germany. Nearly half (45 percent) of UK digital consumers said they would



be frustrated with new security processes during online checkout and a fifth (23 percent) would shop less if new security measures were introduced. Add to that the fact that the EU's new Strong Customer Authentication (SCA) rules will mandate two-factor authentication from the end of 2020, and the impetus to find an answer that's easy to use, fast and secure becomes obvious: the introduction of any more friction to the process risks turning consumers off the whole idea of shopping online.

WHAT'S ON OFFER: MORE SECURITY – AND MORE FRICTION?

So far, solutions proposed to counter online fraud have varied. Some have attempted to strengthen fraud detection in transaction processing through the use of Artificial Intelligence and Machine Learning techniques. Though promising, such techniques remain in their infancy – and the same might be said of biometric factors, though their use is increasingly rapidly. As a result, a lot of companies have relied on mandating changes to consumer behaviour through multi-factor authentication to help them fight online fraud.

While multi-factor authentication may be more effective than a single factor, not all two-factor authentication systems are created equal. Many recent solutions have evolved from a desktop computer environment and involve the introduction of various elements of user friction, such as the entry of one-time passcodes (OTPs). These passcodes are typically delivered via SMS for input on the merchant website or app. However, as more websites and apps come to depend on SMS OTP to secure their operations, there are growing concerns about the vulnerability of this form of authentication to compromise and fraud.

The proliferation of SMS OTP as a confirmatory factor risks creating a false sense of security in consumers – some studies suggest that as much as 70 percent of online fraud over mobile devices could be linked to the interception of OTPs delivered by SMS. India, for instance, has

> **"As much as 70 percent of mobile fraud could be linked to the intercept of SMS OTPs."**

experienced very high levels of fraud through its Adhaar digital ID and Jan Dhan mobile finance system, directly linked to the interception of SMS OTPs. Fraud events such as those experienced in India explain why regulators in France, Germany and the UK are all reviewing the status of OTPs as a means of securing online transactions.

At this point, it's important to stress that merchants and acquirers have a wide range of solutions at their disposal, including 3D Secure v 2.2 as promoted by the card networks. However, even 3D Secure v2.2 in isolation looks unlikely to meet the SCA compliancy standards, and will most probably require the use of a 2nd biometric factor at higher transaction levels. While there may be no doubt that 3D Secure 2.2 has improved security and reduces fraud for conventional CNP transactions, it has done so at considerable cost to merchants who have seen cart abandonment rates dramatically increase when password is prompted for. A 2019 research paper from the fraud technology company Ravelin found that even forward-thinking banks who have already implemented one-time password and app-based verification still lost 19% of transactions through 3DS 2. In some instances, this has caused merchants to turn off 3D Secure completely. 3DS V 2.2 is also known to cause further customer friction when being employed across multiple devices or when used on a shared device.

While it may be that there's no "one size fits all" answer to securing e- and m-commerce, there's no doubt that current solutions do, at the least, propose some increase in consumer friction via additional user inputs. And that, in turn, puts business growth and profits at risk.

THE SOLUTION: TAPPING IN TO TRENDS

If we're currently in the middle of an e- and m-commerce revolution, then another huge change in this industry, less written about but no less significant, is the growth in contactless card transactions in recent years. 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.

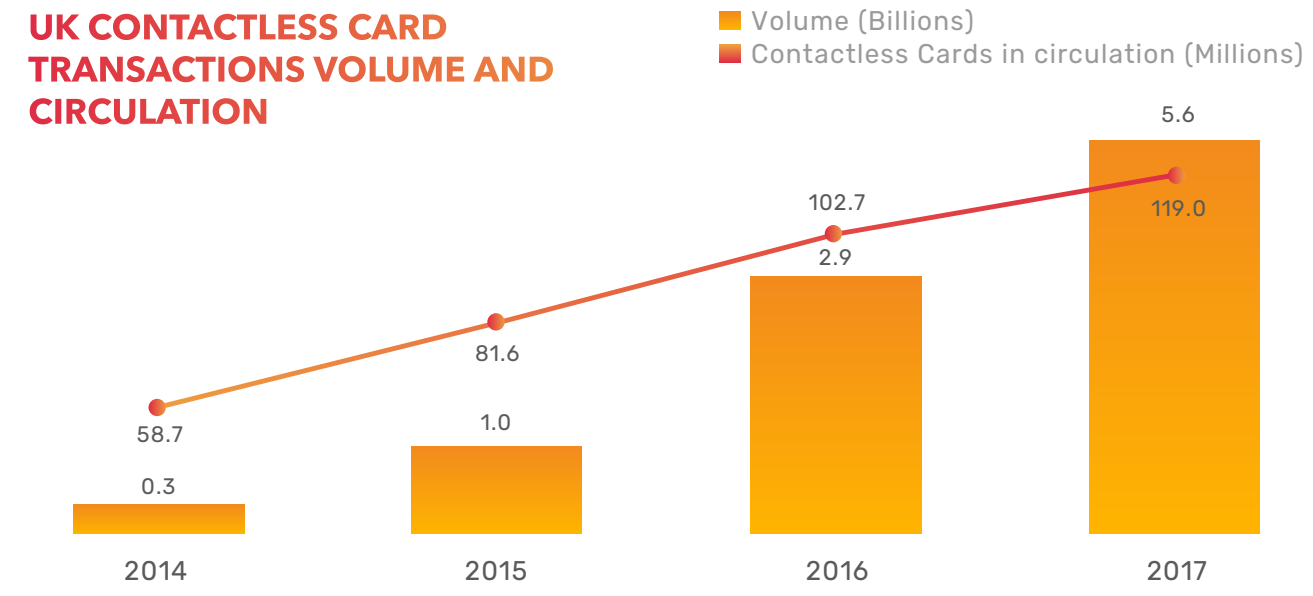
Contactless transactions are quick and easy, and do not require a card to be inserted into a device, nor the provision of a Personal Identification Number (PIN). More than this, contactless transactions are consistent with the wider digital payments transformation, in which – for younger consumers especially – 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.

Maxa's ground-breaking technology stands at the convergence of online commerce and contactless transactions. Maxa offers SCA-compliant e-commerce 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

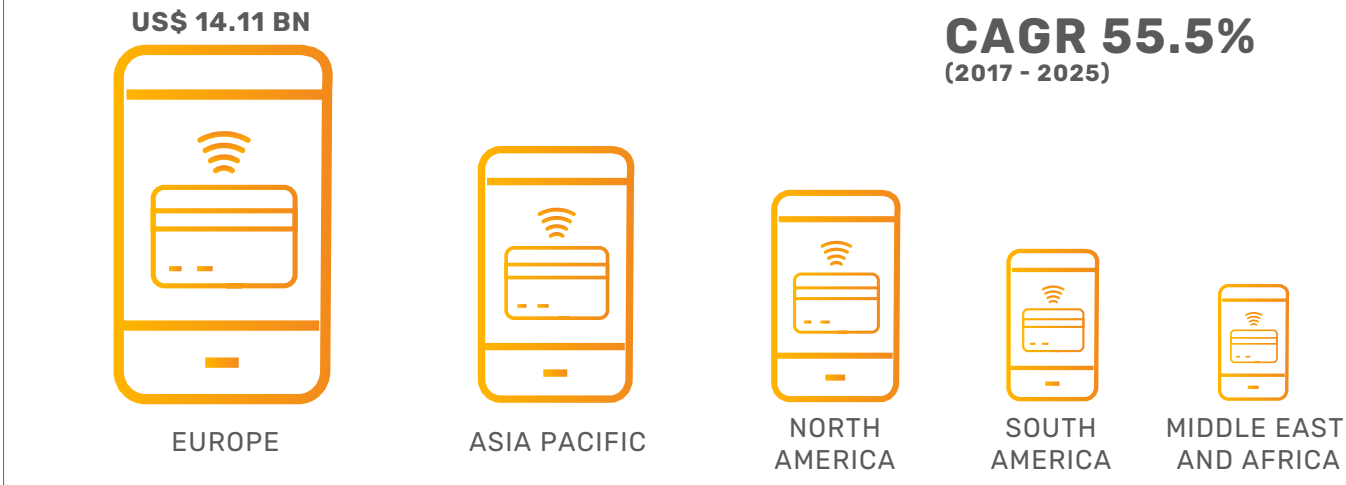
UK CONTACTLESS CARD TRANSACTIONS VOLUME AND CIRCULATION



Source: UK Cards Association, UK Finance

GLOBAL CONTACTLESS PAYMENT TRANSACTION MARKET VOLUME

By region, 2017 (US$ Bn)



Source: Transparency Market Research, 2017

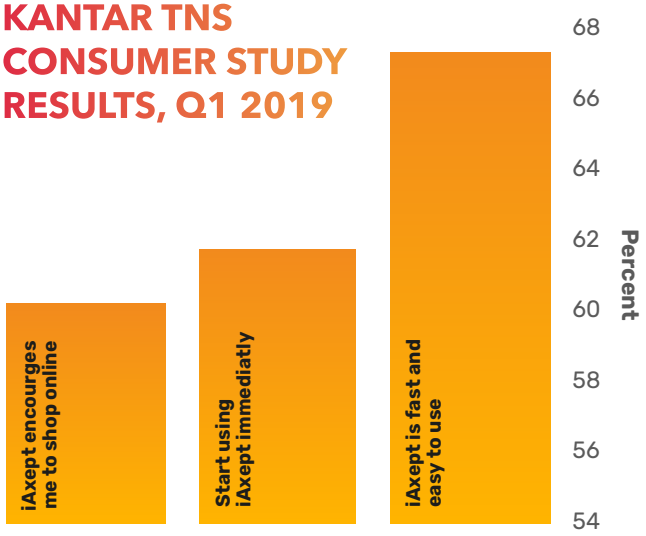
e-commerce possible. All consumers require is a payment card, a mobile device, and one tap of their contactless-enabled payment card against their mobile device. For higher-value transactions, consumers simply key in the same PIN they use at their ATM or in Chip-and-PIN transactions: no need to remember third-party passwords, transfer iris or fingerprint information, or run the risk associated with OTPs via SMS.

Following one tap from the consumer, their mobile device then communicates with the merchant's website to confirm the transaction. As the consumer's card is physically present in the transaction, each purchase is treated as a card-present transaction, removing the risk of card-not-present fraud for these transactions and eliminating the need to fill out countless checkout boxes. Furthermore, the presence of two factors – the consumer's payment card, and their 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. Research undertaken by Kantar TNS, the 2nd-largest global market research company, reveals that consumers are responding enthusiastically to Maxa. This research showed that 33% of cardholders said they would buy more online if there was a secure and easy checkout process, however after learning about Maxa Online Contactless 59% said they would buy more using it. 60% of consumers who expressed an interest in Maxa wanted to start using it immediately, and 83% said they found it "the fastest, and easiest solution to use."

Online security is of paramount importance to all merchants and banks, especially given rising levels of fraud. Maxa's hardware is secured using industry strength end-to-end RSA 2048 bit encryption and public key infrastructure to guarantee only verified online shops and consumer devices are used

KANTAR TNS CONSUMER STUDY RESULTS, Q1 2019



maxa

for payments over the system. Maxa transactions are secured using a cryptogram created by the contactless EMV card during the transaction.

For issuers, acquirers and merchants, Maxa will drive up card usage online, growing revenues 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 on offer.

Maxa provides a unique opportunity to accelerate e-commerce revenues, build customer loyalty and meet new regulatory requirements under the EU's SCA provisions. Above all, there's solid evidence that consumers love this system, and can't wait to get started using it.

Maxa combines two of the most popular trends in payments - contactless transactions and mobile e-commerce - to create a fully SCA-compliant, secure solution for online payments that's fast, simple and safe to use. To find out more about how Maxa fits your payments strategy, get in touch with us via:

www.maxagroup.com
info@maxagroup.com

www.maxagroup.com | info@maxagroup.com

maxa
online contactless