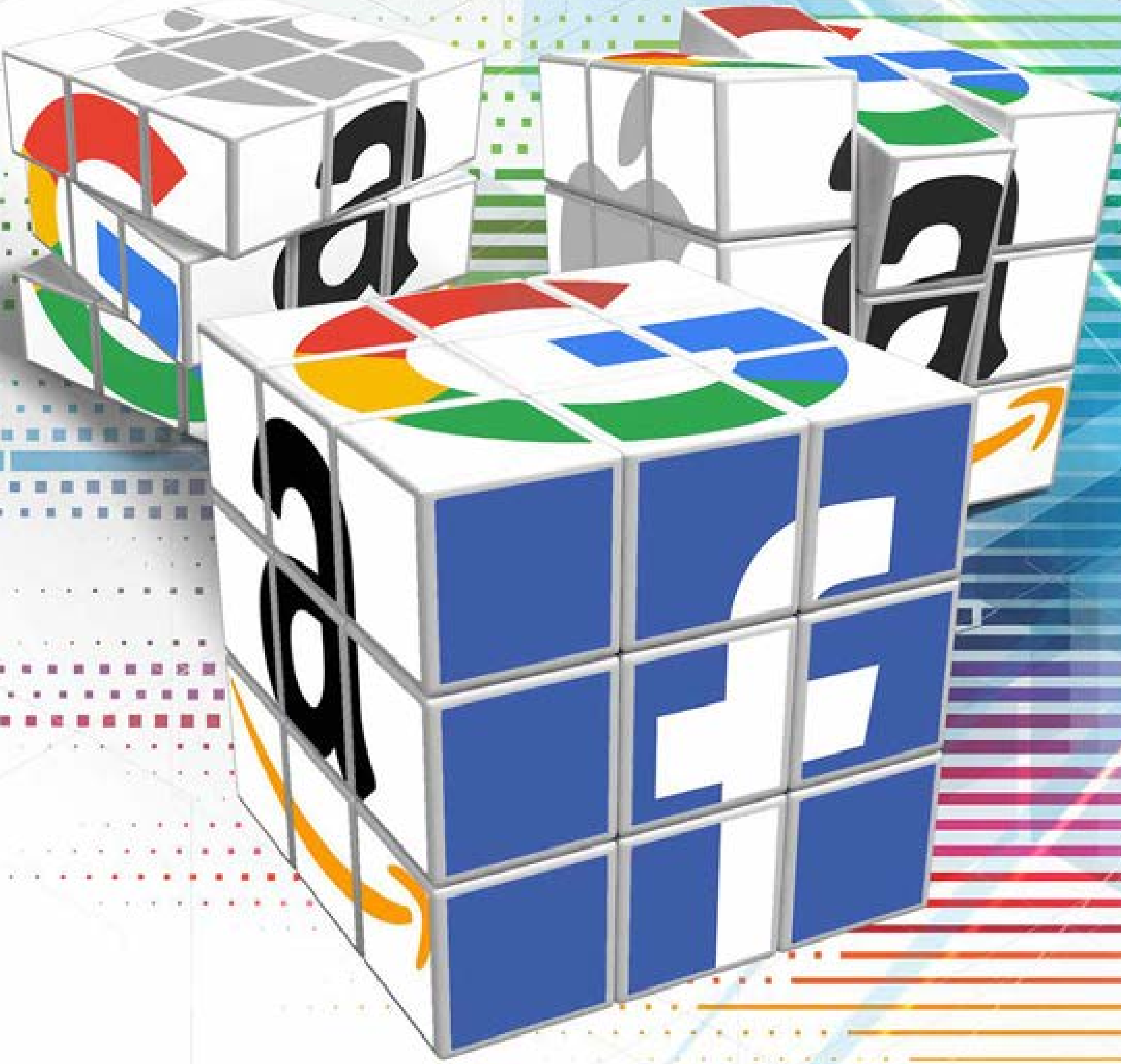
PAYMENTS INDUSTRY INTELLIGENCE

Payments
CARDS & MOBILE

March / April 2019

25 YEARS



COVER FEATURE

BIG TECH AND PAYMENTS

IS THE SUN SETTING ON RETAIL POS ESTATES?

by James Wood

Successive waves of Point-of-Sale (POS) terminals are "sunsetting" – no longer receiving software updates – leading to significant upgrade or replacement costs for retailers. Meanwhile, non-POS methods of payment are proliferating, adding to the complexity retailers face. But is a completely new infrastructure really the answer? PCM Editor James Wood investigates.

According to figures from the British Retail Consortium, some 76 percent of all retail payments in the UK use cards at the point of sale (POS). A recent TSYS study confirms a similar pattern in the United States, with 77 percent of consumers preferring debit or credit cards in-store. Whether these transactions happen via signature, chip and PIN or contactless card, all POS transactions require a terminal infrastructure that needs updating and replacement to keep up with changing technology and security concerns.

Whilst retailers see this as part of the cost of doing business, these upgrades can become prohibitively expensive. As a result, retailers are looking for more flexible payment strategies that protect them against fraud and can be adapted. Some claim the answer is new infrastructure that can deal with all payment types seamlessly – but while this is an attractive proposition, it's not without its own complexities.

Sunsets and Sunrises

Leading card networks – including Visa, Mastercard, Amex, JCB and Discover – set up the Payment Card Industry Data Security Standards (PCI DSS) in 2006 to protect all actors in the payments chain from fraud, including banks, retailers, acquirers, processors and consumers. PCI assesses fraud risk for payments companies, and frequently updates its seventeen different hardware and software security standards for POS terminals, including contactless card acceptance. At present, there are 900 different kinds of payment terminals using PCI standards around the world, with a new standard, PCI v4, due to "sunrise", or roll out, in late 2020. After roll-out of v4, devices using v 3.2 PCI DSS will no longer be supported by the major card networks, or "sunsetted." Additionally, the card networks do not advocate the purchase of v3-compliant terminals after April 2020.

If this sounds burdensome for merchants, then a failure on the merchant's part to have their terminals audited against current PCI standards will lead to liability for fraudulent transactions being transferred to them by issuers and acquirers. Amidst these changes, card networks are also mandating a requirement to upgrade to contactlessenabled terminals by 2019 (EMEA) and 2023 (globally), which means merchants who haven't already done so will need to upgrade their terminals as well.

For larger merchants, such upgrades are relatively easily amortised: but for smaller chains and single stores, it's likely that the costs of these upgrades will be significant. Marcello Bellitto, Director in the Milan office of management consultants AlixPartners, confirms the POS hardware market is polarising between simple and more advanced devices that embed other functions such as smart POS solutions. Bellitto says, "hardware replacement will occur at different speeds depending on local market characteristics, with some merchants struggling to see why they should replace their existing terminals. Increasingly, hardware companies are looking to position themselves as payment systems providers, challenging the positioning of traditional incumbent acquirers and other PSPs."

Looking ahead to a future in which mobile and Person-to-Business (P2B) payments are increasingly important, some retailers may question the value of a significant infrastructure upgrade for POS terminals alone. That's because new payment methods are proliferating that have nothing to do with cards, from mobile and non-card P2B, to wearables, biometrics, and RFID-enabled systems which let consumers leave stores and have payment taken from their bank accounts. This last example effectively does away with the payment terminal, checkouts and associated queues.

Get Uber It

One arrangement rocketing in popularity in Europe and North America is the "uberisation" of payments in verticals such as restaurants and events. Companies like Uber Eats, Skipthedishes.com, GrubHub and StubHub remove the need to pay in person by linking their app to a consumer's credit card or bank account. Hungry customers make their order over the internet and receive their meal by delivery or pick up at the restaurant, with settlement directly to the restaurant's bank. In the last year, GrubHub has seen 47 percent revenue growth and a 21 percent increase in its customer numbers in the US.

Despite strong growth in these alternative payments, and the rapid rise of digital and mobile, cash, cheques and cards still constitute 95 percent of all payments made in Europe and North America. As one industry source puts it, "There's a lot of talk about new methods, but the payment card is a low-cost, high-value, high usage item. The cost of issuing cards has always been low compared to their utility as global payments devices."

So if neither cards nor the POS terminal are going away any time soon, what upgrade option should merchants consider? One choice is simply to upgrade the existing POS infrastructure to accept contactless and the new v4 PCI standards – but it's possible this could risk missing out on the development of new methods of payment such as cardless digital payments which have proven enormously popular in China and other markets.

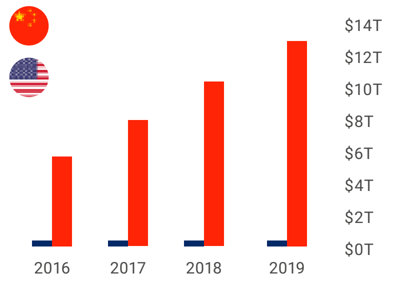
Whilst it's conceivable that mobile and digital could grow to be as important as POS in Western markets, few industry experts see any real threat to the dominance of cards and terminals in the next five to ten years. Nonetheless, new forms of payment will begin encroaching on cards' traditional dominance in store – and retailers need to be ready to respond to this trend, as well as maintaining compliance for their existing infrastructure.

The Customer is Fragmenting

Another coming challenge for retailers linked to infrastructure is fragmentation of their customer base, with different demographics increasingly expecting to pay using different methods. Depending on age and social status, customers want to pay with cash, cheque, card, mobile and, for the younger groups, P2B digital payments without physical check-out.

What's more, the advent of PSD2 in Europe and plans for Open Banking around the world threaten yet more complexity. Intended to foster more competition in the financial services market, Open Banking will also see the delivery of more direct-to-account solutions. In other words, retailers will be able to create products that debit consumers' bank accounts directly, without the intermediary of a card network or P2P system such as PayPal or Square. Given recent media reports that Visa and Mastercard are considering increasing interchange fees on US credit card transactions from April 2019, the fee reductions represented by these direct-to-account solutions look like an attractive alternative, especially for larger retailers who can bear the cost.

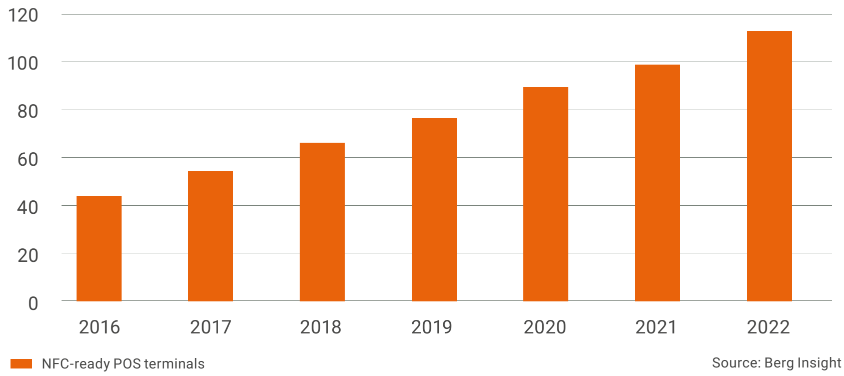
M PAYMENTS TRANSACTION VALUE



Source: Forrester Research

So one possible alternative for larger retailers might be an upgrade of existing infrastructure coupled with the creation of an own-brand direct-to-account solution through open banking. However, there are

INSTALLED BASE OF NFC-READY POS TERMINALS (WORLD 2016-2022)



Source: Berg Insight

still many challenges to be overcome with third party direct-to-account products, including responsibility for chargebacks, consumer rights and guarantees, and managing failed transactions. To date, the regulatory environment for such products is still developing.

Cash out of Chaos

Lots of different customer types looking to pay in many different ways, including via third parties through Open Banking: it sounds like an expensive headache for retailers. But industry experts insist there are opportunities for retailers that manage this new environment the right way. Alison Wilkes, Head of European Payments at FIS, notes that, "Anyone from a payment service provider to a retailer will need to embrace new payment types and provide a one-stop service for all payments." Wilkes goes on to list the opportunities on offer via new infrastructure, including instant loyalty rewards during purchase, and pop-up marketing campaign offers via digital device, from home or in-store. Andrew Cregan, Head of Payments Policy at the British Retail Consortium, agrees: "Done right, investing in new payments platforms can add value. It's possible to argue it costs more not to invest in these platforms, given the demand generation opportunities that the data created can bring."

The emerging retail payments environment will be about establishing consumer identity and protecting that identity. One means of establishing identity will be through Secure Customer Authentication, or SCA, which is mandated by the EU's PSD2 directive for open banking. And there will be benefits to those retailers that manage to establish a single digital identity for consumers across all their payment channels. Establishing this single identity is key to something Chris Kronenthal from payment systems integrator FreedomPay calls "unified commerce." According to Kronenthal, "the method of payment will come to mean less in the years ahead. What will matter will be secure multi-factor authentication to confirm the identity of all parties in a transaction, a smooth transaction process with confirmation of transaction, and uniform engagement across any channel including a customer's preferences: reward programmes, loyalty, and payments."

FreedomPay have successfully installed an EMV commerce platform for MGM Resorts in North America which removes some conditions in which PCI validation is required, and allows transactions to be stored offline for batch processing. The system uses enhanced data security at all points of sale inside MGM Resorts whether on-line, in person or via mobile device. But it's not clear that a EMV-compliant system would necessarily remove all compliance requirements, according to Troy Leach, Chief Technology Officer at PCI. Leach notes that, "the EMV standard addresses data functionality, but not concerns over security breaches to the system. For most issuers and acquirers, the expectation will still exist that all terminals will be tested to PCI standards."

So even if an infrastructure upgrade helps manage the technical complexity of multiple payment methods for merchants, it may not remove the need for continued security upgrades and testing. And then there's the cultural issue - some consumers may still want physical receipts after every transaction, rather than digital messages or a final settlement email confirming that they've paid what they owe. FreedomPay's Kronenthal predicts "we'll see some demographics switch to non-device transactions" given their preference for physical transaction confirmation.

Again, larger retailers appear to have an advantage, inasmuch as they can create their own bespoke payments infrastructure for roll-out across thousands of locations. This is something Starbucks' Coffee has done to good effect, integrating in-store, online and mobile payments via an app, card and loyalty points scheme.

Identifying the future

The nexus between payments and customer ID verification is one that retailers should consider carefully when looking to upgrade or replace their infrastructure. FreedomPay's work with MGM is further evidence that the online and physical retail environments are merging – and that identity is at the heart of it all. Other examples include Amazon offering a 5 percent discount on purchases from Whole Foods stores for its Prime customers following in-store verification, and Kenneth Cole and other US retailers trialling in-store and online offers based on consumers' geolocation data and web search history. None of these innovations would be possible without confirmed customer identity.

> "All players need to embrace new payment types and provide a one-stop service for all payments."
>
> - Alison Wilkes, Head of European Payments, FIS

Beat the breach

If one accepts that identity is central to the new payments landscape, then protecting that identity through improved data security becomes key for retailers. Recent data breaches to India's Aadhaar identification system which compromised the country's Unified Payments Interface (UPI) show just how important data security is to making next-generation payments work. Indeed, one senior industry figure speaking on condition of anonymity described data security as "the next major public policy issue", calling the UK Government's proposed fine of £500,000 for Facebook after the Cambridge Analytica scandal, "the tip of the iceberg."

As new forms of payment proliferate, retailers need to manage complexity and deliver on customer expectations of smooth, secure and rapid payment experiences. While new comprehensive infrastructure solutions appear to offer some benefits, they will not remove all testing and upgrade requirements for retailers. What's more, the need to identify customers accurately in multiple environments – and the requirement to protect their data – would appear to be large and growing concerns for retailers that may end up dwarfing their choice of payments infrastructure over the next decade. The management challenge will lie in identifying the right problem to fix at the right time, and to find a solution that best fits the needs of each retailer and the requirements of their customer base.